

# EXHIBIT 1

# CONGRESSIONAL LEADERS CITE TELECOMMUNICATIONS CONCERNS WITH FIRMS THAT HAVE TIES WITH CHINESE GOVERNMENT

Search this Site

---

**Tuesday, October 19, 2010**

**WASHINGTON, D.C.** – A bipartisan group of congressional leaders today wrote the Chairman of the Federal Communications Commission requesting more information regarding plans for ensuring the security of our nation’s telecommunications networks, in light of a proposed deal between Sprint, Cricket, and two Chinese-based companies.

“As you are aware, two Chinese companies, Huawei Technologies Co., Ltd. and ZTE Corporation, are aggressively seeking to supply sensitive equipment for U.S. telecommunications infrastructure and/or serve as operator and administrator of U.S. networks, and increase their role in the U.S. telecommunications sector through acquisition and merger,” U.S. Sens. Jon Kyl (R-Ariz.), Joe Lieberman (ID-Conn.), and Susan Collins (R-Maine), and U.S. Rep. Sue Myrick (R-N.C.) wrote.

The senators went on to cite recent government and media reports that show Huawei and ZTE have “significant ties to the Chinese military,” and that both companies have “received tens of billions of dollars in export financing and ‘low- to no-interest loans’ that needn’t be repaid from the Chinese government.”

“We are very concerned that these companies are being financed by the Chinese government and greatly influenced by the Chinese military, which may create an opportunity for the Chinese military to manipulate switches, routers, or software embedded in American telecommunications network so that communications can be intercepted, tampered with, or purposely misrouted. This would pose a real threat to our national security.”

The full text of the letter can be found below:

October 19, 2010



The Honorable Julius Genachowski  
Chairman  
Federal Communications Commission  
445 12th Street, SW  
Room 8B201  
Washington, DC 20554

Dear Chairman Genachowski:

We write to request information concerning the FCC's plans for ensuring the security of our nation's telecommunications networks. As you are aware, two Chinese companies, Huawei Technologies Co., Ltd. and ZTE Corporation, are aggressively seeking to supply sensitive equipment for U.S. telecommunications infrastructure and/or serve as operator and administrator of U.S. networks, and increase their role in the U.S. telecommunications sector through acquisition and merger. We understand they are in active discussions with two U.S. companies – Sprint and Cricket – and other prospective deals may be on the horizon. The sensitivity of information transmitted in communications systems, as well as the potential for foreign espionage, requires that the U.S. government take decisive action to ensure the security of our telecommunications networks.

Huawei and ZTE are among the largest manufacturers of sensitive telecommunications equipment in the world. In fact, the New York Times reported in November that Huawei is now the world's second largest telecommunications equipment manufacturer. A 2009 report by the Department of Defense (DOD) and a 2005 report from the RAND Corporation state that Huawei has significant ties to the Chinese military, the People's Liberation Army (PLA). In addition, both companies have, according to published reports, received tens of billions of dollars in export financing and "low- to no-interest 'loans' that needn't be repaid" from the Chinese government.

We are very concerned that these companies are being financed by the Chinese government and are potentially subject to significant influence by the Chinese military which may create an opportunity for manipulation of switches, routers, or software embedded in American telecommunications network so that communications can be disrupted, intercepted, tampered with, or purposely misrouted. This would pose a real threat to our national security. We understand that other governments, including those of the United Kingdom, Australia, Canada, and India may already have raised such concerns.

In addition, changes in the telecommunications market are causing domestic carriers to outsource their network operations to telecommunications equipment suppliers. So it is possible that U.S. telecommunications will be managed in whole or in part from China or by Chinese nationals if the market is unconstrained. This trend has already emerged in the telecommunications networks of many of our closest allies, including those with whom we conduct sensitive intelligence activities.

While Huawei and ZTE have in the past focused on other parts of the world, they have recently taken aggressive steps to increase penetration into the U.S. telecommunications market. Huawei, for example, has made several bids to supply telecommunications equipment at low prices with attractive financing, and it has been making more sales of late. Deals to directly supply equipment to the U.S. telecommunications infrastructure are, of course, not subject to CFIUS requirements, which only apply when a foreign firm is seeking to purchase or obtain a controlling interest in a U.S. company that is deemed to have a national security consequence. But when telecommunications carriers purchase equipment from Huawei, the result is that U.S. communications will travel over switches, routers, and other equipment that was manufactured and designed in China and may be remotely accessed and programmed from that country, and the CFIUS process cannot protect against it.

Given the role of the FCC, and its requirement to take actions to protect the public interest, we would like to know what the FCC is doing to protect the U.S. telecommunications system and would appreciate your prompt and detailed response to the following questions:

1. Does the FCC have the legal authority to review (in consultation and coordination with other agencies) foreign technologies, including equipment and software, to determine the risk posed to U.S. telecommunication networks? Is it doing so? How?
2. Does the FCC work with the Department of Homeland Security or the Intelligence Community to better understand potential risks posed to U.S. telecommunications networks? What is the mechanism for this consultation?
3. Does the FCC believe there are risks to U.S. telecommunications carriers buying foreign technology that may subject U.S. telecommunications networks to increased risk of espionage or interference with operations? What are those risks? Has the FCC so advised U.S. telecommunications carriers of these risks? Specifically, has the FCC had any discussions with Sprint or Cricket about the transactions they are considering with

Huawei, according to reports? And has the FCC considered whether there should be limitations on foreign equipment employed in the proposed build out of the 700 MHz “D” Block of spectrum that may be used to provide a broadband network for public safety?

4. Has the FCC monitored the sale of foreign telecommunications equipment, software or services to U.S. carriers? How much of this equipment has been manufactured, produced or provided by companies like Huawei and ZTE that are closely linked to a foreign government and/or foreign military? Which U.S. telecommunications companies have purchased it? (Please include a detailed analysis of the geographic regions covered by those networks.)

5. Does the FCC have information, or has it seen reports, that ZTE and Huawei are subsidized – e.g., including low- or no-interest loans, loan forgiveness, or restrictions on access to People’s Republic of China (PRC) or PLA procurement markets – by the PRC? Has it shared or sought this information through the U.S. Trade Representative or Department of Commerce and asked either office to investigate unfair trade practices for potential WTO violations? Does the FCC believe such subsidies create an unfair advantage over U.S. firms for Huawei and ZTE?

6. Does the FCC believe there are risks of outsourcing to foreign companies the responsibility for operating and administering U.S. telecommunications carrier networks? Please explain what the FCC has determined are those risks. Has the FCC so advised U.S. telecommunications carriers about these risks? What steps has the FCC taken to mitigate those risks?

7. Please describe in detail whether the effective implementation of the Communications Assistance for Law Enforcement Act (CALEA) is impacted by outsourcing to foreign companies the responsibility for operating and administering U.S. telecommunications carrier networks. Is effective implementation of CALEA impacted by the provision of telecommunications equipment, software, or services used by U.S. telecommunications companies by foreign companies tied to foreign militaries or foreign governments? What policies has the FCC adopted to deal with these impacts?

We appreciate your responses and your service to ensure the security of U.S. telecommunications networks.

Sincerely,

JON KYL

United States Senator

JOSEPH LIEBERMAN

United States Senator

SUSAN M. COLLINS

United States Senator

SUE MYRICK

United States Representative

CC: The Honorable Janet Napolitano, Secretary, Department of Homeland  
Security

The Honorable Ron Kirk, United States Trade Representative

The Honorable Robert Mueller, Director, Federal Bureau of Investigation

---

**Print**

**Email**

Like [Sign Up](#) to see what your friends like.

Tweet

# EXHIBIT 2



## **Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE**

A report by Chairman Mike Rogers and Ranking Member C.A.  
Dutch Ruppersberger of the Permanent Select Committee on  
Intelligence

U.S. House of Representatives  
112th Congress  
October 8, 2012

## Contents

<b>Executive Summary .....</b>	<b>iv</b>
<b>Report.....</b>	<b>1</b>
I. The threat posed to U.S. national-security interests by vulnerabilities in the telecommunications supply chain is an increasing priority given the country’s reliance on interdependent critical infrastructure systems; the range of threats these systems face; the rise in cyber espionage; and the growing dependence all consumers have on a small group of equipment providers. ....	1
A. China has the means, opportunity, and motive to use telecommunications companies for malicious purposes. ....	2
B. Suggested “mitigation measures” cannot fully address the threat posed by Chinese telecommunications companies providing equipment and services to United States critical infrastructure. ....	4
II. Investigation .....	7
A. Scope of Investigation .....	7
B. Investigative Process .....	8
C. Investigative Challenges.....	10
III. Summary of Findings .....	11
A. The Committee finds that Huawei did not fully cooperate with the investigation and was unwilling to explain its relationship with the Chinese government or Chinese Communist Party, while credible evidence exists that Huawei fails to comply with U.S. laws. ....	12
i. Huawei did not provide clear and complete information on its corporate structure and decision-making processes, likely remains dependent on the Chinese government for support. ....	13
ii. Huawei failed to explain its relationships with the Chinese government, and its assertions denying support by the Chinese government are not credible.....	21
iii. Huawei admits that the Chinese Communist Party maintains a Party Committee within the company, but it failed to explain what the Party	

Committee does on behalf of the Party or which individuals compose the Committee.....	22
iv. Huawei’s corporate history suggests ties to the military, and Huawei failed to provide detailed answers to questions about those connections. ....	24
v. Huawei’s failure to provide information about the Chinese government’s 1999 investigation of the company for tax fraud exemplifies a company that refuses to be transparent; the apparent ease with which Huawei ended the investigation undermines Huawei’s assertion that the Chinese government finds Huawei to be a disfavored telecommunications solutions provider in China. ....	25
vi. Huawei failed to explain its relationships with western consulting firms, and any claims that its success is on account of those relationships, rather than support by the Chinese government, are not credible. ....	26
vii. Huawei failed to answer key questions or provide supporting documentation for its claims to be financially independent of the Chinese government. ....	27
viii. Huawei failed to provide sufficient details or supporting documentation on its operations, financing, and management in the United States, undermining its claims of being a completely independent subsidiary of Huawei’s parent company in Shenzhen, China. ....	29
ix. Evidence shows that Huawei exhibits a pattern of disregard for the intellectual property rights of other entities and companies in the United States. ....	31
x. Huawei failed to provide details of its operations in Iran, though it denied doing business with the government of Iran, and did not provide evidence to support its claims that it complies with all international sanctions or U.S. export laws. ....	32
xi. Huawei refused to provide details on its R&D programs, and other documents undermine its claim that Huawei provides no R&D for the Chinese military or intelligence services. ....	33
xii. Former and current Huawei employees provided evidence of a pattern and practice of potentially illegal behavior by Huawei officials. ....	34



B.	ZTE failed to answer key questions or provide supporting documentation supporting its assertions; instead, it asserted that answering the Committee’s requests about its internal corporate activities would leave the company criminally liable under China’s states-secrets laws.....	35
i.	ZTE did not alleviate Committee concerns about the control of Chinese state-owned enterprises in ZTE’s business decisions and operations. ....	37
ii.	ZTE maintains a Chinese Party Committee within the company, but has not fully clarified how the Party Committee functions, who chooses its members, and what relationship it has with the larger Chinese Communist Party. ....	40
iii.	ZTE failed to disclose information about its activities in the U.S.....	42
iv.	ZTE failed to provide any answers or evidence about its compliance with intellectual property or U.S. export-control laws.....	42
v.	ZTE failed to provide clear answers to Committee questions about its R&D activities, particularly as they relate to any military or government projects. ....	43
Conclusion and Recommendations.....		44

**House Permanent Select Committee on Intelligence**

**Chairman and Ranking Member Investigative Report on**

**The U.S. National Security Issues Posed by Chinese  
Telecommunications Companies Huawei and ZTE**

**Executive Summary**

In February 2011, Huawei Technologies Company, the leading Chinese telecommunications equipment manufacturer, published an open letter to the U.S. Government denying security concerns with the company or its equipment, and requesting a full investigation into its corporate operations.<sup>1</sup> Huawei apparently believed – correctly – that without a full investigation into its corporate activities, the United States could not trust its equipment and services in U.S. telecommunications networks.<sup>2</sup>

The House Permanent Select Committee on Intelligence (herein referred to as “the Committee”) initiated this investigation in November 2011 to inquire into the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States. Prior to initiating the formal investigation, the Committee performed a preliminary review of the issue, which confirmed significant gaps in available information about the Chinese telecommunications sector, the histories and operations of specific companies operating in the United States, and those companies’ potential ties to the Chinese state. Most importantly, that preliminary review highlighted the potential security threat posed by Chinese telecommunications companies with potential ties to the Chinese government or military. In particular, to the extent these companies are influenced by the state, or provide Chinese intelligence services access to telecommunication networks, the opportunity exists for further economic and foreign espionage by a foreign nation-state already known to be a major perpetrator of cyber espionage.

As many other countries show through their actions, the Committee believes the telecommunications sector plays a critical role in the safety and security of our nation, and is thus a target of foreign intelligence services. The

Committee's formal investigation focused on Huawei and ZTE, the top two Chinese telecommunications equipment manufacturers, as they seek to market their equipment to U.S. telecommunications infrastructure. The Committee's main goal was to better understand the level of risk posed to the United States as these companies hope to expand in the United States. To evaluate the threat, the investigation involved two distinct yet connected parts: (1) a review of open-source information on the companies' histories, operations, financial information, and potential ties to the Chinese government or Chinese Communist Party; and (2) a review of classified information, including a review of programs and efforts of the U.S. Intelligence Community (IC) to ascertain whether the IC is appropriately prioritizing and resourced for supply chain risk evaluation.<sup>3</sup>

Despite hours of interviews, extensive and repeated document requests, a review of open-source information, and an open hearing with witnesses from both companies, the Committee remains unsatisfied with the level of cooperation and candor provided by each company. Neither company was willing to provide sufficient evidence to ameliorate the Committee's concerns. Neither company was forthcoming with detailed information about its formal relationships or regulatory interaction with Chinese authorities. Neither company provided specific details about the precise role of each company's Chinese Communist Party Committee. Furthermore, neither company provided detailed information about its operations in the United States. Huawei, in particular, failed to provide thorough information about its corporate structure, history, ownership, operations, financial arrangements, or management. Most importantly, neither company provided sufficient internal documentation or other evidence to support the limited answers they did provide to Committee investigators.

During the investigation, the Committee received information from industry experts and current and former Huawei employees suggesting that Huawei, in particular, may be violating United States laws. These allegations describe a company that has not followed United States legal obligations or international standards of business behavior. The Committee will be referring these allegations to Executive Branch agencies for further review, including possible investigation.

In sum, the Committee finds that the companies failed to provide evidence that would satisfy any fair and full investigation. Although this alone does not prove wrongdoing, it factors into the Committee's conclusions below. Further, this report contains a classified annex, which also adds to the Committee's concerns about the risk to the United States. The investigation concludes that the risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national-security interests.

Based on this investigation, the Committee provides the following recommendations:

**Recommendation 1:** The United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies.

- The United States Intelligence Community (IC) must remain vigilant and focused on this threat. The IC should actively seek to keep cleared private sector actors as informed of the threat as possible.
- The Committee on Foreign Investment in the United States (CFIUS) must block acquisitions, takeovers, or mergers involving Huawei and ZTE given the threat to U.S. national security interests. Legislative proposals seeking to expand CFIUS to include purchasing agreements should receive thorough consideration by relevant Congressional committees.
- U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts. Similarly, government contractors – particularly those working on contracts for sensitive U.S. programs – should exclude ZTE or Huawei equipment in their systems.

**Recommendation 2:** Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and

ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.

**Recommendation 3:** Committees of jurisdiction within the U.S. Congress and enforcement agencies within the Executive Branch should investigate the unfair trade practices of the Chinese telecommunications sector, paying particular attention to China's continued financial support for key companies.

**Recommendation 4:** Chinese companies should quickly become more open and transparent, including listing on a western stock exchange with advanced transparency requirements, offering more consistent review by independent third-party evaluators of their financial information and cyber-security processes, complying with U.S. legal standards of information and evidentiary production, and obeying all intellectual-property laws and standards. Huawei, in particular, must become more transparent and responsive to U.S. legal obligations.

**Recommendation 5:** Committees of jurisdiction in the U.S. Congress should consider potential legislation to better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure. Such legislation could include increasing information sharing among private sector entities, and an expanded role for the CFIUS process to include purchasing agreements.

## Report

**I. The threat posed to U.S. national-security interests by vulnerabilities in the telecommunications supply chain is an increasing priority given: the country's reliance on interdependent critical infrastructure systems; the range of threats these systems face; the rise in cyber espionage; and the growing dependence all consumers have on a small group of equipment providers.**

The United States' critical infrastructure, and in particular its telecommunications networks, depend on trust and reliability. Telecommunications networks are vulnerable to malicious and evolving intrusions or disruptive activities. A sufficient level of trust, therefore, with both the provider of the equipment and those performing managed services must exist at all times. A company providing such equipment, and particularly any company having access to or detailed knowledge of the infrastructures' architectural blueprints, must be trusted to comply with United States laws, policies, and standards. If it cannot be trusted, then the United States and others should question whether the company should operate within the networks of our critical infrastructure.

The risk posed to U.S. national-security and economic interests by cyber-threats is an undeniable priority. First, the country's reliance on telecommunications infrastructure includes more than consumers' use of computer systems. Rather, multiple critical infrastructure systems depend on information transmission through telecommunications systems. These modern critical infrastructures include electric power grids; banking and finance systems; natural gas, oil, and water systems; and rail and shipping channels; each of which depend on computerized control systems. Further, system interdependencies among these critical infrastructures greatly increase the risk that failure in one system will cause failures or disruptions in multiple critical infrastructure systems.<sup>4</sup> Therefore, a disruption in telecommunication networks can have devastating effects on all aspects of modern American living, causing shortages and stoppages that ripple throughout society.

Second, the security vulnerabilities that come along with this dependence are quite broad, and range from insider threats<sup>5</sup> to cyber espionage and attacks from sophisticated nation states. In fact, there is a growing recognition of vulnerabilities resulting from foreign-sourced telecommunications supply chains used for U.S. national-security applications. The FBI, for example, has assessed with high confidence that threats to the supply chain from both nation-states and criminal elements constitute a high cyber threat.<sup>6</sup> Similarly, the National Counterintelligence Executive assessed that

“foreign attempts to collect U.S. technological and economic information will continue at a high level and will represent a growing and persistent threat to US economic security.”<sup>7</sup>

Third, the U.S. government must pay particular attention to products produced by companies with ties to regimes that present the highest and most advanced espionage threats to the U.S., such as China. Recent cyber-attacks often emanate from China, and even though precise attribution is a perennial challenge, the volume, scale, and sophistication often indicate state involvement. As the U.S.-China Commission explained in its unclassified report on China’s capabilities to conduct cyber warfare and computer network exploitation (CNE), actors in China seeking sensitive economic and national security information through malicious cyber operations often face little chance of being detected by their targets.<sup>8</sup>

Finally, complicating this problem is the fact that Chinese telecommunications firms, such as Huawei and ZTE, are rapidly becoming dominant global players in the telecommunications market. In another industry, this development might not be particularly concerning. When those companies seek to control the market for sensitive equipment and infrastructure that could be used for spying and other malicious purposes, the lack of market diversity becomes a national concern for the United States and other countries.<sup>9</sup> Of note, the United States is not the only country focusing on these concerns. Australia expressed similar concerns when it chose to ban Huawei from its national broadband infrastructure project.<sup>10</sup> Great Britain has attempted to address the concerns by instituting an evaluation regime that limits Huawei’s access to the infrastructure and evaluates any Huawei equipment and software before they enter the infrastructure.<sup>11</sup>

**A. China has the means, opportunity, and motive to use telecommunications companies for malicious purposes.**

Chinese intelligence collection efforts against the U.S. government are growing in “scale, intensity and sophistication.”<sup>12</sup> Chinese actors are also the world’s most active and persistent perpetrators of economic espionage.<sup>13</sup> U.S. private sector firms and cyber-security specialists report an ongoing onslaught of sophisticated computer network intrusions that originate in China, and are almost certainly the work of, or have the backing of, the Chinese government.<sup>14</sup> Further, Chinese intelligence services, as well as private companies and other entities, often recruit those with direct access to corporate networks to steal trade secrets and other sensitive proprietary data.<sup>15</sup>

These cyber and human-enabled espionage efforts often exhibit sophisticated technological capabilities, and these capabilities have the potential to translate into efforts to insert malicious hardware or software implants into Chinese-manufactured

telecommunications components and systems marketed to the United States. Opportunities to tamper with telecommunications components and systems are present throughout product development, and vertically integrated industry giants like Huawei and ZTE provide a wealth of opportunities for Chinese intelligence agencies to insert malicious hardware or software implants into critical telecommunications components and systems.<sup>16</sup> China may seek cooperation from the leadership of a company like Huawei or ZTE for these reasons. Even if the company's leadership refused such a request, Chinese intelligence services need only recruit working-level technicians or managers in these companies. Further, it appears that under Chinese law, ZTE and Huawei would be obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security.<sup>17</sup>

A sophisticated nation-state actor like China has the motivation to tamper with the global telecommunications supply chain, with the United States being a significant priority. The ability to deny service or disrupt global systems allows a foreign entity the opportunity to exert pressure or control over critical infrastructure on which the country is dependent. The capacity to maliciously modify or steal information from government and corporate entities provides China access to expensive and time-consuming research and development that advances China's economic place in the world. Access to U.S. telecommunications infrastructure also allows China to engage in undetected espionage against the United States government and private sector interests.<sup>18</sup> China's military and intelligence services, recognizing the technological superiority of the U.S. military, are actively searching for asymmetrical advantages that could be exploited in any future conflict with the United States.<sup>19</sup> Inserting malicious hardware or software implants into Chinese-manufactured telecommunications components and systems headed for U.S. customers could allow Beijing to shut down or degrade critical national security systems in a time of crisis or war. Malicious implants in the components of critical infrastructure, such as power grids or financial networks, would also be a tremendous weapon in China's arsenal.

Malicious Chinese hardware or software implants would also be a potent espionage tool for penetrating sensitive U.S. national security systems, as well as providing access to the closed American corporate networks that contain the sensitive trade secrets, advanced research and development data, and negotiating or litigation positions that China would find useful in obtaining an unfair diplomatic or commercial advantage over the United States.

In addition to supply chain risks associated with hardware and software, managed services also pose a threat. Managed services, sold as part of the systems maintenance



contract, allow for remote network access for everyday updates to software and patches to glitches. Unfortunately, such contracts may also allow the managed-service contractor to use its authorized access for malicious activity under the guise of legitimate assistance. Such access also offers an opportunity for more-tailored economic or state-sponsored espionage activities. Telecommunications companies such as Huawei are seeking to expand service portions of their business.<sup>20</sup>

The U.S. Government has acknowledged these concerns with telecommunications supply chain risk for several years. Indeed, as one of twelve critical infrastructure protection priorities outlined in the White House's 2009 Comprehensive National Cybersecurity Initiative (CNCI), Supply Chain Risk Management (SCRM) is identified as a national concern. Similarly, the Executive Branch continues to review supply chain issues consistent with its National Strategy for Global Supply Chain Security, released in January 2012. A key part of the management of supply chain risk, as explained in the report, is to properly "understand and identify vulnerabilities to the supply chain that stem from both exploitation of the system by those seeking to introduce harmful products or materials and disruptions from intentional attacks, accidents, or natural disasters."<sup>21</sup>

**B. Suggested "mitigation measures" cannot fully address the threat posed by Chinese telecommunications companies providing equipment and services to United States critical infrastructure.**

Many countries struggle with the potential threats posed by untrustworthy telecommunications companies. In Great Britain, the government took initial steps (as part of an overall mitigation strategy) to address its concerns by entering into an agreement with Huawei to establish an independently managed Cyber Security Evaluation Centre (CSEC). CSEC conducts independent reviews of Huawei's equipment and software deployed to the United Kingdom's telecommunications infrastructure, and provides such results to the relevant UK carriers and UK government. The goal of the British government is to attempt to lessen the threat that Huawei products deployed in critical UK telecommunications infrastructure pose to the availability or integrity of UK networks.

Huawei and ZTE have proposed similar schemes for products entering the United States market, administered without U.S. government involvement, but by Electronic Warfare Associates or other private-sector security firms.<sup>22</sup> These partnerships seek to address concerns that the companies could permit the Chinese government to insert features or vulnerabilities into their products, which would assist espionage or cyber warfare. Unfortunately, there are concerns that such efforts if taken in the United States

will fall short of addressing security concerns given the breadth and scale of the U.S. telecommunications market.

Post-production evaluation processes are a standard approach to determining the security properties of complex, software-intensive systems. Processes like the Common Criteria for Information Technology Security Evaluation and various private certification services define a process by which an evaluator measures a product against a set of standards and assigns a security rating. The rating is meant to help a consumer know how much confidence to place in the security features of the device or software package. Both the implementation of the system and the methodology used to develop it, as documented by the manufacturer, are typically used as evidence for the chosen rating. Further, such processes are not necessarily designed to uncover malicious code but to encourage a foundational security baseline in security-enabled products.

For a variety of technical and economic reasons, evaluation programs as proposed by Huawei and ZTE are less useful than one might expect. In fact, the programs may create a false sense of security that an incomplete, flawed, or misapplied evaluation would provide. An otherwise careful consumer may choose to forego a thorough threat, application, and environment-based risk assessment, and the costs such evaluations entail, because an accredited outside expert has “blessed” the product in some way.

One key issue not addressed by standardized third-party security evaluations is product and deployment diversity. The behavior of a device or system can vary wildly depending on how and where it is configured, installed, and maintained. For time and cost reasons, an evaluation usually targets a snapshot of one product model configured in a specific and often unrealistically restrictive way. The pace of technology development today drives products to evolve far more rapidly than any third-party comprehensive evaluation process can follow. The narrow configuration specification used during testing almost ensures that an evaluated device will be deployed in a way not specifically covered by a formal evaluation. A security evaluation of a complex device is useless if the device is not deployed precisely in the same configuration as it was tested.

The evaluation of products prior to deployment only addresses the product portion of the lifecycle of networks. It is also important to recognize that how a network operator oversees its patch management, its trouble-shooting and maintenance, upgrades, and managed-service elements, as well as the vendors it chooses for such services, will affect the ongoing security of the network.

Vendors financing their own security evaluations create conflicts of interest that lead to skepticism about the independence and rigor of the result. A product

manufacturer will naturally pursue its own interests and ends which are not necessarily aligned with all interests of the consumers. A different, but related, race to the bottom has been noted for the similarly vendor-financed Common Criteria evaluations.<sup>23</sup> The designers of the Common Criteria system understood this danger and implemented government certification for evaluators. The precaution seems mostly cosmetic as no certification has ever been challenged or revoked despite gaming and poor evaluation performance. Given similar concerns and about conflicts of interest, Huawei's U.K. evaluators of Huawei equipment have been vetted by the U.K. government and hold government security clearances, and the U.K. process has the support of the U.K. Carriers. It is not clear yet, however, that such steps would readily transfer to the U.S. market or successfully overcome the natural incentives of the situation and lead to truly independent investigations.

The task of finding and eliminating every significant vulnerability from a complex product is monumental. If we also consider flaws intentionally inserted by a determined and clever insider, the task becomes virtually impossible.<sup>24</sup> While there is a large body of literature describing techniques for finding latent vulnerabilities in hardware and software systems, no such technique claims the ability to find all such vulnerabilities in a pre-existing system. Techniques do exist that can prove a system implementation matches a design which has been formally verified to be free of certain types of flaws.<sup>25</sup> However, such formal techniques must be incorporated throughout the design and development process to be effective. They cannot currently be applied to a finished product of significant size or complexity. Even when embedded into a design and development process, formal techniques of this type do not yet scale to the size of complete commercial telecommunication systems. It is highly unlikely that a security evaluation partnership such as that proposed by Huawei or ZTE, independent of its competence and motives, will be able to identify all relevant flaws in products the size and complexity of core network infrastructure devices. If significant flaws remain in widely fielded products and processes that are known to a potential adversary, it seems like the evaluation process has provided only marginal benefit.

A security evaluation of potentially suspect equipment being deployed in critical infrastructure roles may seem like an answer to the security problems posed. Unfortunately, given the complexity of the telecommunications grid, the limitations of current security evaluation techniques, and the economics of vendor-financed analyses provide a sense of security but not actual security. Significant security is available only through a thoughtful design and engineering process that addresses a complete system-of-systems across its full lifecycle, from design to retirement and includes aspects such as discrete technology components, their interactions, the human environment, and threats

from the full spectrum of adversaries. The result of such a process should be a convincing set of diverse evidence that a system is worthy of our trust.<sup>26</sup>

## **II. Investigation**

### **A. Scope of Investigation**

The House Permanent Select Committee on Intelligence is responsible for authorizing the intelligence activities of the United States and overseeing those activities to ensure that they are legal, effective, and properly resourced to protect the national security interests of the United States. Specifically, the Committee is charged with reviewing and studying on a continuing basis the authorities, programs, and activities of the Intelligence Community and with reviewing and studying on an exclusive basis the sources and methods of the community.<sup>27</sup> Along with this responsibility is the obligation to study and understand the range of foreign threats faced by the United States, including those directed against our nation's critical infrastructure. Similarly, the Committee must evaluate the threats from foreign intelligence operations and ensure that the country's counterintelligence agencies are appropriately focused on and resourced to defeat those operations.<sup>28</sup>

The Committee's goals in this investigation were to inquire into the potential security risk posed by the top two Chinese telecommunications companies and review whether our government is properly positioned to understand and respond to that threat. An additional aim of this process has been to determine what information could be provided in an unclassified form to shed light on the key questions of whether the existence of these firms in our market would pose a national-security risk through the potential loss of control of U.S. critical infrastructure.

Of course, the United States' telecommunications sector increasingly relies on a global supply chain for the production and delivery of equipment and services. That reliance presents significant risks that other individuals or entities – including those backed by foreign governments – can and will exploit and undermine the reliability of the networks. Better understanding the supply-chain risks we face is vital if we are to protect the security and functionality of our networks and if we are to guard against national security and economic threats to those networks. The investigation's scope reflects the underlying need for the U.S. to manage the global supply chain system using a risk-based approach.

Recent studies highlight that actors in China are the source of more cyber-attacks than in any other country. The National Counterintelligence Executive, for example,

explained, in an open report on cyber-espionage, that “Chinese actors are the world’s most active and persistent perpetrators of economic espionage.”<sup>29</sup> Thus, the Committee focused on those companies with the strongest potential Chinese ties and those that also seek greater entry into the United States market. Both Huawei and ZTE are indigenous Chinese firms, with histories that include connections to the Chinese government. Both Huawei and ZTE have already incorporated United States’ subsidiaries, and both are seeking to expand their footprint in the United States market. Huawei has received, thus far, the greatest attention from analysts and the media. Given the similarities of the two companies, however, including their potential ties to the Chinese government, support by the Chinese government, and goals to further their U.S. presence, the Committee focused on both Huawei and ZTE.

Both Huawei and ZTE assert that the Committee should not focus only on them to the exclusion of all other companies that manufacture parts or equipment in China. The Committee recognizes that many non-Chinese companies, including U.S. technology companies, manufacture some of their products in China. But it is not only the location of manufacturing that is important to the risk calculation. It is also ownership, history, and the products being marketed. These may not be the only two companies presenting this risk, but they are the two largest Chinese-founded, Chinese-owned telecommunications companies seeking to market critical network equipment to the United States. To review supply chain risk, the Committee decided to focus first on the largest perceived vulnerabilities, with an expectation that the conclusion of this investigation would inform how to view the potential threat to the supply chain from other companies or manufacturers operating in China and other countries.

## **B. Investigative Process**

The Committee’s investigative process included extensive interviews with company and government officials, numerous document requests, and an open hearing with a senior official from both Huawei and ZTE. Committee staff reviewed available information on the specific companies, and Committee staff and members met with Huawei and ZTE officials for lengthy, in-depth meetings and interviews. Committee staff also toured the companies’ facilities and factories.

Specifically, on February 23, 2012, Committee staff met with and interviewed corporate executives of Huawei at its corporate headquarters in Shenzhen, China. The delegation toured Huawei’s corporate headquarters, reviewed company product lines, and toured a large manufacturing factory. Officials involved in the discussion from Huawei included Ken Hu, Huawei’s Deputy Chairman of the Board and Acting CEO; Evan Bai,

Vice President of the Treasury Management Office; Charlie Chen, Senior Vice President in charge of Huawei (USA); Jiang Xisheng, Secretary of the Board; John Suffolk, Global Security Officer; and Rose Hao, Export Regulator.

On April 12, 2012, Committee staff met with and interviewed corporate executives of ZTE at its corporate headquarters in Shenzhen, China. In addition to these meetings, the delegation took a brief tour of ZTE's corporate headquarters, including a factory site. Officials from ZTE included Zhu Jinyun, ZTE's Senior Vice President, U.S. and North America Market; Fan Qingfeng, Executive Vice President of Global Marketing and Sales; Guo Jianjun, Legal Director; Timothy Steinert, Independent Director of the Board (and Ali Baba Counsel); Ma Xuexing, Legal Director; Cao Wei, Security and Investor Relations with the Information Disclosure Office; Qian Yu, Security and Investor Relations with the Information Disclosure Office; and John Merrigan, attorney with DLA Piper.

In May of 2012, Ranking Member Ruppertsberger along with Committee members Representative Nunes, Representative Bachmann, and Representative Schiff traveled to Hong Kong to meet with senior officials of both Huawei and ZTE. In addition to the senior officials present at the staff meetings, the Committee members met with Ren Zhengfei, the founder and President of Huawei.

After the meetings, the Committee followed-up with several pages of written questions and document requests to fill in information gaps, inconsistent or incomplete answers, and the need for corroborating documentary evidence of many of the companies' factual and historical assertions. Unfortunately, neither company was completely or fully responsive to the Committee's document requests. Indeed, neither Huawei nor ZTE provided internal documents in response to the Committee's letter.<sup>30</sup> To attempt, again, to answer the remaining questions, the Committee called each company to an open hearing.

On September 13, 2012, the Committee held an open hearing with representatives of both ZTE and Huawei. The witnesses included Mr. Charles Ding, corporate senior vice president and Huawei's representative to the United States, and Mr. Zhu Jinyun, ZTE senior vice president for North America and Europe. The hearing was designed to be both thorough and fair. The witnesses were each given twenty minutes for an opening statement and each was aided by an interpreter during the question and answer portion of the hearing to ensure that the witnesses were given the maximum opportunity to understand the questions and answer completely and factually.<sup>31</sup>

Once again, the witnesses' answers were often vague and incomplete. For example, they claimed to have no understanding or knowledge of commonly used terms, could not answer questions about the composition of their internal Party Committees, refused to provide straightforward answers about their operations in the United States, sought to avoid answering questions about their histories of intellectual property protection, and claimed to have no understanding or knowledge of Chinese laws that force them to comply with the Chinese government's requests for access to their equipment. The companies' responses to the Committee's questions for the record after the hearing included similar evasive answers.

### **C. Investigative Challenges**

This unclassified report discloses the unclassified information the Committee received when trying to understand the nature of these companies, the formal role of the Chinese government or Chinese Communist Party within them, and their current operations in the United States. In pursuing this goal, the Committee faced many challenges, some of which are shared by many who seek to understand the relationship between the government and business in China and the threat posed to our infrastructure. These challenges include: the lack of transparency in Chinese corporate and bureaucratic structures that leads to a lack of trust; general private sector concerns with providing proprietary or confidential information; fears of retribution if private-sector companies or individuals discuss their concerns; and uncertain attribution of cyber attacks.

The classified annex provides significantly more information adding to the Committee's concerns. That information cannot be shared publicly without risking U.S. national security. The unclassified report itself, however, highlights that Huawei and ZTE have failed to assuage the Committee's significant security concerns presented by their continued expansion into the United States. Indeed, given the companies' repeated failure to answer key questions thoroughly and clearly, or support those answers with credible internal evidence, the national-security concerns about their operations have not been ameliorated. In fact, given their obstructionist behavior, the Committee believes addressing these concerns have become an imperative for the country.

In addition to the Committee's discussions with the companies, the Committee investigators spoke with industry experts and former and present employees about the companies. Companies around the United States have experienced odd or alerting incidents using Huawei or ZTE equipment. Officials with these companies, however, often expressed concern that publicly acknowledging these incidents would be detrimental to their internal investigations and attribution efforts, undermine their ongoing efforts to defend their systems, and also put at risk their ongoing contracts.



Similarly, statements by former or current employees describing flaws in the Huawei or ZTE equipment and other potentially unethical or illegal behavior by Huawei officials were hindered by employees' fears of retribution or retaliation.<sup>32</sup>

Further, the inherent difficulty in attributing the precise individual or entity responsible for known attacks within the United States continues to hinder the technological capability for investigators to determine the source of attacks or any connections among industry, government, and the hacker community within China.<sup>33</sup>

### **III. Summary of Findings**

Chinese telecommunications companies provide an opportunity for the Chinese government to tamper with the United States telecommunications supply chain. That said, understanding the level and means of state influence and control of economic entities in China remains difficult. As Chinese analysts explain, state control or influence of purportedly private-sector entities in China is neither clear nor disclosed.<sup>34</sup> The Chinese government and the Chinese Communist Party, experts explain, can exert influence over the corporate boards and management of private sector companies, either formally through personnel choices, or in more subtle ways.<sup>35</sup> As ZTE's submission to the Committee states, "the degree of possible government influence must vary across a spectrum."<sup>36</sup>

The Committee thus focused primarily on reviewing Huawei's and ZTE's ties to the Chinese state, including support by the Chinese government and state-owned banks, their connections to the Chinese Communist Party, and their work done on behalf of the Chinese military and intelligence services. The Committee also probed the companies' compliance with U.S. laws, such as those protecting intellectual property, to determine whether the companies can be trusted as good corporate actors. The Committee did not attempt a review of all technological vulnerabilities of particular ZTE and Huawei products or components. Of course, the Committee took seriously recent allegations of backdoors, or other unexpected elements in either company's products, as reported previously and during the course of the investigation. But the expertise of the Committee does not lend itself to comprehensive reviews of particular pieces of equipment.

The investigation sought to answer several key questions about the companies that would, including:

- What are the companies' histories and management structures, including any initial ties to the Chinese government, military, or Communist party?



- How and to what extent does the Chinese government or the Chinese Communist Party exert control or influence over the decisions, operations, and strategy of Huawei and ZTE?
- Are Huawei and ZTE treated as national champions or otherwise given unfair or special advantages or financial incentives by the Chinese government?
- What is the presence of each company in the United States market and how much influence does the parent company in Shenzhen influence its operations in the United States?
- Do the companies comply with legal obligations, including those protecting intellectual property rights and international sanctions regimes (such as those with respect to Iran)?

The Committee found the companies' responses to these lines of inquiry inadequate and unclear. Moreover, despite repeated requests, the companies' consistently provided very little – if any – internal documentation substantiating their answers. The few documents provided could rarely be authenticated or validated because of the companies' failure to follow standard document-production standards as provided by the Committee and standard with such investigations. Moreover, the apparent control of the Chinese government over this information remains a hindrance to a thorough investigation. One of the companies asserted clearly both verbally and in writing that it could not provide internal documentation that was not first approved by the Chinese government.<sup>37</sup> The fact that Chinese companies believe that their internal documentation or information remains a “state secret,” only heightens concerns about Chinese government control over these firms and their operations.

The Committee is disappointed that Huawei and ZTE neither answered fully nor chose to provide supporting documentation for their claims, especially given that Huawei requested a thorough and complete investigation. The Committee simply cannot rely on the statements of company officials that their equipment's presence in U.S. critical infrastructure does not present a threat, and that the companies are not, or would not be, under pressure by the Chinese government to act in ways contrary to United States interests. The findings below summarize what the Committee has learned from information available, and suggest avenues for further inquiry.

**A. The Committee finds that Huawei did not fully cooperate with the investigation and was unwilling to explain its relationship with the Chinese government or Chinese Communist Party, while credible evidence exists that it fails to comply with U.S. laws.**

Throughout this investigation, Huawei officials sought to portray the company as transparent. Huawei consistently refused, however, to provide detailed answers in

written form or provide internal documentation to support their answers to questions at the heart of the investigation. Specifically, Huawei would not fully describe the history, structure, and management of Huawei and its subsidiaries to the Committee's satisfaction. The Committee received almost no information on the role of Chinese Communist Party Committee within Huawei or specifics about how Huawei interacts in formal channels with the Chinese government. Huawei refused to provide details about its business operations in the United States, failed to disclose details of its dealings with the Chinese military or intelligence services, and would not provide clear answers on the firm's decision-making processes. Huawei also failed to provide any internal documents in response to the Committee's written document requests, thus impeding the Committee's ability to evaluate fully the company's answers or claims.

In addition to discussions with Huawei officials, the Committee has interviewed several current and former employees of Huawei USA, whose employees describe a company that is managed almost completely by the Huawei parent company in China, thus undermining Huawei's claims that its United States operations are largely independent of parent company. The testimony and evidence of individuals who currently or formerly worked for Huawei in the United States or who have done business with Huawei also brought to light several very serious allegations of illegal behavior that require additional investigation. The Committee will refer these matters to the Executive Branch for potential investigation.

These allegations were not the focus or thrust of the investigation, but they were uncovered in the course of the investigation. The Committee believes that they reveal a potential pattern of unethical and illegal behavior by Huawei officials, allegations that of themselves create serious doubts about whether Huawei can be trusted to operate in the United States in accordance with United States legal requirements and international codes of business conduct.

**i. Huawei did not provide clear and complete information on its corporate structure and decision-making processes, and it likely remains dependent on the Chinese government for support.**

Huawei markets itself as a "leading global ICT ["Information Communications Technology"] solution provider," that is "committed to providing reliable and secure networks."<sup>38</sup> Throughout the investigation, Huawei consistently denied having any links to the Chinese government and maintains that it is a private, employee-owned company.<sup>39</sup> Many industry analysts, however, have suggested otherwise; many believe, for example, that the founder of Huawei, Ren Zhengfei, was a director of the People's Liberation

Army (PLA) Information Engineering Academy, an organization that they believe is associated with 3PLA, China's signals intelligence division, and that his connections to the military continue.<sup>40</sup> Further, many analysts suggest that the Chinese government and military proclaim that Huawei is a "national champion" and provide Huawei market-distorting financial support.<sup>41</sup>

In seeking to understand the Chinese government's influence or control over Chinese telecommunications companies, the Committee focused on Huawei's corporate structure and decision-making processes. Better information about Huawei's corporate structure would also help answer lingering questions caused by Huawei's historic lack of transparency.<sup>42</sup> For years, analysts have struggled to understand how Huawei's purported employee-ownership model works in practice, and how that ownership translates into corporate leadership and decision-making.<sup>43</sup> Huawei repeatedly asserts that it is a private, employee-owned and controlled company that is not influenced by the Chinese government or Chinese Communist Party.<sup>44</sup> Executives also asserted that the unique shareholder and compensation arrangement is the foundation of the company's rise and success.

Available information does not align with Huawei's description of this structure, and many analysts believe that Huawei is not actually controlled by its common shareholders, but actually controlled by an elite subset of its management.<sup>45</sup> The Committee thus requested further information on the structure of the company's ownership. For example, the Committee requested that Huawei list the ten largest shareholders of the company. Huawei refused to answer.<sup>46</sup> At the hearing on September 13, 2012, Huawei admits that its shareholder agreement gives veto power to Ren Zhengfei, the founder and president of the company.<sup>47</sup> Other public statements by the company undermine the suggestion that the 60,000 supposed shareholders of Huawei control the company's decisions. For example, in the company's 2011 report, Mr. Ren highlighted that Huawei's Board of Directors:

will not make maximizing the interests of stakeholders (including employees, governments, and suppliers) its goal. Rather, it holds on to the core corporate values that are centered on customer interests and encourage employee dedication.<sup>48</sup>

Such statements undermine the credibility of Huawei's repeated claims that its employees control the company. Thus, to explore these conflicts, the Committee focused much attention on the shareholder program. Of note, the only nonpublic, purportedly internal documents that Huawei provided to the Committee in the course of the

investigation are unsigned copies of its shareholder agreement documents. Unfortunately, the Committee could not verify the legitimacy of these documents, because they were unsigned and non-official.

Huawei officials explained that Chinese law forbids foreigners from holding shares in Chinese companies absent a special waiver.<sup>49</sup> Current and former Huawei employees confirm that only Chinese nationals working at Huawei in the United States participate in the shareholding plan. The inability of non-Chinese employees of Huawei to hold shares of the company further erodes its claim that it is truly an employee-run organization as an entire group of employees are not only disadvantaged, but automatically excluded from any chance to participate in the process.

Huawei consistently asserted that the Chinese government has no influence over corporate behavior and that the company is instead managed as an employee-owned enterprise through Huawei's Employee Stock Ownership Program (ESOP). Officials explained that the shareholding plan is not a benefits plan; rather, it provides high-performing employees an option to buy dividend-providing shares and thereby share in the value of the company. Eligible employees are given the option to buy shares at a certain company determined price, and can only sell the shares when they leave the company or with approval.<sup>50</sup>

Huawei also provided staff access to shareholder ballots for shareholder representatives and the Board of Directors. These too did not appear to be facially fraudulent, but they were impossible to authenticate, especially as investigators were not allowed to remove the documents from Huawei's facilities for third-party validation. The documents appeared to highlight that shareholders have a write-in option for union representatives, but there is no such option for the Board of Directors. Rather, Huawei officials stated that the nominees for the Board are chosen prior to the vote by the previous Board. It was unclear how the original Board was established, and Huawei has consistently failed to provide any answers about who was previously on its Board of Directors.

Huawei further explained that in 1994, the first Company Law of China was officially published, regulating the establishment and operations of limited liability companies.<sup>51</sup> Under this law, the maximum number of shareholders was 50 individuals. Thus, in 1997, Huawei claims to have changed its legal structure to a limited liability company, and started the employee stock ownership program through the union. Similarly, Huawei asserted that in 1997, the City of Shenzhen issued policies regarding

employee shareholdings. According to Huawei, it designed its shareholder program to conform to the the Company Law of China, and the laws and policies of the City of Shenzhen.<sup>52</sup>

According to Huawei, the union, known as Union of Huawei Investment and Holding Co., Ltd., facilitates ESOP implementation. The Union is a lawfully registered association of China. Huawei officials stated that “Huawei’s success can be directly linked to the company’s unique compensation structure.”<sup>53</sup> Currently, Huawei claims that the Union holds 98.7% of the ESOP shares, and Mr. Ren holds 1.3%. At the Huawei explained that as of December 31, 2011, ESOP has 65,596 participants, which it alleges are all Huawei employees (current and retired), it claims that there are no third parties, including government institutions, holding any ownership-stake in the company.

Questions remained after the Committee staff’s meeting with Huawei officials. Most importantly, the Committee did not receive clear information about how precisely candidates for the Board of Directors are chosen. This is a concern because such individuals are key decision-makers of the company and those whose potential connections to the government are of high concern. According to Huawei officials, the previous Board nominates the individuals for the current Board. But it is not clear how the original Board was established and Huawei refuses to describe how the first Board of Directors and first Supervisory Board were chosen.<sup>54</sup>

As described above, Huawei provided the Committee unsigned, unauthenticated documents purporting to be: (1) Articles of Restricted Phantom Shares; (2) Letter of Undertakings of Restricted Phantom Shares; (3) Notice of Share Issuance and Confirmation Letter; (4) List of Shareholding Employees; (5) Record of Employee Payments and Buyback, (6) Receipts of Employee Share Payments and Buyback; (7) Election Records of the 2010 ESOP Representatives Election (procedures, ballots, results, announcements, etc.); (8) and conclusions of the 2010 ESOP Representatives Meeting. The Committee could not validate the legitimacy of these documents given that Huawei only provided unsigned drafts. Below are summaries of key information from these documents.<sup>55</sup>

*(1) ESOP Restricted Phantom Shares--Summary*

- ESOP Restricted Phantom Shares Article 20 states that target grantees of employee stocks are current employees with high performance.

- Each year, the company determines the numbers of shares an employee can purchase based on job performance. Eligible employees must sign the Confirmation Letter and the Letter of Undertakings and make payments for the shares.
- An employee's stocks can be held only by the employee him/herself, and cannot be transferred or disposed by the employee. When an employee leaves the company (except for those who meet the retirement requirements with minimal eight years of tenure and 45 years old), stocks will be purchased back by the company.
- The current stock price is the net asset value of the stock from the previous year. When an employee purchases more shares or the Union takes shares back, it is based on the current stock price. The dividend amount of each year is based on the performance of the company.

*(2) Articles of Restricted Phantom Shares—*

*a. The Commission*

- The Commission is composed of 51 Representatives and nine alternates, elected by the Active Beneficiaries as organized by the Union with a term of five years.
  - Active beneficiary is defined as an active employee who works at Shenzhen Huawei Investment and Holding Co, Ltd or any of its equity affiliates and participates in the Plan of the Union.
  - In the event there is a vacancy, the Alternate shall take up the vacancy in sequence. The Alternates can attend, but not vote at, all meetings.
  - The Commission reviews and approves restricted phantom share issuance proposals; reviews and approves dividend distribution proposals; reviews and approves reports of the

board of shareholding employees; elects and replaces any member of the board; elects and replaces any member of Supervisory Board; reviews and approves procedures for electing representatives; approves amendments of these articles; reviews and approves the use of the reserve fund; reviews and approves other material matters with respect to restricted phantom share; perform functions as the shareholders of the company, exercises the rights of the shareholder, and develops resolutions regarding material matters such as capital increase, profit distribution, and selection of Directors and Supervisors.

- Meetings of the Commission shall be convened at least once a year, and shall be convened by the Board and presided over by the Chairman of the Board or the Vice Chairman.

*b. The Board*

- The Board is responsible for regular management authority and shall be responsible to the Commission.
- The main functions of the Board are to: prepare restricted phantom share issuance proposal; preparation of the dividends distribution proposal; formulation, approval, and amendment of the detailed rules, processes, and implementation methods with respect to the restricted phantom shares; preparation of the amendments to articles; determination on the detailed proposal as to the use of the Reserve Fund; execution of the resolutions of the Commission; exercise of the specific rights and powers of a shareholder of the Investee Company except for the matters on which a resolution from Commission is required; determination of other matters that shall be determined by the Board.
- The Board consists of 13 directors selected by the Commission; each serves for five years.

- The Board must convene at least once a year; it needs 2/3 present, and resolutions of the meetings shall be approved by at least 1/2 of all Directors.
- The Board may establish a restricted phantom share management committee and other necessary organizations responsible for carrying out and implementing the work assigned by the Board and for detailed matters with respect to the management of the restricted phantom shares, such as evaluation, distribution, and repurchase of the restricted phantom shares as well as management of the account and the Reserve Fund/treasury shares related to restricted phantom shares.

*c. Supervisory Board*

- The Supervisory Board is the organization responsible for supervising the implementation of the shareholder plan with its main functions and powers as follows:
  - supervising the implementation of the resolutions by the Board;
  - making recommendations or inquiries in event of any violation of any law, regulation or these Articles by the Board;
  - making work reports to the Commission; and
  - other regular functions and powers.
- Supervisors may attend Board meetings as non-voting delegate.
- The Supervisory Board shall consist of five Supervisors who shall be elected by the Commission to five year terms; no Director can serve concurrently as a Supervisor.
- Convene at least once a year, need minimum of 2/3 present, resolutions require approval of at least 2/3 of all Supervisors

*d. Validity of Resolutions*



- Before 31 December 2018, Mr. Ren shall have a right to veto the decisions regarding restricted phantom shares and Huawei's material matters (resolutions of the Board, Commission, and Shareholder's Meeting of the Company).
- Starting from 1 January 2013, the confirmed Active Beneficiaries who represent a minimum of 15% of the restricted phantom shares (excluding the restricted phantom shares held by the Restructuring Beneficiaries and the Retained Restricted Phantom Shares) shall have a right to veto the decisions regarding restricted phantom shares and Huawei's material matters (including resolutions of the Board, the Commission, and the Shareholders' Meeting of the Company).
- The relevant resolutions shall take effect in the event that the owner(s) of the right of veto does (do) not exercise the right of veto against the aforementioned resolutions.

*(3) Acquisition of Restricted Phantom Shares*

- The restricted phantom shares of the Union shall be issued to those key employees of the Company who have displayed excellent work performance.
- The Restricted Phantom Share Management Committee shall decide annually whether to issue shares, and the number of shares to be issued, based on the comprehensive evaluation of the work performance of such employee and in accordance with the evaluation rules of the restricted phantom shares. Retired or restructuring beneficiaries are not allowed to purchase new shares.

*(4) Confidentiality and Non-Competition Obligations of the Beneficiaries*

- No Active Beneficiary or Restructuring Beneficiary shall directly or indirectly have a second job in any way, work for any enterprise other than the Company without written consent of the Company or without entering into the relevant agreement with the Company.

\*\*\*\*\*

**ii. Huawei failed to explain its relationships with the Chinese government, and its assertions denying support by the Chinese government are not credible.**

The nature of the modern Chinese economy is relevant for understanding Huawei's connection to the Chinese state. The Chinese government often provides financial backing to industries and companies of strategic importance. Indeed, analysts of the Chinese political economy state that:

Huawei operates in what Beijing explicitly refers to as one of seven “strategic sectors.” Strategic sectors are those considered as core to the national and security interests of the state. In these sectors, the CCP [Chinese Communist Party] ensures that “national champions” dominate through a combination of market protectionism, cheap loans, tax and subsidy programs, and diplomatic support in the case of offshore markets. Indeed, it is not possible to thrive in one of China's strategic sectors without regime largesse and approval.<sup>56</sup>

Similarly, the U.S.-China Commission has explained, with Chinese companies, “the government's role is not always straightforward or disclosed.” Despite some reforms, “much of the Chinese economy remains under the ownership or control of various parts of the Chinese government.”<sup>57</sup> The U.S. China-Commission lists Huawei as a form of enterprise in China that exists in a relatively new market and receives generous government policies to support its development and impose difficulties for foreign competition.<sup>58</sup>

The Committee thus inquired into the precise relationship between the Chinese government and Huawei. During the Committee's meetings with Huawei executives, and during the open hearing on September 13, 2012, Huawei officials consistently denied having any connection to or influence by the Chinese government beyond that which is typical regulation.<sup>59</sup> Specifically, Huawei explained in its written responses to the Committee, that “Huawei maintains normal commercial communication and interaction with relevant government supervisory agencies, including the Ministry of Industry and Information Technology and the Ministry of Commerce.”<sup>60</sup> Huawei claims that it “does not interact with government agencies that are not relevant to its business activities, including the Ministry of National Defense, the Ministry of State Security, and the Central Military Commission.”<sup>61</sup> Huawei, however, did not provide information with which the Committee could evaluate these claims, as Huawei refused to answer the

specific questions of the Committee inquiring about the company's precise mechanisms of interaction with and regulation by these government bodies.

The Committee did not expect Huawei to prove that it has "no ties" to the government. Rather, in light of even experts' lack of certainty about the state-run capitalist system in China, the Committee sought greater understanding of its actual relationship with the Chinese government. The Committee requested that Huawei support and prove its statements about its regulatory interaction by providing details and evidence explaining the nature of this formal interaction. Any company operating in the United States could very easily describe and produce evidence of the federal entities with which it must interact, including which government officials are their main points of contact at those regulatory agencies.

In its written submission in response to the Committee's questions, Huawei simply asserted that it "maintains normal commercial communication and interaction with relevant government supervisory agencies, including the Ministry of Industry and Information Technology and the Ministry of Commerce."<sup>62</sup> Huawei's failure to provide further detailed information explaining how it is formally regulated, controlled, or otherwise managed by the Chinese government undermines the company's repeated assertions that it is not inappropriately influenced by the Chinese government. Huawei appears simply unwilling to provide greater details that would explain its relationships with the Chinese government in a way that would alleviate security concerns.

Similarly, Huawei officials did not provide detailed answers about the backgrounds of *previous* Board Members. Rather, the Committee simply received the same biographies as previously disclosed of current members of the Board of Directors and Supervisory Board.<sup>63</sup> Previous Board Members may have significant ties to the Party, military, or government. And since the previous Board is responsible for nominating the current Board members, this information is important to understanding the historical progression of the company. Because the biographies of the previous members would highlight possible connections to military or intelligence elements of the Chinese government, Huawei's consistent failure to provide this information is alerting.

**iii. Huawei admits that the Chinese Communist Party maintains a Party Committee within the company, but it failed to explain what that Committee does on behalf of the Party or which individuals compose the Committee.**

Huawei's connection to the Chinese Communist Party is a key concern for the Committee because it represents the opportunity for the State to exert its influence over

the decisions and operations of a company seeking to expand into the critical infrastructure in the United States. This concern is founded on the ubiquitous nature of the Chinese Party in the affairs of institutions and entities in China, and the consensus view that the Party exerts pressure on and directs the resources of economic actors in China.<sup>64</sup>

In response to the numerous opportunities to answer questions about its connection to the Party, Huawei stated that the company has no relevant connections. For example, in response to the Committee's written questions about the role of the Party in the company's affairs, Huawei merely stated that it "has no relationship with the Chinese Communist Party in its *business* activities."<sup>65</sup>

Huawei admits, however, that an internal Party Committee exists within Huawei. Huawei simply states that party committees are required by Chinese law to exist in all companies in China.<sup>66</sup> The existence of these Committees is, however, of particular relevance. Huawei states in its defense that all economic institutions in China are required to have a state Party apparatus inside the company. This is not, however, a compelling defense for companies seeking to build critical infrastructure in the United States. Indeed, experts in Chinese political economy agree that it is through these Committees that the Party exerts influence, pressure, and monitoring of corporate activities. In essence, these Committees provide a shadow source of power and influence directing, even in subtle ways, the direction and movement of economic resources in China.<sup>67</sup> It is therefore suspicious that Huawei refuses to discuss or describe that Party Committee's membership. Huawei similarly refuses to explain what decisions of the company are reviewed by the Party Committee, and how individuals are chosen to serve on the Party Committee.

Similarly, Huawei officials did not provide information about Mr. Ren's role or stature in the Party. In his official biography, Mr. Ren admits that he was asked to be a member of the 12<sup>th</sup> National Congress of the Communist Party of China in 1982. The National Congress is the once-in-a-decade forum through which the next leaders of the Chinese state are chosen. The Party members asked to play a role in China's leadership transition are considered key players in the state apparatus.<sup>68</sup> Mr. Ren proudly admits that he was invited to that Congress, but he will not describe his duties. Shortly after being given such a prestigious role, Mr. Ren successfully founded Huawei, though he asserts he did so without any government or Party assistance.<sup>69</sup> Huawei likewise refuses to answer whether Mr. Ren has been invited to subsequent National Congresses or has played any role in Party functions since that time.<sup>70</sup>

From the review of available information, Huawei may have connections and ties to Chinese leadership that it refuses to disclose. In light of Huawei's refusal to discuss details of its acknowledged Chinese Communist Party Committee, the Committee questions the company's ability to be candid about any other possible connections to the government, military, or Chinese Communist Party.

**iv. Huawei's corporate history suggests ties to the Chinese military, and Huawei failed to provide detailed answers to questions about those connections.**

Huawei explained the founding and development of the company by focusing on the life and history of Ren Zhengfei, Huawei's founder. According to Huawei officials, Mr. Ren was a member of the Chinese military's engineering corps as a soldier tasked to establish the Liao Yang Chemical Fiber Factory and was promoted as a Deputy Director, which was a professional role equivalent to a Deputy Regimental Chief, but without military rank.<sup>71</sup> Mr. Ren then retired from the army in 1983 after the engineering corps disbanded, and next worked for a State Owned Enterprise (SOE) following his retirement. According to this account, Mr. Ren was "dissatisfied" with his low salary and career path at the SOE, so in 1987, he established Huawei. Huawei officials did not explain how he was able to leave his employment with a SOE or whether he got agreement of the state to do so. Huawei officials denied that Mr. Ren was a senior member of the military.<sup>72</sup> The Committee's requests for more information about Mr. Ren's military and professional background were unanswered. Huawei refused to describe Mr. Ren's full military background. Huawei refused to state to whom he reported when he was in the military. Huawei refused to answer questions about how he was invited to join the 12<sup>th</sup> National Congress, what duties he performed for the Party, and whether he has been asked to similar state-party matters.

Huawei similarly denied allegations that Ms. Sun Yafang, Chairwoman of Huawei, was previously affiliated with the Ministry of State Security. Mr. Ding responded to Committee questions after the hearing that, to his knowledge, reports about Ms. Yafang in Chinese publications, such as those in *Xinjing Bao*, are erroneous.<sup>73</sup> Mr. Ding did not respond to questions asking about how such publications received such information, or whether Ms. Yafang's previous biography on the Huawei website was erroneous as well. Rather, Mr. Ding simply provided again Ms. Yafang's corporate biography from the Huawei Annual Report 2011.<sup>74</sup>

With respect to Huawei's founders, Huawei cited a Chinese legal requirement that new companies in the economic development zone must have a minimum of five

shareholders and 20,000 RMB registered capital. During meetings with the Committee, Huawei officials claimed that in 1987, Mr. Ren raised 21,000 RMB with personal savings and five other private investors. To the best of the officials' knowledge, none of the five investors had worked with Mr. Ren prior to start-up and one individual has previous affiliation with the government.<sup>75</sup> According to Huawei officials, the five investors never actually worked for Huawei and withdrew their investments several years later.<sup>76</sup>

The Committee struggled to get answers from Huawei on the details of this founding, including how Mr. Ren came to know the initial individual investors, whether his connections to the military were important to the eventual development of the firm, and whether his role in the Party remains a factor in his and his company's success.

- v. The Committee finds that Huawei's failure to provide information about the Chinese government's 1999 investigation of the company for tax fraud exemplifies how it refuses to be transparent; the apparent ease with which Huawei ended the investigation undermines Huawei's assertion that the Chinese government finds Huawei to be a disfavored telecommunications solutions provider in China.**

Huawei officials claimed that after growing in rural areas in China throughout the 1990s, the Chinese government investigated the company at length between 1998-99 for tax fraud.<sup>77</sup> Huawei officials stated that they believed this investigation was politically motivated and performed at the urging of the company's competition – specifically, other telecommunications companies that are also state-owned enterprises. Mr. Ken Hu explained the investigation was a turning point in the history of the company. Specifically, Mr. Hu stated that Huawei's movement to opportunities outside of China was the result of this investigation.<sup>78</sup> Indeed, these officials sought to explain that this episode proves that Huawei was not in fact a “national champion” or otherwise a favored company in China.<sup>79</sup>

Given the obvious importance Huawei placed on this tax-fraud investigation, the Committee's subsequent questions and document requests sought detailed information and further documentary support for its version of events. In particular, the Committee sought information on the conclusion of the Chinese investigation. This information is particularly important to the Committee given the apparent pride displayed by certain Huawei officials in Shenzhen when describing how they successfully used their connections to end the investigation. The ability of these corporate officers to end a politically-motivated investigation suggests that Huawei officials were not as lacking in political power or influence with the government as they suggested.

Despite the importance placed on this event, Huawei failed to address the Committee's questions in its written submission.<sup>80</sup> The company also failed to provide any material that would support Huawei's assertions that the investigation was closed legitimately or without attendant conditions placed on Huawei.<sup>81</sup>

**vi. Huawei failed to explain its relationships with western consulting firms, and any claims that its success is on account of those relationships, rather than support by the Chinese government, are not credible.**

Huawei officials stated that one reason for the company's success was its reliance on the advice of western consulting firms, such as IBM, Accenture, and Price Waterhouse Cooper.<sup>82</sup> Huawei sought to convince the Committee that it was the advice of these companies -- and not support by the Chinese government -- that explains Huawei's miraculous growth in recent years.<sup>83</sup>

Because of the importance Huawei places on the advice given by these consulting firms, the Committee sought greater information and evidence showing that such advice had important effects for the company. The Committee made clear that it did not seek information on the terms of the contractual arrangements with the consulting firms, but rather what information they reviewed from Huawei and what advice was provided. The Committee offered to keep such information confidential to avoid concerns about disclosing proprietary information.

Huawei responded with only a vague description of the advice provided by these companies. Specifically, although "[s]ince 1997, Huawei has relied on western management consulting firms to help improve [its] capabilities, build [its] processes, and develop a comprehensive management system driven by customer requirements," Huawei failed to provide details about how those companies reformed the company other than providing a few sentences mentioning standard business practices, including lead to cash (LTC), integrated product development (IPD), issue to resolution (ITR), and integrated financial services (IFS). Huawei, refused "to provide additional details as to [its] consultancy relationships" citing concerns about proprietary information contained in that advice.<sup>84</sup> The Committee explained that it is most interested in evidence revealing what Huawei did in response to the advice of these firms, and specifically financial or other evidence that supports its position that those changes were responsible for efficiencies, growth, and market success.<sup>85</sup> Huawei could have answered such questions without revealing proprietary information held by these companies.<sup>86</sup> The Committee



was also willing to enter into a confidentiality agreement with all parties, an offer Huawei declined to accept or pursue.<sup>87</sup>

Huawei has made the details of this consulting advice relevant to this investigation by attributing its rapid success to the advice rendered by these consulting firms. It is not then reasonable for Huawei to withhold that information from the Committee so that it could evaluate those claims. If Huawei has within its possession information and documents that would prove that the advice given by these firms was key to Huawei's success, Huawei should provide such information.<sup>88</sup> The Committee was and remains willing to enter into confidentiality agreements with all parties to solve any concerns about the release of proprietary information. Huawei has failed to accept this offer. Its failure to do so is indicative of the lack of cooperation shown throughout this investigation.

**vii. Huawei failed to answer key questions or provide supporting documentation for its claims to be financially independent of the Chinese government.**

As a company of strategic importance to China, Huawei's stature will be reflected in the level of financial support and direction it receives from the Chinese government and Party.<sup>89</sup> One way to review that support and direction provided by the state is through the financing the company receives. Many industry experts and telecommunications companies describe below-market pricing.<sup>90</sup> Thus, the Committee sought more information about Huawei's financing, including its customer financing. Such financial information would also help provide greater understanding about the financial structuring of a firm that remains largely opaque.

During the Committee's hearing, Mr. Ding suggested he did not understand and had no knowledge of the term "national champion," which is often used to describe favored Chinese companies throughout the economic literature on China.<sup>91</sup> The Committee finds that Mr. Ding's suggestion that he does not understand the term is not credible. Huawei itself provided Capitol Hill offices a slide presentation in November 2011, which used the term "national champion" several times.<sup>92</sup> In response to the Committee's questions about use of the term in that document, Huawei did not deny that it used the document and provided the document containing the term.<sup>93</sup> Rather, Huawei stated that the particular slide in the larger document was created by a third party and thus not Huawei's responsibility.<sup>94</sup> The Committee finds that Huawei's knowing use of the document in its discussions with United States elected representatives is sufficient evidence to prove that Huawei does in fact have an understanding of the term. Mr.



Ding's consistent refusal to answer questions about which firms are considered national champions in the Chinese telecommunications sector was obstructionist. In fact, his response to the Committee's question that "Huawei has not paid attention to the meaning of 'national champion' before," is obviously untrue given the company's use of the term in its presentations previously.<sup>95</sup> Moreover, his answers suggest that he did not want to explain how it was that Huawei, the number one telecommunications provider in China, is not a company of strategic importance in China, as recognized by others around the world.

Huawei officials also deny that they have received any special financial incentives or support from the Chinese government.<sup>96</sup> Huawei claimed that the company simply takes advantage of general Chinese banking opportunities, but does not seek to influence or coordinate with banks such as the Chinese Development Bank and the Export-Import Bank, which are both state owned. In previous presentations, Huawei had suggested that it served as an "intermediary and bridge" between the state-backed financial institutions and Huawei customers.<sup>97</sup> Huawei refused, however, to provide more detail about precisely how those lines of credit developed. Huawei also refused to answer specifics about its formal relationships with the Chinese banks, opting to simply answer that it maintains "normal business relations" with the Export-Import Bank of China.<sup>98</sup>

In its presentation to the Committee during the February meeting, Huawei provided a list of the Memoranda of Understanding (MOUs) it claims to have signed with Chinese banks for lines of credit for its customers.<sup>99</sup> Huawei admits that its customers have a US \$100 billion in credit available, yet Huawei asserts that only \$5.867 billion has been drawn in the period between 2005 and 2011. Further, in its written responses, Huawei states that it is a "financing opportunity available to customers, not to Huawei."<sup>100</sup> Yet Huawei explained at the February 23, 2012, meeting with Committee investigators that the goal of the large available credit lines was for China "to appear impressive" and that "Huawei had to participate or would no longer receive loans" from Chinese banks.<sup>101</sup> In response to repeated questions and document requests, Huawei failed to provide further written explanation of the benefits Huawei gains from these financing arrangements, and it did not provide internal documents or any auditable information that would substantiate its claims about the scope and processes of this financing.

Similarly, Huawei refused to describe the details of its relationships with Chinese state-owned banks. For example, in Mr. Ding's statement for the record, he explained that Huawei receives loans from ten Chinese banks. But Mr. Ding refused to answer how many of those ten banking institutions in China are state-owned.<sup>102</sup> As described in the

previous section, Huawei also refused to provide “additional details as to [its] consultancy relationships” because it would “include highly sensitive proprietary information” governed by non-disclosure agreements.<sup>103</sup> In response to Committee questions about Huawei’s success and whether it was owing to the company’s support from the Chinese government, Huawei represented to the Committee that its relationships with and advice received from these companies are the source of the company’s global success.<sup>104</sup> Because Huawei refuses to provide details on those relationships and advice rendered, the Committee cannot evaluate its claim that any of its success is due to these relationships. Accordingly, the Committee discounts the role played by these consulting companies, and continues to find it likely that Huawei has substantially benefited from the support of the Chinese government.

In sum, Huawei admits that its customers receive billions of dollars in support from Chinese state-owned banks and that it has received favorable loans from Chinese banks for years. Huawei refuses to provide answers to direct questions about how this support was secured, nor does it provide internal documentation or auditable financial records to evaluate its claims that the terms of these agreements comply with standard practice and international trade agreements. The Committee is equally concerned with statements by company leaders that undermine the Committee’s confidence in the financial information the company has provided. For example, in a June 2007 speech to Huawei employees in the United Kingdom, Mr. Ren stated that he appreciated the subsidiary’s attempt to create financial statements, “whether the data is accurate or not.”<sup>105</sup> Based on available information, the Committee finds that Huawei receives substantial support from the Chinese government and Chinese state-owned banks, which is at least partially responsible for its position in the global marketplace.

**viii. Huawei failed to provide sufficient details or supporting documentation on its operations, financing, and management in the United States; evidence undermines its claims of being a completely independent subsidiary of Huawei’s parent company in Shenzhen, China.**

To understand the United States’ current vulnerability to supply-chain threats posed by Huawei equipment, it is necessary to know the extent to which Huawei’s equipment is already placed in U.S. infrastructure. Because the U.S. telecommunications infrastructure is largely built and owned by the private sector, the U.S. government does not have the full picture of what is contained within it and thus is not yet fully informed to develop policies to protect that critical infrastructure from vulnerabilities.<sup>106</sup>

The Committee thus asked Huawei for information on its contracts for products and services within the United States. Understanding the extent to which Huawei equipment already exists in the United States is necessary to evaluate the present risk to the country, as well as to confirm Huawei's statements about the size and scope of its operations in the United States. Unfortunately, Huawei failed to provide specific information about its dealings within the United States. Huawei did provide the Committee a list of Huawei's major customers in the United States: Cricket Communications; Clearwire; Cox TMI Wireless, Hibernia Atlantic, Level 3/BTW Equipment, Suddenlink; Comcast and Bend Broadband. Huawei, however, did not provide information on the size and scope of its operations, which elements of the infrastructure it is providing, and where these operations are located.<sup>107</sup>

The information requested by the Committee about Huawei's contracts in the United States is also necessary to evaluate Huawei's claims that they comply with all laws and trade obligations regarding the price of their products and services.<sup>108</sup> To date, Huawei has failed to provide any information to validate its claims that the prices of Huawei's products are based on market conditions. Huawei's refusal to answer clearly or provide documents supporting its claims necessitates the Committee finding that Huawei's defense is not credible. The Committee considers it possible that Huawei receives substantial support from the Chinese government such that Huawei can market at least some of its products in the United States below the costs of production.

Similarly, the extent to which Huawei's subsidiaries in the United States operate independently of the parent company in Shenzhen remains unclear. Such information is important, because any connections between the parent company in China to the Chinese government might affect the operations and behavior of the company in the United States. The Committee therefore requested information on the extent to which Huawei USA's decisions are controlled, influenced, or reviewed by the parent company.

Huawei explained that the first US-based Huawei subsidiary was established in the United States in 2005 with headquarters in Plano, Texas. Huawei stated that the parent company does not require approval for individual contracts in the United States.<sup>109</sup> Rather, it stated that the Board of Directors in China does set general terms for operations in the United States, and the parent company can help mobilize resources and set strategy should the subsidiary need it. The Committee has heard from several former Huawei employees in the United States who dispute Huawei's explanation of its business model. Sources from around the United States have provided numerous specific instances of business decisions in the United States requiring approval by the parent company in China. In one instance, an individual with first-hand knowledge explained that senior

level executives in the United States could not sign a contract for cyber-security services in the United States without approval in China. In fact, in one instance, a contract previously signed by a U.S.-based senior official at Huawei was repudiated by the parent company.<sup>110</sup> These employees provided documentary evidence, including internal memoranda and emails, discussing corporate policy from China. This description of Huawei's US subsidiaries also comports with reports about the ties between other Huawei subsidiaries and the parent company in China.<sup>111</sup>

To resolve this conflict, the Committee sought more information through its written questions to understand the precise mechanisms through which the Huawei parent company in Shenzhen controls Huawei's strategy for entry and growth into the United States market. Concerns that Beijing's support to Huawei could impact the U.S. market were heightened by Huawei officials' statements to Committee staff that Huawei USA is given general guidance and "resources" from the parent company if needed.<sup>112</sup> In its written response, however, Huawei failed to answer the Committee's detailed questions or provide any further information about the level of coordination between Huawei USA and the parent company.<sup>113</sup>

The information and material provided by Huawei employees with first-hand access coupled with Huawei's failure to provide detailed, internal information, undermines Huawei's claims. For these reasons, the Committee does not find credible Huawei's claims that its U.S. subsidiaries operate independently of the Huawei headquarters in Shenzhen, China.

**ix. Evidence shows that Huawei exhibits a pattern of disregard for the intellectual property rights of other entities and companies in the United States.**

Huawei's ability to protect intellectual property rights is an important indicator of the company's ability to abide by the laws of the United States. Thus, the Committee sought greater information on Huawei's history of IP protection.

The Committee has reason to believe that Huawei is careless with its compliance with intellectual property protections. Investigators heard from numerous sources that Huawei has a checkered history when it comes to protecting the intellectual property of other entities.<sup>114</sup> Specifically, several former employees of Huawei said it is known to purposely use the patented material of other firms. First-hand accounts of former employees suggest that Huawei does not appropriately purchase software applications for use by its employees.<sup>115</sup> Similarly, the Committee heard from industry experts that

Huawei has purposely used and marketed patented products of other companies.<sup>116</sup> Finally, the Committee is in receipt of a Huawei slide presentation that was provided to Capitol Hill offices that itself violates copyright obligations by knowingly using proprietary material from an outside, nonaffiliated consulting firm.<sup>117</sup>

Huawei officials consistently denied ever infringing other companies' intellectual property rights. Even with respect to the litigation with Cisco, in which Huawei agreed to remove certain products from the marketplace, Huawei asserts that it had not violated Cisco's interests.<sup>118</sup> Rather, Huawei suggested that the expert's review in that case of their equipment found no infringement of Cisco patents.<sup>119</sup>

Huawei's defense is not credible. First, with respect to the Cisco litigation, Huawei's statements do not comport with statements made by Huawei officials at the time of the lawsuit acknowledging that the company will remove infringing equipment.<sup>120</sup> Second, the Cisco settlement itself required Huawei to "update and change all of the products that have been accused of violating copyright or intellectual property rights."<sup>121</sup> Finally, during the hearing on September 13, 2012, Charles Ding refused to answer the clear question of whether Cisco code had ever been in Huawei equipment.<sup>122</sup> Mr. Ding's obstructionism during the hearing undermines Huawei's claims that it did not violate Cisco's patented material.

The Committee finds that Huawei's denials of intellectual property infringement were not credible or supported by available evidence. Because Huawei failed to produce any internal documents or support for its defenses, the Committee finds that Huawei has exhibited a pattern of, at the very least, reckless disregard for the intellectual property rights of other entities.

**x. Huawei failed to provide details of its operations in Iran, though it denied doing business with the government of Iran, and did not provide evidence to support its claims that it complies with all international sanctions or U.S. export laws.**

Huawei's ability to comply with international sanctions regimes and U.S. export control regulations is an important indicator of the company's ability to comply with international standards of corporate behavior and to abide by U.S. laws irrespective of China's influence or interests. Public reporting raises questions about the company's compliance with these laws.

In response to the Committee's questions, Huawei officials provided only vague assertions about their commitment to all laws. Specifically, Huawei asserted that the company seeks to abide by all legal obligations and has transformed its business practices with the help of outside consultants to better monitor its actions to ensure compliance with international sanctions regimes. To highlight the lack of influence of the Chinese regime over its decisions, Huawei indicated the Chinese Embassy in Iran was surprised by Huawei's decision to limit its business dealings in Iran. Huawei also stated that it does not allow its employees to participate in cyber activities, such as population monitoring, anywhere in Iran.

Huawei has refused, however, to answer detailed questions about its operations in Iran or other sanctioned countries. In its written submission to the Committee, Huawei again reiterated that it limited its future business in Iran because of the enhanced sanctions and an inability to collect payment for operations in Iran. Huawei highlights, though, that "Huawei respects the contracts signed with [its] customers" and thus will not end current contracts in Iran.<sup>123</sup> Huawei claims to "observe laws and regulations of the UN, the U.S., the E.U. and other countries and regions on sanctions."<sup>124</sup> It also claims to have instituted an internal program on trade compliance representing best practices to manage these issues.<sup>125</sup> But Huawei refused to provide any internal documents relating to its decision to scale-back operations in Iran or otherwise ensure compliance with U.S. laws.

Such documents would have validated Huawei's claims that the decision was based on legal compliance requirements and not influenced by any pressure by the Chinese government.

**xi. Huawei refused to provide details on its R&D programs, and other documents undermine its claim that Huawei provides no R&D for the Chinese military or intelligence services.**

To understand the extent to which Huawei performs R&D activity on behalf of the Chinese military or intelligence services, the Committee asked for information about its activities on behalf of the Chinese government or military. Specifically, the Committee requested information on the technologies, equipment, or capabilities that the funding or grants by the Chinese government was supporting. In its written submission to the Committee, Huawei failed to provide responsive answers to the Committee's questions about the specifics of government-backed R&D activities.<sup>126</sup> Rather, Huawei simply asserted that it only bid on R&D projects open to the rest of the industry.<sup>127</sup>

Huawei similarly claimed in its meetings with the Committee that it does not provide special services to the Chinese military or state security services.<sup>128</sup>

In its answers to the Committee's questions after the hearing, Huawei again simply asserted that it "has never managed any of the PLA's networks" and "has never been financed by the Chinese government for R&D projects for military systems." Huawei did admit, however, that it develops "transport network products, data products, videoconferencing products, and all centers, and voice over IP (VoIP) products" for the Chinese military "accounting for .1% of Huawei's total sales."<sup>129</sup> Huawei also claimed, however, that it "develops, researches, and manufactures communications equipment for civilian purposes only."<sup>130</sup>

The Committee also received internal Huawei documentation from former Huawei employees showing that Huawei provides special network services to an entity the employee believes to be an elite cyber-warfare unit within the PLA.<sup>131</sup> The documents appear authentic and official Huawei material, and the former employee stated that he received the material as a Huawei employee.<sup>132</sup> These documents suggest once again that Huawei officials may not have been forthcoming when describing the company's R&D or other activities on behalf of the PLA.

The Committee finds that Huawei's statements about its sales to the Chinese military are inherently contradictory. The Committee also finds that Huawei's failure to respond fully to questions about the details of its R&D activities, coupled with its admission that it provides products for the Chinese military and documents received from employees, undermine the credibility of its assertion that it does not perform R&D activities for the Chinese government or military.

**xii. Former and current Huawei employees provided evidence of a pattern and practice of potentially illegal behavior by Huawei officials.**

During the course of the investigation, several former and current Huawei employees came forward to provide statements and allegations about Huawei's activities in the United States. Given the sensitivities involved, and to protect these witnesses from retaliation or dismissal, the Committee has decided to keep the identities of these individuals confidential. The Committee has received multiple, credible reports from these individuals of several potential violations by Huawei officials. Those allegations include:



- Immigration violations;
- Bribery and corruption;
- Discriminatory behavior; and
- Copyright infringement.

Specifically, the Committee heard from numerous employees that Huawei employees visiting from China on tourist or conference visas are actually working full-time at Huawei facilities, in violation of U.S. immigration law. Similarly, Huawei employees provided credible evidence that individuals coming to the United States on particular visas, for example, for jobs requiring engineering expertise were not in fact employed by Huawei as engineers. These and other alleged violations of immigration law will be referred to the Department of Homeland Security for review and potential investigation.

Second, employees have alleged instances fraud and bribery when seeking contracts in the United States.<sup>133</sup> Those allegations will be referred to the Justice Department for further review and potential investigation.

Third, employees with whom the Committee spoke discussed allegations of widespread discriminatory behavior by Huawei officials. These individuals assert that it is very difficult if not impossible for any non-Chinese national to be promoted in Huawei offices in the United States. Further, these employees assert that non-Chinese nationals are often laid-off only to be replaced by individuals on short-term visas from China.<sup>134</sup> These allegations will be referred to the appropriate agencies in the Executive Branch to review and consider.

Finally, the Committee heard from former Huawei employees that may constitute a pattern and practice of Huawei using pirated software in its United States facilities. As previously described, the Committee received information with Huawei's logo that knowingly and admittedly violated another firm's copyrighted material.<sup>135</sup> The Committee thus finds that Huawei has exhibited a careless disregard for the copyrighted material of other entities. As there may indeed be credibility to these employee allegations, the Committee will also refer these claims to the Justice Department for investigation.

**B. ZTE failed to answer key questions or provide supporting documentation supporting its assertions, arguing that answering the Committee's**



**requests about its internal corporate activities would leave the company criminally liable under China's states-secrets laws.**

ZTE sought to appear cooperative and timely with its submissions to the Committee throughout the investigation. ZTE consistently refused, however, to provide specific answers to specific questions, nor did the company provide internal documentation that would substantiate its many claims. As with Huawei, the Committee focused its review of ZTE on the company's ties to the Chinese state, as well as the company's history, management, financing, R&D, and corporate structure. The Committee did not receive detailed answers on a number of topics described below. ZTE did not describe its formal interactions with the Chinese government. It did not provide financial information beyond that which is publicly available. It did not discuss the formal role of the ZTE Communist Party Committee and only recently provided any information on the individuals on the Committee. The Committee did not receive details on ZTE's operations and activities in Iran and other sanctioned countries. Finally, ZTE refused to provide detailed information on its operations and activities in the United States.

Importantly as well, ZTE argued at great length that it could not provide internal documentation or many answers to Committee questions given fear that the company would be in violation of China's state-secrets laws and thus subject ZTE officials to criminal prosecution in China.<sup>136</sup> In fact, ZTE refused even to provide the slides shown to the Committee staff during the meeting in April, 2012, for fear that they might be covered by state secrets. To the extent ZTE cannot provide detailed and supported answers to the Committee because China's laws treat such information important to the security of the Chinese regime, the Committee's core concern that ZTE's presence in the U.S. infrastructure represents a national-security concern is enhanced.

The Committee notes that ZTE's many written submissions were never numbered to align with the Committee's specific questions and document requests, as would be typical with formal legal processes. The Committee believes that, through this method, ZTE sought to avoid being candid and obvious about which questions it refused to answer. Moreover, ZTE's answers were often repetitive, lacking in documentary or other evidentiary support, or otherwise incomplete.

The Committee also notes that ZTE did not simply deny all national-security concerns arising from the global telecommunications supply chain. ZTE has advocated for a solution – one based on a trusted delivery model – in which approved “independent third-party assessors” transfer “hardware, software, firmware, and other structural elements in the equipment to the assessor.”<sup>137</sup> Such a model, as advocated by ZTE,

would include among other things, a “thorough review and analysis of software codes,” “vulnerability scans and penetration test,” “review of hardware design and audit of schematic system diagram,” “physical facility review and independent comprehensive audit of vendor’s manufacturing, warehousing, processing, and delivery operations,” “periodic assessments.”

ZTE suggests that a model, as previously proposed by Huawei and other companies, and similar in some respects to that introduced in United Kingdom, be implemented across the spectrum for telecommunications equipment providers. As discussed above, the Committee remains concerned that, although mitigation measures can be of some assistance, this model fails to appreciate the nature of telecommunications equipment.

**i. ZTE did not alleviate Committee concerns about the control of Chinese state-owned enterprises in ZTE’s business decisions and operations.**

As with Huawei, the Committee is concerned with the influence of the Chinese state in ZTE’s operations. Such access or influence would provide a ready means for the Chinese government to exploit the telecommunications infrastructure containing ZTE equipment for its own purposes. To evaluate the ties to the Chinese state, the Committee focused on the company’s history, structure, and management. Many commentators have noted that ZTE’s founding included significant investment and involvement by Chinese state-owned enterprises, and thus the Committee sought to unpack the current operations and ownership structure with the hope of understanding whether there are remaining ties to the Chinese state.

ZTE describes itself as a global provider of telecommunications equipment and network solutions across 140 countries. Founded in 1985, ZTE states that its 2011 revenue led the industry with a 24% increase to \$13.7 billion; its overseas operating revenue grew 30% to U.S. \$7.42 billion during the period, accounting for 54.2% of overall operating revenue.<sup>138</sup> ZTE markets itself by explaining that its systems and equipment have been used by top operators in markets around the world. Importantly, ZTE also highlighted in its 2011 Annual Report that China’s 12<sup>th</sup> five-year national plan has significantly contributed to ZTE’s recent domestic success.<sup>139</sup>

During the interviews with ZTE officials in April and May 2012, ZTE officials stressed that ZTE is a publicly traded company, having been listed on the Shenzhen stock exchange in 1997, and the Hong Kong stock exchange in 2004. ZTE contends that it did not begin with government assistance, either with technology transfers or financial

assistance. Rather, ZTE stated that the Chinese government became a shareholder during the 1997 public offering. ZTE has also asserted that the state-owned-enterprise shareholders have no influence on strategic direction of the company.<sup>140</sup> ZTE officials often contrasted themselves with Huawei, though often did not mention Huawei by name. In particular, officials suggested that Huawei is ZTE's main competitor, but often stated that ZTE is more transparent since it is a publicly traded company.

These officials often relied on this public listing to claim that ZTE finances are transparent and comply with both Chinese and Hong Kong regulations regarding financial disclosures. The officials often simply referred to the fact that they have annual reports that detail information requested, such as amount and extent of government loans, subsidies, and credits. ZTE refused, however, to explain whether it would be willing to meet the reporting and transparency requirements of a western stock exchange such as the New York Stock Exchange.<sup>141</sup> As with Huawei, when the Committee sought more detailed answers from ZTE on its interactions with key government agencies, ZTE refused to answer.

The history and structure of ZTE, as admitted by the company in its submissions to the Committee, reveal a company that has current and historical ties to the Chinese government and key military research institutes. In response to questioning, the ZTE officials first discounted and seemingly contradicted their own public statements, which suggest that ZTE formed originally from the Ministry of Aerospace, a government agency. In fact, exhibits displayed during the meeting in Shenzhen highlighted an early collaboration between ZTE and the government-run No. 691 Factory, and other state-owned enterprises. ZTE refused to provide the Committee copies of the slides presented during this meeting.

ZTE officials instead suggested that Mr. Hou Weigui founded ZTE in 1985 with five other "pioneer" engineers. Although they had all previously worked for state owned enterprises, ZTE officials insisted that the formation of ZTE did not arise from any relationship with the government. The company's written submission to the Committee admits that the company had an early connection to No. 691 Factory, which was established by the Chinese government.<sup>142</sup> As described by ZTE, No. 691 Factory is now known as Xi'an Microelectronics Company, and is a subsidiary of China Aerospace Electronics Technology Research Institute, a state-owned research institute. In its submission, ZTE admits that Xi'an Microelectronics owns 34% of Zhongxingxin, a shareholder of ZTE.<sup>143</sup> ZTE's evolution from research entities with connections to the Chinese government and military highlight the nature of the information-technology (IT) sector in China. In fact, taking as true ZTE's submission of its history and ownership,

ZTE's evolution confirms the suspicions of analysts who study the IT sector in China and describe it as a hybrid serving both commercial and military needs.<sup>144</sup>

In 1997, ZTE was publicly listed for the first time on the Shenzhen stock exchange. ZTE executives claim that it was at this point that other state owned enterprises began investing in ZTE.

Currently, 30% of ZTE is owned by Zhongxingxin group and the remaining 70% is held by dispersed public shareholders. The Committee is particularly interested in whether the 30% ownership by Zhongxingxin constitutes a controlling interest or otherwise provides the state owned enterprises an opportunity to exert influence over the company. This question is particularly relevant because two state owned enterprises own 51% of Zhongxingxin. ZTE executives stressed that the public ownership of ZTE is increasing as Zhongxingxin sells its shares (for example, in 2004, Zhongxingxin owned 44% of ZTE, and now Zhongxingxin holds only 30%). In ZTE's July 3 submission to the Committee, ZTE states that "[v]ery few knowledgeable individuals in China would characterize ZTE as a state-owned entity (SOE) or a government-controlled company."<sup>145</sup> But the Committee specifically asked how it is that ZTE remains accountable to its shareholders and not influenced or controlled by its largest shareholder given this ownership structure. In its submission to the Committee, ZTE admits that a 30% share is the point at which Hong Kong and Chinese law considers the holder to be a "controlling shareholder."<sup>146</sup> ZTE simply stated that the company's fiduciary duty to the numerous shareholders means that the controlling shareholder does not in fact exert much actual control over the company.<sup>147</sup> ZTE does not explain in more detail how the Board members, five of whom are chosen by state-owned enterprises, and some of whom are acknowledged members of the Chinese Communist Party and members of ZTE's internal Communist Party Committee, would not exert any influence over the decisions of the company.

Zhongxingxin, ZTE's largest shareholder is owned in part by two state-owned enterprises, Xi'an Microelectronics and Aerospace Guangyu, both of which not only have ownership ties to the Chinese government, but also allegedly partake in sensitive technological research and development for the Chinese government and military. ZTE failed to address the Committee's questions seeking detailed information on the history and mission of these two companies. ZTE also failed to answer questions about these companies' relationship to key leaders within ZTE, specifically Mr. Weigu Hou, and ZTE's other major shareholder, Zhongxing WXT.

Because ZTE failed to answer key questions about its history and the connections to government institutions, the Committee cannot trust that it is free of state influence, particularly through its major shareholders and Board members.

**ii. ZTE maintains a Chinese Party Committee within the company, and has not fully clarified how that Committee functions, who chooses its members, and what relationship it has with the larger Chinese Communist Party.**

As with Huawei, ZTE's connection to the Chinese Communist Party is a key concern for the Committee. Such a connection offers the Party the opportunity to influence the decisions and operations of a company seeking to expand into the critical infrastructure in the United States. As described previously, the modern Chinese state-capitalistic economy is largely influenced if not controlled by the Party, in large part through the party committees that exist within individual firms.

During interviews with ZTE officials, ZTE refused to answer whether the executives or board members are members of the Chinese Communist Party. ZTE first downplayed the existence of the Party Committee within ZTE, and company representatives were unable to answer whether any members of the Board were also members of the state Party. Subsequently, in response to continued Committee questions, ZTE acknowledged that it does, in fact, contain an internal Committee Party, which ZTE suggests is required by the laws of China.<sup>148</sup> In response to the Committee's written questions, ZTE again refused, however, to provide information about the names and duties of the Party Committee members. At the September 13, 2012, hearing, Mr. Zhu attested under oath that ZTE would provide the names of those individuals on the Party Committee.<sup>149</sup>

In response to questions posed at the September 13, 2012, hearing ZTE did provide the Committee a list of 19 individuals who serve on the Communist Party Committee within ZTE. At least two of those individuals appear to be on the ZTE Board of Directors. Other individuals are major shareholders in ZTE entities. ZTE has requested and the Committee has agreed to keep the names of these individuals out of the public domain. ZTE discounts the influence of that these individuals may have over the company. The company asked that the Committee not release the names of the individuals for fear that the company or the individuals might face retaliation by the Chinese government or Communist Party. The Committee has decided to keep the names of those members out of this public report, but the company's concern with the potential retaliatory measures it faces by the government for simply providing the

Committee the names of an internal ZTE body highlights why this Committee remains very concerned that the Chinese state is, or could be, responsible for the actions of the company. China clearly seeks to maintain deep ties into and secrecy about its role in economic actors in China. The control Chinese government maintains over the company's actions and level of transparency is of particular concern when that company seeks to build critical U.S. infrastructure.

ZTE also did not fully explain the function of the Party Committee. Instead, ZTE simply states that the Party Committee is controlled by company management. This assertion is contradicted by ZTE's own statement that ZTE executives and board members actually are members of the [Chinese Communist Party] and delimit its activities.<sup>150</sup> To the extent these executives and Board Members have obligations to both the company's shareholders and the State through the Communist Party, there is an inherent conflict of interest in their duties, and this statement provides confirmation that the Party likely does in fact have influence and input into the business affairs of the company through these individuals.

The affidavit by the independent director, Timothy Steinert, seeks to allay any concerns of influence by the government or Party by stating that:

In my experience and to my knowledge, no member of ZTE's Board of Directors has raised for consideration an interest on behalf of the Chinese Government, the People's Liberation Army or the Chinese Communist Party.<sup>151</sup>

This statement does not resolve the Committee's concerns. First, there is a range of operational and strategic decisions made on a daily basis within companies that are not decided by or reviewed by the Board. Mr. Steinert's affidavit says nothing about the role of the Party Committee in those decisions prior to their reaching the Board, or for decisions that do not reach the Board at all. Second, the Party's influence through ZTE's Party Committee may not be facially obvious in the decision documents appearing for review to the Board. Since at least two members of the Board are also members of the Chinese State Party, it is impossible to know whether the votes of the Board are conducted without influence by the Chinese Communist Party. When considering ZTE's activities or voting on certain measures, those Board members need not cite the Party to be acting on the state's behalf or in pursuit of the state's interests. For these reasons, the Committee finds unpersuasive ZTE's claims that Mr. Steinert's affidavit "confirms that ZTE business decision making is not influence by the government or Party considerations"<sup>152</sup>

ZTE recently suggested that the Party Committee “performs only ceremonial and social functions.” For six months, the Committee has asked ZTE about the role of the Party Committee, but only at the final hour, did it provide any response at all. Without further information and specifics about the role and influence of the Party Committee in the operations of the company, the Committee simply cannot allay the concerns about the internal party apparatus existing within a company seeking to build U.S. critical infrastructure.

**iii. ZTE failed to disclose information about its activities in the United States.**

ZTE discussed its extensive presence in 140 countries, but significantly downplayed any potential threats to the U.S., by suggesting that 95% of its U.S. sales are from handsets. ZTE officials highlighted that they have five R&D centers in the U.S. employing about 300 people. ZTE officials attempted to suggest that the company’s presence in rural infrastructure and networks was to assist the U.S. effort with its rural broadband plans. Committee staff questioned this logic, and ZTE officials admitted that ZTE’s role in these projects were not for charity or public service, as they had initially suggested, but to get a “foothold” in the country and learn the technology in the United States. ZTE officials even admitted that they are willing to provide this equipment to the U.S. below cost in order to learn the U.S. market. Specifically, during the Committee’s meeting with ZTE officials in Shenzhen, Mr. Zhu stated that the company was willing to lose money on projects in the United States to get a foothold in the United States and to understand the technology and standards in the United States.

ZTE’s description of its current U.S. activity is simply a picture at a particular point in time. The Committee could not confirm the extent of the company’s contracts or access to the United States market absent responses to the Committee’s document requests.<sup>153</sup> Despite numerous requests, ZTE has not provided detailed information on infrastructure projects in the United States.<sup>154</sup> ZTE also failed to answer follow-up questions that would explain whether ZTE purposely bids on projects below cost and how the company is able to sustain these losses. Further, at the HPSCI hearing on September 13, Mr. Zhu reversed his previous answers and refused to acknowledge that ZTE ever bids below cost for projects in the United States.<sup>155</sup>

**iv. ZTE failed to provide any answers or evidence about its compliance with intellectual property or U.S. export-control laws.**

The protection of intellectual property and compliance with United States export control laws are a core concern for U.S. interests. The ability of a company to comply



with these laws provide a useful test of that company's ability to follow international codes of business conduct and remain free of undue state influence.

Representatives of the company consistently declined to comment on recent media reports that ZTE had sold export-controlled items to Iran.<sup>156</sup> At the hearing on September 13, 2012, ZTE acknowledged that it is performing an internal review to determine if the company destroyed any documents or other evidence related to its activities in Iran.<sup>157</sup> Mr. Zhu provided no information that could allow the Committee to evaluate the extent of those activities, their compliance with U.S. laws, or management's involvement in the potential destruction of documents and evidence. ZTE did not answer in specific written questions from the Committee asking why it sought to limit its Iranian business activities; whether ZTE will honor its current contracts in Iran; or whether those contracts include training or maintenance of surveillance equipment. Further, ZTE refused to answer questions about what products ZTE resold in Iran. ZTE also refused to provide any documents on its activities in Iran.

**v. ZTE failed to provide clear answers to Committee questions about its R&D activities, particularly as they relate to any military or government projects.**

Given ZTE's background, the Committee was interested in ZTE's R&D activities, and particularly its R&D activities with or on behalf of the Chinese military or security services. This information would help the Committee evaluate whether a company seeking to build critical infrastructure in the United States could also be working with the Chinese government on R&D projects with the purpose of finding or exploiting vulnerabilities in those systems.

ZTE's known connections to Chinese government-related research institutes are of particular interest. For example, ZTE acknowledges that one of its primary shareholders, Zhongxingxin, is owned in part by Xi'an Microelectronics, a subsidiary of China Aerospace Electronics Technology Research Institute, a state-owned research institute.<sup>158</sup> Another 17% of Zhongxingxin is held by Aerospace Guangyu, a subsidiary of a state-owned enterprise whose business includes production of, among other things, aerospace technology products.<sup>159</sup> ZTE failed to answer questions from the Committee seeking further details about the range of products these research institute have produced on the Chinese government so the committee could not evaluate whether those technologies were produced for military or intelligence purposes.<sup>160</sup>

These ties to Chinese government research institutes and production companies, the Committee sought more information on the details of ZTE's R&D activities, and



particularly its potential work on behalf of the government, military, or security services. ZTE was proud to explain that it had established 18 state-of-the-art R&D centers throughout China, France, and India, and to employ over 30,000 research professionals. ZTE further claims that 10% of the company's annual revenue is invested in R&D. ZTE failed, however, to answer Committee questions about the technologies it may create or sell to the Chinese government and military. During the Committee's April 12, 2012 meeting with company officials, Mr. Steinert, the independent board member, stated that, ZTE's work on behalf of the Chinese telecommunications providers that happen to be state-owned enterprises does not suggest that ZTE does work on behalf of the military or intelligence services. When providing written answers ZTE refused to provide clear answers about the nature and extent of any work it does on behalf of the Chinese military or security services. Rather, ZTE states that "[t]he funding ZTE has received from government or consortia during the past several years is indistinguishable from similar funding available throughout the world in companies engaged in R&D through normal procurement processes."<sup>161</sup>

To the extent ZTE's R&D activities are simply in response to standard government procurement processes, the Committee does not understand why it refuses to answer direct questions about the details of those projects. For this reason, the Committee cannot allay concerns that ZTE is aligned with Chinese military and intelligence activities or research institutes.

## **Conclusion and Recommendations**

The Committee launched this investigation to seek answers to some persistent questions about the Chinese telecommunications companies Huawei and ZTE and their ties to the Chinese government. Throughout the months-long investigation, both Huawei and ZTE sought to describe, in different terms, why neither company is a threat to U.S. national-security interests. Unfortunately, neither ZTE nor Huawei have cooperated fully with the investigation, and both companies have failed to provide documents or other evidence that would substantiate their claims or lend support for their narratives.

Huawei, in particular, provided evasive, nonresponsive, or incomplete answers to questions at the heart of the security issues posed. The failure of these companies to provide responsive answers about their relationships with and support by the Chinese government provides further doubt as to their ability to abide by international rules.

## **Recommendations**

Based on this investigation, the Committee provides the following recommendations:

**Recommendation 1:** The United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies.

- The United States Intelligence Community (IC) must remain vigilant and focused on this threat. The IC should actively seek to keep cleared private sector actors as informed of the threat as possible.
- The Committee on Foreign Investment in the United States (CFIUS) must block acquisitions, takeovers, or mergers involving Huawei and ZTE given the threat to U.S. national security interests. Legislative proposals seeking to expand CFIUS to include purchasing agreements should receive thorough consideration by relevant Congressional committees.
- U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including in component parts. Similarly, government contractors – particularly those working on contracts for sensitive U.S. programs – should exclude ZTE or Huawei equipment in their systems.

**Recommendation 2:** Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.

**Recommendation 3:** Committees of jurisdiction within the U.S. Congress and enforcement agencies within the Executive Branch should investigate the unfair trade practices of the Chinese telecommunications sector, paying particular attention to China's continued financial support for key companies.

**Recommendation 4:** Chinese companies should quickly become more open and transparent, including listing on western stock exchange with advanced transparency requirements, offering more consistent review by independent third-party evaluators of their financial information and cyber-security processes, complying with U.S. legal standards of information and evidentiary production, and obeying all intellectual-property

laws and standards. Huawei, in particular, must become more transparent and responsive to U.S. legal obligations.

**Recommendation 5:** Committees of jurisdiction in the U.S. Congress should consider potential legislation to better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure. Such legislation could include increasing information sharing among private sector entities, and an expanded role for the CFIUS process to include purchasing agreements.

---

<sup>1</sup> Ken Hu, “Huawei Open Letter.” <http://online.wsj.com/public/resources/documents/Huawei20110205.pdf> (accessed August 2, 2012).

<sup>2</sup> Huawei’s letter was issued in February, 2011, when the Committee on Foreign Investment in the United States (CFIUS) issued a recommendation that Huawei voluntarily divest assets it received in a 2010 deal with 3Leaf, a United States company that developed advanced computer technologies. Shayndi Raice, “Panel Poised to Recommend Against Huawei Deal,” *Wall Street Journal*, February, 11, 2011. <http://www.wsj.com/article/SB20001424052748704629004576136340771329706.html> (accessed August 2, 2012)

<sup>3</sup> A classified annex to this report provides both classified information relevant to the discussion, as well as information about the resources and priorities of the IC.

<sup>4</sup> Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies,” *IEEE Control Systems Magazine*, December 2001.

<sup>5</sup> “The former National Counterintelligence Executive, Mr. Robert Bryant, recently noted that, ‘Insider threats remain the top counterintelligence challenge to our community.’ An insider threat arises when a person with authorized access to U.S. Government resources, to include personnel, facilities, information, equipment, networks, and systems, uses that access to harm the security of the United States. Malicious insiders can inflict incalculable damage. They enable the enemy to plant boots behind our lines and can compromise our nation’s most important endeavors. Over the past century, the most damaging U.S. counterintelligence failures were perpetrated by a trusted insider with ulterior motives.” <http://www.ncix.gov/issues/ithreat/index.php>

<sup>6</sup> FBI, *Intelligence Bulletin*, “Supply Chain Poisoning: A Threat to the Integrity of Trusted Software and Hardware,” June 27, 2011: 1.

<sup>7</sup> Office of National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage*, “Foreign Spies Stealing US Economic Secrets in Cyberspace.” (October 2011, Washington, DC: 1.)

<sup>8</sup> United States Congress, *2011 Annual Report of U.S.-China Economic and Security Review*. (2011, Washington DC: 59.)

<sup>9</sup> National Institute of Standards and Technology, *Draft NISTIR 7622*, “Piloting Supply Chain Risk Management for Federal Information Systems,” June 2010, 28.

<sup>10</sup> Joint Press Conference, March, 29, 2012, Sydney, Australia. <http://www.pm.gov.au/press-office/transcript-joint-press-conference-sydney-1>.

<sup>11</sup> The Economist, “Huawei: The Company that Spooked the World,” *Economist*, August, 4, 2012. <http://www.economist.com/node/21559929> (accessed September 30, 2012).

<sup>12</sup> United States Congress, *2011 Annual Report of U.S.-China Economic and Security Review*. (2011, Washington DC: 148.)

<sup>13</sup> Office of National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage*, “Foreign Spies Stealing US Economic Secrets in Cyberspace.” (October 2011, Washington, DC: i.)

<sup>14</sup> Ibid, 5: HPSCI staff interviews with cyber-security experts.

<sup>15</sup> Ibid, 5.

<sup>16</sup> Defense Science Board, *Report on Mission Impact of Foreign Influence on DoD Software*, September 2007: viii.

<sup>17</sup> “Where State security requires, a State security organ may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organization or individual.” State-Security Law of the People’s Republic of China, Article 11.

<sup>18</sup> Defense Science Board, *Report on Mission Impact of Foreign Influence on DoD Software*, September 2007: viii.

<sup>19</sup> Northrop Grumman Corp, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, prepared for U.S.-China Economic and Security Review Commission, March 7, 2012, 6-8.

<sup>20</sup> The Economist, “The Long March of the Invisible Mr. Ren,” *the Economist*, June 2, 2011.

<http://www.economist.com/node/18771640> (accessed on September 15, 2012).

<sup>21</sup> FBI, *Intelligence Bulletin*, “Supply Chain Poisoning: A Threat to the Integrity of Trusted Software and Hardware,” June 27, 2011: 4.

<sup>22</sup> ZTE, *Submissions to HPSCI*, July 3, 2012; ZTE, *Submission to HPSCI*, August 3, 2012; Ken Hu, “Huawei Open Letter.” <http://online.wsj.com/public/resources/documents/Huawei20110205.pdf> (accessed August 2, 2012). John Suffolk, Huawei’s Global Security Officer, previously served as the Chief Information Officer with the UK government at a time when the UK entered into its agreement with Huawei to set up the Cyber Security Evaluation Center (CSEC). Mr. Suffolk advocated for a cyber-security and supply-chain solution that would recognizing the issues as a global concern that must be addressed at an international level, preferably by an international standards-setting organization through which all products must pass. Mr. Suffolk also highlighted that in the present age, technology is moving faster than our ability to adapt our institutions. Key assumptions are that security requires a whole systems approach, and that all systems will be breached at some point. Thus, in Mr. Suffolk’s view, telecommunications companies and governments must manage the risk, focus on areas of most concern, instill diversity and adaptability, and learn to deal with the consequences. Mr. Suffolk acknowledged that Huawei’s desire to be an end-to-end provider for whole network solutions does not align with his proposed solutions to the supply-chain concerns, which depend on diversity of supply. HPSCI meeting with John Suffolk, February 23, 2012.

<sup>23</sup> Anderson, R., & Fuloria, S. *Certification and Evaluation: A Security Economics Perspective. Emerging Technologies and Factory Automation*, (2009).

<sup>24</sup> Ken Thompson, *Reflections on Trusting Trust. Turing Award Lecture*, (1984).

<sup>25</sup> Gerwin Klein, *Formal Verification of an OS Kernel. Symposium on Operating Systems Principles*. Big Sky, MT, USA: Association of Computing Machinery, (2009).

<sup>26</sup> Daniel Jackson, Martyn Thomas, and Lynette I. Millett, Eds. *Software for Dependable Systems: Sufficient Evidence? Committee on Certifiably Dependable Software Systems*, National Research Council (National Academies Press, 2007.)

<sup>27</sup> Rules of the House of Representatives, 112<sup>th</sup> Congress, Rules 10(3)(m), 11.

<sup>28</sup> Understanding and developing a strategy to protect the country from Chinese cyber espionage in the United States is one of the obligations of U.S. counterintelligence professionals. Many reports have suggested that the Intelligence Community continues to struggle integrating and acting on its counterintelligence mission. As Michelle Van Cleave, former head of the National Counterintelligence Executive, has explained, “the U.S. government has been slow to appreciate the effects of foreign intelligence operations, much less to address the threats they pose to current U.S. foreign policy objectives or enduring national security interests.” Michelle Van Cleave, “Chapter 2: The NCIX and the National Counterintelligence Mission: What Has Worked, What Has Not, and Why,” in *Meeting Twenty-First Century Security Challenges*, 62.



Office of National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage*, “Foreign Spies Stealing US Economic Secrets in Cyberspace.” (October 2011, Washington, DC)

<sup>30</sup> In response to the Committee’s June 12, 2012, document request, ZTE provided one document: a summary of its cyber-security measures. Huawei provided no documents other than materials already on the company’s website or otherwise publicly released. After the September 13, 2012 hearing, Huawei provided a document labeled “Internal Compliance Program (ICP),” dated March 2012. That document summarizes Huawei’s internal policy with respect to trade control policies. Huawei provided no material that would allow the Committee to evaluate their compliance with or enforcement of that policy. Huawei also provided a copy of the publicly released paper entitled “Cyber Security Perspectives” prepared by John Suffolk, and Huawei’s public statement regarding its Commercial Operations in Iran.

<sup>31</sup> House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112<sup>th</sup> Congress, 2nd session (September 13, 2012).

<sup>32</sup> Given the sensitivities involved, and to protect these witnesses from retaliation or dismissal, the Committee decided to keep the identities of these individuals confidential.

<sup>33</sup> As the U.S.-China Commission has highlighted, even the largely circumstantial evidence that known incidents appear state sponsored is compelling -- as the actors’ targeting often focuses on key defense and foreign-policy sources of information, which are of most concern to the state and not commercial entities. United States Congress, *2011 Annual Report of U.S.-China Economic and Security Review*. (2011, Washington DC: 59.)

<sup>35</sup> United States Congress, *2011 Annual Report of U.S.-China Economic and Security Review*. (2011, Washington DC: 59-60.)

<sup>36</sup> ZTE, *Submission to HPSCI*, July 3, 2012, 3.

<sup>37</sup> Discussion with PLA Piper, June 2012. Huawei, in its responses to Questions for the Record after the September 13, 2012, hearing, denied that there is any state-secret concern with their documentation. The Committee is left wondering, then, why Huawei has refused to provide internal documentation that could substantiate its claims. Moreover, Huawei’s failure to provide the list of individuals on Huawei’s Chinese Communist Party Committee is an example in which the Committee believes the state’s concerns with state secrets is particularly relevant. Huawei’s continuous failure to provide such information cannot be explained otherwise.

<sup>38</sup> Huawei Investment & Holding Co., Ltd., *2011 Annual Report*, 7.

<sup>39</sup> Ken Hu, “Huawei Open Letter.” <http://online.wsj.com/public/resources/documents/Huawei20110205.pdf> (accessed August 2, 2012).

<sup>40</sup> That report suggests that Huawei “was founded in 1988 by Ren Zhengfei, a former director of the PLA General Staff Department’s Information Engineering Academy, which is responsible for telecom research for the Chinese military. Huawei maintains deep ties with the Chinese military, which serves a multi-faceted role as an important customer, as well as Huawei’s political patron and research and development partner. Both the government and the military tout Huawei as a national champion, and the company is currently China’s largest, fastest-growing, and most impressive telecommunications-equipment manufacturer. Evan Medeiros et al., *A New Direction for China’s Defense Industry*, Rand Corporation: 218-219. [http://www.rand.org/pubs/monographs/2005/RAND\\_MG334.pdf](http://www.rand.org/pubs/monographs/2005/RAND_MG334.pdf).

<sup>41</sup> *Ibid*, 217-219

<sup>42</sup> The Economist, “Huawei: The Company that Spooked the World,” *Economist*, August, 4, 2012. <http://www.economist.com/node/21559929> (accessed September 30, 2012).

<sup>43</sup> Juha Saarinen, “Analysis: Who Really Owns Huawei?,” *ITNews*, May 28, 2012.

<sup>44</sup> Ken Hu, “Huawei Open Letter.” <http://online.wsj.com/public/resources/documents/Huawei20110205.pdf> (accessed August 2, 2012).

<sup>45</sup> Richard McGregor, *The Party: The Secret World of China’s Communist Rulers*, 2010: 204.

<sup>46</sup> Huawei, *Submission to HPSCI*, July 3, 2012.

- 
- <sup>47</sup> House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112<sup>th</sup> Congress, 2nd session (September 13, 2012).
- <sup>48</sup> Huawei Investment & Holding Co., Ltd., *2011 Annual Report*, 2.
- <sup>49</sup> Huawei, *September 25, 2012 Response to Questions for the Record*, at \_\_\_\_.
- <sup>50</sup> Huawei, *September 25, 2012 Responses to Questions for the Record*, 6-7.
- <sup>51</sup> Interviews with Huawei officials, February 23, 2012.
- <sup>52</sup> Interviews with Huawei officials, February 23, 2012.
- <sup>53</sup> Interviews with Huawei officials, February 23, 2012.
- <sup>54</sup> Mike Rogers and Dutch Ruppersburg, letter to Huawei, June 12, 2012; Huawei, *letter to HPSCI*, “Response to June 12, 2012 Letter,” July 3, 2012.
- <sup>55</sup> Huawei, *Documents Provided in Advance of February 23, 2012 entitled Shareholder Agreements*.
- <sup>56</sup> John Lee, “The Other Side of Huawei,” *Business Spectator*, March 30, 2012.
- <sup>57</sup> United States Congress, *2011 Annual Report of U.S.-China Economic and Security Review*. (2011, Washington DC: 59)
- <sup>58</sup> *Ibid.*
- <sup>59</sup> House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112<sup>th</sup> Congress, 2nd session (September 13, 2012).
- <sup>60</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 1.
- <sup>61</sup> *Ibid.*
- <sup>62</sup> *Ibid.*
- <sup>63</sup> Huawei, *July 2, 2012 Submission*, 7-15
- <sup>64</sup> Highlighting that as China moved from a pure control economy in the 1990s, Chinese companies experienced particular difficulties raising capital in foreign capital markets, including the “most sensitive of all, how would they explain the role of the internal party bodies, which for years had run companies, free of any of the inconvenient structuring of corporate reporting and governance rules.” Richard McGregor, *The Party: The Secret World of China’s Communist Rulers*, 2010: 47; See John Lee, “The Other Side of Huawei,” *Business Spectator*, March 30, 2012
- <sup>65</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 2.
- <sup>66</sup> *Ibid.*
- <sup>67</sup> See John Lee, “The Other Side of Huawei,” *Business Spectator*, March 30, 2012; Richard McGregor, *The Party: The Secret World of China’s Communist Rulers*, 2010.
- <sup>68</sup> Richard McGregor, *The Party: The Secret World of China’s Communist Rulers*, 2010: 72.
- <sup>69</sup> Meeting with Mr. Ren, May 23, 2012.
- <sup>70</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012.
- <sup>71</sup> Huawei officials stated that China had cancelled ranking system at the time. HPSCI Interviews with Huawei officials, February 23, 2012.
- <sup>72</sup> Huawei officials suggested that the rumors that Mr. Ren is a former PLA General is the result of confusion with Julong, another Chinese telecommunications company and state-owned enterprise whose President is a Major General in the PLA. HPSCI Interviews with Huawei officials, February 13, 2012.
- <sup>73</sup> Huawei, *September 25, 2012 Responses to HPSCI Questions for the Record*, 8.
- <sup>74</sup> Huawei, *September 25, 2012 Responses to HPSCI Questions for the Record*, 8.
- <sup>75</sup> Huawei asserted that Chen Jinyang, who invested 3,500 RMB, was a 26-year-old manager at the Chinese Trade Department.
- <sup>76</sup> Interviews with Huawei officials, February 23, 2012.
- <sup>77</sup> Interviews with Huawei officials, February 23, 2012.
- <sup>78</sup> Interview with Ken Hu, February 23, 2012.
- <sup>79</sup> Scholars of the Chinese political economy suggest that national champions are those chosen by China to be supported both financially and otherwise by the state because of the strategic importance of the sector and the company to China’s national interests. See John Lee, “The Other Side of Huawei,” *Business Spectator*, March 30, 2012

- 
- <sup>80</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 19.
- <sup>81</sup> *Ibid.*
- <sup>82</sup> Interviews with Huawei officials, February 23, 2012; Huawei presentation, February 23, 2012.
- <sup>83</sup> Interviews with Huawei officials, February 23, 2012
- <sup>84</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 19-20.
- <sup>85</sup> Mike Rogers and Dutch Ruppersburg, letter to Huawei, June 12, 2012, 6.
- <sup>86</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 19-20.
- <sup>87</sup> Phone conversations with Huawei representatives, June 2012.
- <sup>88</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 20-21.
- <sup>89</sup> John Lee, "The Other Side of Huawei," *Business Spectator*, March 30, 2012.
- <sup>90</sup> The Economist, Huawei: The Company that Spooked the World," *Economist*, August, 4, 2012. <http://www.economist.com/node/21559929> (accessed September 30, 2012);
- <sup>91</sup> House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112<sup>th</sup> Congress, 2nd session (September 13, 2012).
- <sup>92</sup> Huawei, *Slide Presentation dated November 2011*, 8.
- <sup>93</sup> Huawei, *Responses to HPSCI Questions for the Record*, September 25, 2012, 1.
- <sup>94</sup> *Ibid.*
- <sup>95</sup> *Ibid.*
- <sup>96</sup> Interviews with Huawei officials, February 23, 2012
- <sup>97</sup> Huawei, *Corporate Presentation*, February 23, 2012, 26.
- <sup>98</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 2.
- <sup>99</sup> Huawei, *Corporate Presentation*, February 23, 2012, 27.
- <sup>100</sup> Huawei, *Responses to HPSCI Questions for the Record*, September 25, 2012, 2.
- <sup>101</sup> Interviews with Huawei officials, February 23, 2012.
- <sup>102</sup> House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112<sup>th</sup> Congress, 2nd session (September 13, 2012).
- <sup>103</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 21.
- <sup>104</sup> Interviews with Huawei officials, February 23, 2012.
- <sup>105</sup> Ren Zhengfei, speech at Huawei BT Division & Huawei UK, June 30, 2007, quoted in Huawei magazine *Improvement*, Issue 58.
- <sup>106</sup> The Commerce Department, working with the Defense Department, has sought information from the private sector to better understand the entire scope of cyber-risks facing the country's critical telecommunication infrastructure. The Commerce issued a survey under the Defense Production Act to dozens of U.S. based companies to gather better information on the security of their networks. The review of that information is still ongoing.
- <sup>107</sup> The Committee has offered on numerous occasions to provide Huawei an opportunity to provide the information the Committee needs to evaluate the security of U.S. networks in a closed forum or under an agreement to provide such information confidentially. Huawei has continuously refused to accept any such offer, option instead to simply assert that such details are confidential. The Committee intends to continue evaluating these issues and plans to approach Huawei in the future for more details on these contracts to fulfill the Committee's duty to evaluate the risk posed by these firms.
- <sup>108</sup> House Committee on Foreign Affairs, *Hearing on Unfair Trade Practices against the US*, 112<sup>th</sup> Congress, 2nd session (July 19, 2012).
- <sup>109</sup> Interview with Huawei officials, February 23, 2012.
- <sup>110</sup> Interview with Employees.
- <sup>111</sup> John Lee, "The Other Side of Huawei," *Business Spectator*, March 30, 2012.
- <sup>112</sup> Interview with Huawei officials, February 23, 2012.
- <sup>113</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012.
- <sup>114</sup> Interview with Huawei Employees.
- <sup>115</sup> Interview with Huawei Employees.

---

<sup>116</sup> Interview with industry experts.

<sup>117</sup> Huawei representatives admitted to Committee staff that using this presentation was in violation of McKinsey's copyright protections, and that McKinsey and Huawei have no business relationship thus undermining any claim that Huawei had a right to use the slide. Huawei, *Slide Presentation dated November 2011*, 8 (using McKinsey & Co. material).

<sup>118</sup> Interview with Huawei Officials, February 13, 2012.

<sup>119</sup> Ibid.

<sup>120</sup> Marguerite Reardon, "Huawei Admits Copying," *Light Reading*, March 25, 2003.

[http://www.lightreading.com/document.asp?doc\\_id=30269](http://www.lightreading.com/document.asp?doc_id=30269) (accessed on August 13, 2012)

<sup>121</sup> Ibid.

<sup>122</sup> House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112<sup>th</sup> Congress, 2nd session (September 13, 2012).

<sup>123</sup> Huawei, *Submission to House Permanent Select Committee on Intelligence*, July 3, 2012, 6.

<sup>124</sup> Ibid.

<sup>125</sup> Ibid, 5-6.

<sup>126</sup> Ibid, 3-4.

<sup>127</sup> Ibid, 3.

<sup>128</sup> Interviews with Huawei officials, February 23, 2012.

<sup>129</sup> Huawei, *September 25, 2012 Responses to Questions for the Record*, 12.

<sup>130</sup> Ibid.

<sup>131</sup> Internal Huawei email, dated July 1, 2011.

<sup>132</sup> Ibid.

<sup>133</sup> Interviews with former Huawei employees.

<sup>134</sup> Interviews with former Huawei employees.

<sup>135</sup> Huawei, *Slide Presentation dated November 2011*, 8.

<sup>136</sup> ZTE August 3, 2012 submission, at 12-17.

<sup>137</sup> ZTE, *Submissions to HPSCI*, August 3, 2012, 23.

<sup>138</sup> ZTE, *2011 Annual Report*, 68-69.

<sup>139</sup> "The national '12th Five Year Plan' has provided driving force for the further development of the domestic telecommunications industry." ZTE, *2011 Annual Report*, 69.

<sup>140</sup> Meeting with ZTE officials, April 12, 2012, Shenzhen, China.

<sup>141</sup> ZTE, *Submissions to HPSCI*, July 3, 2012.

<sup>142</sup> Ibid, 4.

<sup>143</sup> Ibid.

<sup>144</sup> As a report commissioned by the U.S. China-Commission stated: "The IT sector in China can be considered a hybrid defense industry, able to operate with success in commercial markets while meeting the demands of its military customers. The Chinese telecommunications market is heavily influenced by its largest domestic members—such as hardware and networking giants Huawei Shenzhen Technology Company, Zhongxing Telecom (ZTE), and Datang Telecom Technology Co., Limited. These companies and some smaller players are not always directly linked to the PLA or C4ISR modernization because of their strong domestic and international commercial orientation. The digital triangle model, however, allows them to benefit directly from a background network of state research institutes and government funding in programs that do have affiliation or sponsorship of the PLA." Northrop Grumman Corp, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, prepared for U.S.-China Economic and Security Review Commission, March 7, 2012, 69.

<sup>145</sup> ZTE, *Submissions to HPSCI*, July 3, 2012, 2.

<sup>146</sup> Ibid, 9

<sup>147</sup> Ibid.

<sup>148</sup> Ibid, 4.



---

<sup>149</sup> House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112<sup>th</sup> Congress, 2nd session (September 13, 2012).

<sup>150</sup> John Merrigan, letter to Katie Wheelbarger, September 28, 2012.

<sup>151</sup> Affidavit of Timothy Steinert, at para. 6.

<sup>152</sup> ZTE, *Submissions to HPSCI*, August 3, 2012, 5.

<sup>153</sup> Meeting with ZTE officials, April 12, 2012, Shenzhen, China.

<sup>154</sup> *Ibid.*

<sup>155</sup> House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112<sup>th</sup> Congress, 2nd session (September 13, 2012).

<sup>156</sup> Ellen Nakashima, "Chinese telecom firm ZTE probed for alleged sale of U.S. surveillance equipment to Iran," *Washington Post*, July 13, 2012. [http://www.washingtonpost.com/world/national-security/chinese-telecom-firm-zte-probed-for-alleged-sale-of-us-surveillance-equipment-to-iran/2012/07/13/gJQA6mKUW\\_story.html](http://www.washingtonpost.com/world/national-security/chinese-telecom-firm-zte-probed-for-alleged-sale-of-us-surveillance-equipment-to-iran/2012/07/13/gJQA6mKUW_story.html).

<sup>157</sup> House Permanent Select Committee on Intelligence, *Hearing on Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112<sup>th</sup> Congress, 2nd session (September 13, 2012).

<sup>158</sup> ZTE, *Submissions to HPSCI*, April 2012, 4.

<sup>159</sup> *Ibid.*

<sup>160</sup> *Ibid.*

<sup>161</sup> ZTE, *Submissions to HPSCI*, July 3, 2012, 17.

# EXHIBIT 3



**U.S.-China Economic and Security  
Review Commission Staff Report**

**January 2011**

(information current as of November 2010)

**THE NATIONAL SECURITY IMPLICATIONS  
OF INVESTMENTS AND PRODUCTS FROM  
THE PEOPLE'S REPUBLIC OF CHINA  
IN THE TELECOMMUNICATIONS SECTOR**

**by USCC Research Staff**

**supported by Reperi LLC**

**Disclaimer:**

***This paper is the product of professional research performed by staff of the U.S.-China Economic and Security Review Commission, supported by technical analysis and market trend analysis performed by Reperi LLC. The research supporting this report has been monitored by individual members of the Commission; however, this report and its contents do not necessarily reflect the positions or opinions of either the Commission or of its individual members, or of the Commission's other professional staff.***

***Research for this report was performed in 2009 and 2010. A good faith effort has been made to present accurate information that would be current as of the time of publication. Any differences between current data and data in this report may be due to changes occurring during time elapsed for report preparation and review, or to the reliability of data from sources consulted.***

## NOTICE

This paper presents an open source analysis of the impact on U.S. national security interests of China's extensive engagement in the U.S. telecommunications sector.

The paper's research covers the following:

- The nature of changes in the U.S. telecommunications supply chains and the impacts on U.S. national security.
- The technological trends in telecommunications and related technologies.
- The People's Republic of China's (PRC) direct and indirect investment trends in telecommunications and related technologies and in the U.S. telecommunications marketplace.
- The nature of the People's Republic of China's direct and indirect ownership, control, and influence in the U.S. telecommunications supply chain.
- The penetration of the U.S. marketplace by companies subject to ownership, control, or influence by the People's Republic of China.
- The locations where products designed, engineered, or manufactured in China or supplied by companies subject to control or influence by China may appear in the U.S. marketplace and critical supply chains.
- The trends in the marketplace that can be attributed to the influence of China's ubiquitous presence in U.S. supply chains.
- The nature of relationship-building between U.S. companies and companies located in and/or subject to control or influence by the People's Republic of China.
- The potential vulnerabilities of critical elements of the U.S. telecommunications market exploitable by actors in supply chain segments.
- The assessment of potential cyber security impacts.
- The means of assessing telecommunications and supply chain vulnerabilities.
- The impacts of present and emerging vulnerabilities on U.S. defense contractors and government procurement functions.

## TABLE OF CONTENTS

<b>INTRODUCTION</b>	<b>6</b>
 <b>SECTION 1:</b>	
<b>MACRO-LEVEL PATTERNS OF CHINA’S</b>	
<b>TELECOM INVESTMENT ACTIVITIES</b>	<b>9</b>
• <i>Text Box: Telecommunications as a “Strategic” Industry in China</i>	10
• Global Telecommunication Market Trends in 2008-2009	11
• <b>CHINESE TELECOM COMPANIES ENTER THE U.S. MARKET</b>	
China: Developer and Provider within China and	
Global Exporter of Wireless and Next Generation Networks	12
• Huawei Technologies	13
• <i>Text Box: European Controversies over Alleged State Support to Huawei</i>	13
• <i>Figure 1: Huawei Technologies Offices in North America</i>	15
• <i>Text Box: Controversies Surrounding the Activities of Huawei</i>	15
• Recent Unconsummated Huawei Deals, and Potential Deals on the Horizon	19
• <i>Text Box: Concerns Regarding Potential Network Penetration</i> <i>by PRC Intelligence Agencies</i>	20
• ZTE Corporation	21
• The Role of Huawei and ZTE in the U.S. Market	23
• <i>Text Box: Examples of U.S. Market Penetration by Chinese</i> <i>Telecom Companies</i>	23
• The Major Chinese Domestic Telecom Corporations	24
• <i>Text Box: State-Directed Personnel Shuffling and Restructuring</i> <i>At PRC Telecom Corporations</i>	27
• <b>HUAWEI AND 3-COM: A CLASSIC EXAMPLE OF CHINA’S FORAYS INTO</b> <b>THE U.S. MARKET VIA JOINT VENTURE AND ACQUISITION</b>	28
• <i>Text Box: A Timeline History of 3Com</i>	29
• <b>DEALS IN THE TELECOM SECTOR, AND THE ROLE OF CFIUS</b>	30
• <i>Text Box: CFIUS and the Abortive Emcore / Caofeidian Deal</i>	31
• <i>Figure 2: Location of Caofeidian Island</i>	32
• <i>Figure 3: Artist Conception of Caofeidian Island</i>	32
• <b>THE GROWTH STRATEGY OF CHINESE TELECOM FIRMS</b>	33
• <b>EXPANSION INTO DEVELOPING MARKETS</b>	34
• <b>THE EAST-WEST FLOW OF INVESTMENTS</b> <b>IN THE COMMUNICATIONS SECTOR</b>	36
 <b>SECTION 2:</b>	
<b>POTENTIAL VULNERABILITIES IN COMMUNICATIONS</b>	
<b>INFRASTRUCTURE AND PRODUCTS, AND CHINESE</b>	
<b>INVESTMENTS IN THESE SECTORS</b>	<b>39</b>
• <b>INVESTMENTS IN LONG-HAUL FIBER</b>	39
• <i>Text Box: The Security of Optical Fiber Networks, and the</i> <i>Case of Global Crossing and Hutchison-Whampoa</i>	40
• <i>Figure 4: Global Crossing Networks in 2010</i>	41
• <b>ROUTERS, SWITCHES, AND HUBS</b>	42
• <b>WiMAX/WiFi – NETWORK AND NETWORK CONTROL DEVICES</b> <b>AND PROTOCOLS FOR WIRELESS NETWORKING</b>	44
• <i>Text Box: Huawei and the Development of LTE Standards</i>	45
• <b>APPLICATIONS SOFTWARE: Software/Controllers/Drivers</b>	46

• <b>NETWORK SECURITY PRODUCTS: Security Software</b>	<b>46</b>
• <i>Text Box: The Creation of Huawei Symantec</i>	<b>47</b>
• <b>HANDSETS AND SMART PHONES</b>	<b>48</b>
• <i>Figure 5: A T-Mobile UK “Pulse” Smartphone with Huawei Android Technology</i>	<b>49</b>
• <b>HANDSETS AND SMART PHONES: POTENTIAL VULNERABILITIES</b>	<b>49</b>
• <i>Text Box: The Debate Over “Open” vs. “Closed” Standards</i>	<b>50</b>
• <b>WIRELESS HEADSETS, EARPIECES, AND BLUETOOTH</b>	<b>54</b>
• <b>Bluetooth: Potential Vulnerabilities</b>	<b>54</b>
• <i>Text Box: Switching Equipment and Other Networking Services – The Nortel Story</i>	<b>54</b>
• <i>Table 1: Where China's Products Are Found in the U.S. Communications Market</i>	<b>57</b>
• <i>Table 2: Where China's Investments Are Found in the U.S. Communications Market</i>	<b>58</b>
• <i>Figure 6: Sample Integrated Operational Network Model (Healthy)</i>	<b>59</b>
• <i>Figure 7: Sample Integrated Operational Network Model (Corrupted)</i>	<b>60</b>
• <i>Figure 8: Sample Integrated Operational Network Model (Disabled)</i>	<b>61</b>

### **SECTION 3:**

<b>SUPPLY CHAIN INTEGRITY, AND THE IMPACT ON GOVERNMENT/DEFENSE CONTRACTING</b>	<b>62</b>
• <i>Text Box: Supply Chain Integrity and Cyber Security</i>	<b>63</b>
• <i>Text Box: Chinese Cyber Espionage Directed vs. the United States</i>	<b>65</b>
• <b>CONTROL OF MANUFACTURING PROCESSES</b>	<b>65</b>
• <i>Text Box: Lenovo’s Entry into the U.S. Computer Market, and Controversies Surrounding its Government Sales</i>	<b>66</b>
• <b>MICROCHIP MANUFACTURING: Key Cyber Security and National Security Risks</b>	<b>68</b>
• <i>Text Box: The Defense Science Board Task Force 2005 Report on High-Performance Microchip Supply</i>	<b>69</b>
• <i>Text Box: Recent Cases Involving Counterfeited Computer Equipment from China</i>	<b>71</b>
• <b>TESTING OF INTEGRATED CIRCUITS</b>	<b>72</b>
• <b>Kill Switches and Backdoors</b>	<b>74</b>

<b>CONCLUSIONS &amp; RECOMMENDATIONS</b>	<b>75</b>
• <b>SUPPLY CHAIN SECURITY AND POTENTIAL IMPACTS ON GOVERNMENT CONTRACTING FOR SENSITIVE SYSTEMS</b>	<b>75</b>
• <b>RESPONSES TO SUPPLY CHAIN CHALLENGES</b>	<b>76</b>
• <b>THE CHESS GAME OF STANDARDS – THE NEW METHODS FOR OWNING SUPPLY CHAINS</b>	<b>77</b>
• <b>INNOVATION IN AMERICA, AND THE SHORTAGE OF MATHEMATICIANS, SCIENTISTS, AND ENGINEERS</b>	<b>78</b>
• <i>Table 3: Computer Science and Engineering Bachelor’s Degree Enrollments in the United States, 1980-2005</i>	<b>80</b>
• <b>PRODUCT CONTROL ISSUES IN GOVERNMENT COMMUNICATIONS SYSTEMS</b>	<b>80</b>

### **APPENDICES**

• <b>Appendix A: What Is a Cyber Attack?</b>	<b>82</b>
• <b>Appendix B: Glossary</b>	<b>85</b>
• <b>Appendix C: Partial Bibliography</b>	<b>93</b>



## INTRODUCTION

The increased presence of Chinese telecommunications products and services in the American marketplace is the result of bilateral investment between the United States and China. Chinese companies have offered U.S. investors (investment banks, venture firms, business investors, and others) opportunities to balance risk and gain potentially higher rates of return by participating in the world's fastest-growing emerging market. By outsourcing some aspects of operations, U.S. businesses and multinational corporations have been able to increase the amount of value built into products compared to the same dollars expended domestically and have further been able to diversify market holdings in Asia after reaching saturation points in U.S. and European markets.

In a similar way, Chinese companies are increasingly looking to the American market to open up new opportunities.<sup>1</sup> U.S. companies have offered Chinese firms and investment funds access to established business models and advanced research and development processes, increased efficiencies in select areas of business, and opportunities in the world's wealthiest market. Aside from raising their own levels of technical and management expertise, they are also able to affiliate their products with the excellent reputation of U.S. brands in global markets. China's technology industry now appears to be a de facto part of the American communications industry landscape. Based on current market realities, the presence and continued growth of products with at least partial manufacturing and development origins in China will continue to increase and pervade most areas of American life, business, and government.

Chinese telecommunications companies are also actively expanding into global markets. In emerging markets not encumbered by existing legacy infrastructures, demand for new telecom capabilities is often best met by utilizing generation-leaping technologies, a phenomenon that is helping to drive a large global appetite for leading-edge technological innovation. Chinese telecom technology companies are aggressively pursuing customers in emerging communications technologies – and are thus gaining traction in global markets, particularly emerging markets.

The expansion strategy of Chinese telecoms is becoming increasingly more effective as business acumen gained from joint ventures, partnerships, and acquisitions improves their competitive capabilities. Chinese companies have also thoughtfully cultivated global management and recruitment models that are helping them move into positions of global leadership through management excellence.<sup>2</sup> Direct and indirect investment from developed countries into Chinese telecom and technology ventures, and China's own strategic acquisitions of technological know-how and physical infrastructures in other emerging markets, are also facilitating their emergence as a formidable global competitor.

Many aspects of the future global telecom and technology markets are now being shaped by Chinese business and governmental interests. The momentum they are gaining and the way they are applying their advantages are transforming global markets, propelling Chinese telecom

<sup>1</sup> Dezan Shira & Associates, "Made in USA: China and India Invest Abroad," May 13, 2010.

<http://www.2point6billion.com/news/2010/05/13/made-in-usa-china-and-india-invest-abroad-5645.html>.

<sup>2</sup> Northrop Grumman Corporation, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" (contracted research paper for the U.S.-China Economic and Security Review Commission, June 2009).

[http://www.uscc.gov/researchpapers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper\\_FINAL\\_Approved%20Report\\_16Oct2009.pdf](http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf).

and technology ventures toward the leading edge of technology development, manufacturing, and standards setting. If current trends continue, China (combined with proxy interests) will effectively become the principal market driver in many sectors, including telecom, on the basis of consumption, production, and innovation.

This greater potential role for China has generated concerns regarding corresponding potential national security implications of manufacturing and investment by China's telecommunications companies. Signals intelligence (SIGINT) is a significant source of Chinese intelligence collection,<sup>3</sup> and there is growing public concern over the impacts of cyber espionage incidents that appear to originate in China.<sup>4</sup> Furthermore, large China-based, -owned, or -influenced companies – particularly those “national champions” prominent in China's “going out” strategy of overseas expansion – are subject to government direction, to include support for PRC (People's Republic of China) state policies and political goals.<sup>5</sup> In light of this, the large footprints of Chinese state-affiliated companies in global telecommunications markets, and their acquisitions in part or in whole of western telecom firms, may generate concerns in some quarters that this may facilitate increased intelligence exploitation of international communications and computer networks by Chinese state-affiliated entities. Concern over growing Chinese influence in this arena is not unfounded, but should be balanced by a realistic assessment of communications security vulnerabilities as well as by an appreciation of the symbiosis that has developed between the Chinese and western telecommunications industries.

The greatest potential impact on the United States could come in the form of Chinese investments in U.S. telecommunications companies. The vast global telecommunications and technology infrastructures owned or operated by these companies include undersea, terrestrial, wireless, and space-based networks. These investments would increase China's leverage in the U.S. marketplace and beyond (even if indirectly through joint ventures and third parties) and could eventually provide China access to or control of vital U.S. and allied information, networks, or segments of critical supply chains.

Another key concern regarding the security of U.S. communication and computer networks relates to the reliability of electronics components found within the network hardware. National security vulnerabilities attributable to having critical infrastructure components manufactured, implemented, operated, or maintained by foreign actors are increasing at an escalated rate. Within government, steps can be taken to safeguard sensitive areas but at a substantially increased cost in both resources and lost opportunities to innovate. Trusted hardware and software produced domestically may cost more than commoditized products produced abroad. The government may also find that it will have to curb the infusion of ever-newer communications technologies into some especially sensitive areas in favor of retaining secure legacy technology models.

---

<sup>3</sup> Interagency OPSEC (Operations Security) Support Staff, *Intelligence Threat Handbook* (June 2004), p. 23. <http://www.fas.org/irp/threat/handbook/foreign.pdf>; and Interagency OPSEC Support Staff, *Intelligence Threat Handbook – Selected Supplemental Intelligence Service Information* (June 2004), pp. 75-76. <http://www.fas.org/irp/threat/handbook/supplement.pdf>.

<sup>4</sup> Northrop Grumman Corporation, “Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation” (contracted research paper for the U.S.-China Economic and Security Review Commission, June 2009). [http://www.uscc.gov/researchpapers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper\\_FINAL\\_Approved%20Report\\_16\\_Oct2009.pdf](http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16_Oct2009.pdf)

<sup>5</sup> For a detailed explanation and examples of this phenomenon, see “China, Inc.: The Party and Business,” chapter 2, in Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: Harper Collins, 2010).

Staking out a middle course between being unduly alarmist and unduly complacent, this report seeks to lay out in greater detail many of the issues involved in the international investments made by Chinese telecommunications firms. It also seeks to describe some of the *potential* security vulnerabilities in communications networks that might be exploited by hostile actors, whether state sponsored or otherwise. It is hoped that this will help to better illuminate for Congress and the general public a critical area of concern that stands astride the crossroads of U.S. national security and future economic security.

## SECTION 1

# MACRO-LEVEL PATTERNS OF CHINA'S TELECOM INVESTMENT ACTIVITIES

The Chinese government treats the telecommunications sector as a “strategic” industry (see *text box below*) and has expended significant effort and resources to promote and enable new business opportunities in the telecommunications field. These efforts are supported by national-level policies, as the country’s senior leadership perceives investment in high-technology sectors to be instrumental in closing the technological gap between China and western nations.<sup>6</sup> The large and growing state-controlled telecommunications sector is also a major source of government revenue. As stated by political scientist Cheng Li:

*The Chinese government has always considered the telecom sector to be one of the most strategically important and commercially lucrative industries in the country. [As of] 2005, the six leading Chinese telecom operation providers [were]: China Telecom, China Mobile, China Netcom, China Unicom, China Railcom, and China Satcom, all of which [were] state-owned enterprises (SOEs), reported that they had total assets of 10.6 trillion yuan, revenues of 6.6 trillion yuan, and profits of 600 billion yuan. [As of that year,] [t]hese six companies constituted one-sixth of the total assets, and 20 percent of the profits, of all of the enterprises directly under the leadership of the State-Owned Assets Supervision and Administration Commission.*<sup>7</sup>

National security concerns have accompanied the dramatic growth of China’s telecom sector. Signals intelligence is a significant source of Chinese intelligence collection,<sup>8</sup> and there is growing public concern over the impacts of cyber espionage incidents that appear to originate in China.<sup>9</sup> Additionally, large Chinese companies – particularly those “national champions” prominent in China’s “going out” strategy<sup>10</sup> of overseas expansion – are directly subject to direction by the Chinese Communist Party (CCP), to include support for PRC state policies and goals.<sup>11</sup> From this point of view, the clear economic benefits of foreign investment in the United States must be weighed against the *potential* security concerns related to infrastructure

<sup>6</sup> Evan Feigenbaum, *China’s Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age* (Palo Alto, CA: Stanford University Press, 2003).

<sup>7</sup> Cheng Li, “China’s Telecom Industry on the Move: Domestic Competition, Global Ambition, and Leadership Transition,” *China Leadership Monitor* 19 (2006).

<sup>8</sup> Interagency OPSEC Support Staff, *Intelligence Threat Handbook* (June 2004), p. 23.

<http://www.fas.org/irp/threat/handbook/foreign.pdf>; and Interagency OPSEC Support Staff, *Intelligence Threat Handbook – Selected Supplemental Intelligence Service Information* (June 2004), pp. 75-76. <http://www.fas.org/irp/threat/handbook/supplement.pdf>.

<sup>9</sup> Northrop Grumman Corporation, “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation” (contracted research paper for the U.S.-China Economic and Security Review Commission, June 2009). [http://www.uscc.gov/researchpapers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper\\_FINAL\\_Approved%20Report\\_16\\_Oct2009.pdf](http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16_Oct2009.pdf)

<sup>10</sup> The “Going Out” strategy is a Chinese government campaign introduced at the 2002 Communist Party Congress to raise China’s global economic profile by investing overseas and acquiring foreign assets. See U.S.-China Economic and Security Review Commission, *Annual Report to Congress 2009* (Washington, DC: U.S. Government Printing Office, November 2009), p. 94, footnote #52. See also Jamil Anderlini, “China to Deploy Forex Reserves,” *Financial Times*, July 21, 2009; and Accenture Consulting, “China Spreads Its Wings: Chinese Companies Go Global,” 2007.

<sup>11</sup> For a detailed explanation and examples of this phenomenon, see “China, Inc.: The Party and Business,” chapter 2, in Richard McGregor, *The Party: The Secret World of China’s Communist Rulers* (New York: Harper Collins, 2010).

components coming under the control of foreign entities. This seems particularly applicable in the telecommunications industry, as Chinese companies continue systematically to acquire significant holdings in prominent global and U.S. telecommunications and information technology companies.<sup>12</sup>

Some analysts also believe that the government of the People's Republic of China is interested in acquiring meaningful stakes in companies that have significant influence in other national governments. This particularly applies to companies that also have significant investment or stakes in China's markets (such as technology and telecommunications equipment providers). Influencing the behavior of multinational companies with this form of leverage may be one logical way for the Chinese government to seek to protect its interests in a global context.<sup>13</sup>

### **Telecommunications as a "Strategic" Industry in China**

Telecommunications is one of seven "strategic industries" in which the Chinese government seeks to maintain "absolute control" (meaning over 50 percent ownership). The government also wishes to maintain a dominant presence in six "heavyweight" industries through regulation and government control. These industries are as follows:<sup>14</sup>

#### **Strategic Industries:**

- (1) Armaments
- (2) Power Generation and Distribution
- (3) Oil and Petrochemicals
- (4) Telecommunications
- (5) Coal
- (6) Civil Aviation
- (7) Shipping

#### **Heavyweight Industries:**

- (1) Machinery
- (2) Automobiles
- (3) Information Technology
- (4) Construction
- (5) Iron and Steel
- (6) Nonferrous Metals

The Chinese government has actively sought to cultivate state-controlled "national champions" companies in these sectors.<sup>15</sup> It has also offered state support to companies in its "strategic" and "heavyweight" industries, such as land and energy subsidies, favorable tax policies, and below-market interest rate loans issued from state banks with reduced or no expectation of repayment.<sup>16</sup> The PRC's "national champions" are a centerpiece of the government's "going out" strategy to cultivate state-controlled firms capable of competing in the international marketplace.<sup>17</sup>

<sup>12</sup> For examples of overseas acquisitions made, or sought, in 2010 by Chinese telecommunications companies, see (1) A pending purchase of Nigerian Telecom (Nitel) by China Unicom, in "Rumor: China Unicom Leads Nitel Acquisition," C114.com, October 16, 2010. <http://www.cn-c114.net/583/a550716.html>; and (2) the statement that China Telecom "will 'closely examine' opportunities for overseas acquisitions" as it moves into markets such as that of India, in Peter Stein and Yun-Hee Kim, "China Firm Eyes India," *Wall Street Journal*, September 28, 2010.

<sup>13</sup> Wayne M. Morrison and Marc Labonte, "China's Holdings of U.S. Securities: Implications for the U.S. Economy," (Washington, DC: Congressional Research Service, CRS-7, January 9, 2008).

<sup>14</sup> U.S.-China Economic and Security Review Commission, *Annual Report to Congress 2009* (Washington, DC: U.S. Government Printing Office, November 2009), p. 59. For the underlying source, see U.S.-China Economic and Security Review Commission, *Hearing on the Extent of the Government's Control of China's Economy, and Implications for the United States*, written testimony of Barry Naughton and George Haley, May 24, 2007.

<sup>15</sup> U.S.-China Economic and Security Review Commission, *Hearing on the Extent of the Government's Control of China's Economy, and Implications for the United States*, written testimony of Barry Naughton, May 24, 2007.

<sup>16</sup> U.S.-China Economic and Security Review Commission, *Annual Report to Congress 2009* (Washington, DC: U.S. Government Printing Office, November 2009), pp. 57-65.

<sup>17</sup> Accenture Consulting, "China Spreads Its Wings: Chinese Companies Go Global," 2007. [http://www.accenture.com/NR/rdonlyres/1F79806F-E076-4CD7-8B74-3BAFBAC58943/0/6341\\_chn\\_spreads\\_wings\\_final8.pdf](http://www.accenture.com/NR/rdonlyres/1F79806F-E076-4CD7-8B74-3BAFBAC58943/0/6341_chn_spreads_wings_final8.pdf)

Some large Chinese companies, such as the telecommunications firm Huawei and the computer manufacturer Lenovo, retain a “hybrid” structure as “national champions” that receive favorable treatment through close government ties while also enjoying the freedom to operate as private companies domestically and abroad without bearing the onus of government ties.<sup>18</sup> (See more on the background of Huawei on pp. 13-18, of ZTE on pp. 21-23, and of Lenovo on pp. 66-68).

### **Global Telecommunications Market Trends in 2008-2009**

The merger and acquisition (M&A) environment in the telecommunications industry is active, and there are fast-growing markets worldwide, particularly in the developing world, Europe, and the United States.<sup>19</sup> More deals between U.S. and Chinese entities are likely to appear in the future: China has money to spend, telecommunications is a core strategic industry of interest, and a huge percentage of telecom equipment is manufactured in China. Therefore, it is reasonable to expect to see a global presence for Chinese companies as an acquirer and consolidator of assets and as a developer of new market opportunities.

Due to the global nature of communications and information markets, business trends in telecommunications are very often going to flow in a global context, with business transactions occurring within national contexts representing subtrends that will still seek centers of gravity created by global trends. M&A activity in telecommunications tends to fall into two categories:

- A. Consolidations within mature markets.
- B. Growth opportunities in emerging markets.

Some telecommunications businesses willing to risk emerging market hazards may wait for an emerging market's conditions to conform to favorable metrics before attempting to develop a telecom prospect. Early infrastructure developers/service providers may at times wait for opportunities that will allow them to time early risks and will have few intentions of remaining in that particular developing market long term. Their business objectives may be to remain in an emerging market only long enough to develop service areas sufficiently for them to be attractive M&A targets by more long-term-oriented operators.

Following the panic in financial markets in 2008-2009, large telecommunications industry players have been waiting for greater economic distress to push M&A costs down to bargain-basement prices, but this did not happen as fully as had been anticipated. The year 2009 was characterized by “prospecting” in the telecom industry. Few actual mergers & acquisitions deals occurred, however, as deeply discounted bargains did not materialize as much as might have been expected or hoped for by prospective buyers. Future trends are likely to see a continual and marked increase in bids and sales as prospective buyers come back to bargaining tables with more realistic expectations.<sup>20</sup>

Lingering economic distress will undoubtedly push some vulnerable firms past the tipping point; therefore, the future telecom marketplace, both globally and in the United States, should see

<sup>18</sup> Geoff Dyer and Richard McGregor, “China's Champions: Why State Ownership Is No Longer a Dead Hand,” *Financial Times*, March 16, 2008.

<sup>19</sup> Within the United States, a great deal of new focus is to be found in rural markets, in particular.

<sup>20</sup> “Up to Bat Again – Will it be Strike Two for Huawei in the U.S.?” Bill Newman Inbound Acquisitions and Investments Blog, quoting *Financial Times* article, April 16, 2010.



many M&A deals. Globally, telecom businesses are becoming much more tough-minded, are holding their most profitable business units back from M&A's as they are best able to do so, and are disposing of underperforming business units much faster than might have been the case in the past.

## CHINESE TELECOM COMPANIES ENTER THE U.S. MARKET

### China: Developer and Provider within China, and Global Exporter of Wireless and Next Generation Networks

As wireless networking comes under cost pressures in the United States, more incentive has been created in the U.S. market to consider alternative vendors. By keeping costs down and moving ahead to next generation technologies, Chinese manufacturers have taken much of the initiative in developing the Worldwide Interoperability for Microwave Access (WiMAX)<sup>21</sup> and LTE (Long-Term Evolution) standards. As one example of ways in which these companies are creating more opportunities for themselves through innovation and partnerships, press reports have indicated that Huawei will provide equipment to Leap Wireless (Cricket) to support their wireless initiatives.<sup>22</sup>

Meanwhile, the United States has been slower to respond to demands for newer technology standards. U.S. wireless providers are under enormous cost pressures while also being subject to increasing regulatory pressures to open their networks and create network and device interoperability. This comes on the heels of paying off expensive spectrum auctions purchased in efforts to create more contiguous networks.<sup>23</sup> The U.S. market has also been more difficult to penetrate due to security and regulatory concerns, such as those raised by the Committee on Foreign Investment in the United States when Huawei attempted to buy equipment manufacturer 3Com in 2008.<sup>24</sup> *(For more on these issues, see pp. 28-30.)*

China is poised to become the world's number one end-to-end supplier of telecom, cable, and mobile wireless equipment, much like AT&T and IBM dominated technology sectors in the past.<sup>25</sup> The global financial crisis pushed many telecom companies into severely vulnerable positions, allowing their market shares to be acquired easily by buyers as price competition increased globally. As wireless networking comes under cost pressures in the United States, more incentive has been created in the U.S. market to consider alternative vendors to remain competitive. Initially, many Chinese products were found only in certain parts of a telecom

<sup>21</sup> WiMAX (Worldwide Interoperability for Microwave Access), "What is WiMAX," WiMAX.com. <http://www.wimax.com/education>.

<sup>22</sup> "Huawei Supplies Leap Wireless," LightReading.com, August 15, 2006. [http://www.lightreading.com/document.asp?doc\\_id=101446](http://www.lightreading.com/document.asp?doc_id=101446).

<sup>23</sup> A spectrum auction is "a process whereby a government uses an auction system to sell the rights to transmit signals over specific electromagnetic wavelengths." See "Spectrum Auction," *Wikipedia.org*. [http://en.wikipedia.org/wiki/Spectrum\\_auction](http://en.wikipedia.org/wiki/Spectrum_auction). A major spectrum auction for the 700 megahertz frequency band, of interest to wireless providers, was held in January 2008. See Federal Communications Commission Press Release, "Auction of 700 MHz Band Licenses Scheduled for January 16, 2008 / Comment Sought on Competitive Bidding Procedures for Auction 73," August 17, 2007. [http://fjallfoss.fcc.gov/edocs\\_public/attachmatch/DA-07-3415A1.pdf](http://fjallfoss.fcc.gov/edocs_public/attachmatch/DA-07-3415A1.pdf)

<sup>24</sup> Bruce Einhorn, "Huawei's Business Deal Flops," *Business Week*, February 21, 2008.

<sup>25</sup> XChange Magazine, "Huawei: 'It' Vendor 2010," January 8, 2010, notes Huawei sales may be \$36 billion in 2010 and take the place as the number one infrastructure supplier as it closes in on Ericsson. The world strength of global telecom deals by all Chinese firms, including ZTE, and scores of other companies may move China quickly to the number one slot across all categories.



network, but now Chinese companies rapidly are becoming the global, integral, “end-to-end” solution for telecom networks around the world.<sup>26</sup>

## HUAWEI TECHNOLOGIES



Huawei Technologies [*Shenzhen Huawei Jishu Youxian Gongsi* / 深圳华为技术有限公司] is a high-technology enterprise that specializes in research and development (R&D), production, and marketing of communications equipment and providing customized network solutions for telecom carriers. Huawei has emerged as one of the largest global manufacturers of telecommunications equipment, particularly in the wireless market segment.

The dramatic growth of companies like Huawei is an extraordinary accomplishment.<sup>27</sup> By 2007, Huawei served 35 of the top 50 telecom operators and was investing 10 percent of revenue back into R&D each year.<sup>28</sup> By the end of 2009, Huawei was the world's second-largest telecom provider, ranking only behind the Swedish firm Ericsson.<sup>29</sup> The rise of Huawei has been so dramatic that some industry analysts have suspected "unsustainably low prices and government export assistance" as key to the company's rapid expansion.<sup>30</sup> (See text box below.) Others, however, would identify the key to the company's successes as its "sound business strategies," to include an early focus on underserved markets in rural China, "to which multinational titans did not even bother to seek access."<sup>31</sup>

### **European Controversies over Alleged PRC State Support to Huawei**

Allegations of PRC state subsidies to Huawei raised controversy in Europe in summer 2010, with both workers' unions and Option SA, a Belgian manufacturer of wireless wide-area network (WWAN) modems,<sup>32</sup> making complaints that Chinese government assistance to Huawei and ZTE allowed the Chinese companies to compete with an unfair pricing advantage.<sup>33</sup> According to Option SA's complaint, the companies received beneficial financing arrangements from PRC state banks, to include Huawei signing:

*"...a cooperation agreement in September 2009 with the China Development Bank worth \$30 billion—above its 2009 revenue of \$22 billion and the sort of funding line the complaint said*

<sup>26</sup> *China Technology and Telecom Sector M&A Report 1<sup>st</sup> Quarter 2009*, [www.cowenlatitude.com/document/09q1\\_china\\_tech\\_ma.pdf](http://www.cowenlatitude.com/document/09q1_china_tech_ma.pdf).

<sup>27</sup> Annual Reports 2008, Cisco, Huawei, Motorola (Securities and Exchange Commission [SEC] 10K filings).

<sup>28</sup> "China's Technological Challenger", *New Zealand Herald*, March 15, 2007.

<sup>29</sup> Kevin O'Brien, "Upstart Chinese Telecom Company Rattles Industry as it Rises to No. 2", *New York Times*, November 29, 2009.

<sup>30</sup> "The Huawei Way", *Newsweek*, January 15, 2006.

<sup>31</sup> Cheng Li, "China's Telecom Industry on the Move: Domestic Competition, Global Ambition, and Leadership Transition", *China Leadership Monitor*, No. 19 (2006).

<sup>32</sup> Jonathan Stearns, "China Modem Makers May Face EU Anti-Subsidy Tariff," *Bloomberg*, September 16, 2010.

<sup>33</sup> Matthew Dalton, "Europe Raises Cry Over China Tech Exports," *Wall Street Journal*, October 5, 2010.

wouldn't be extended in a market economy... ZTE, with 2009 revenue of \$8.4 billion, got a \$15 billion credit line from the bank in March 2009. The complaint says these and other financing deals were provided with favorable terms, including three-year moratoriums on interest payments... Option said such terms have allowed Chinese companies to sell wireless modems in Europe for as little as €20 (\$27) a device. Option would have to charge more than twice that much, it says, to earn a profit of 10% to 15% on its sales."<sup>34</sup>

In response to these complaints, in September 2010 the European Commission indicated that it would conduct an inquiry into whether Chinese-manufactured modems are "being subsidized and whether this subsidization has caused injury to the Union industry" and also ordered customs authorities to begin registering European Union (EU) imports of Chinese-manufactured WWAN modems as a preparatory action in the event that countervailing duties might be applied in the future.<sup>35</sup>



*Huawei Technologies headquarters, in the Shenzhen Technology Development Park in Shenzhen, China (Source: Associated Press.)*

Although Huawei is headquartered in China, it has established more than 100 international branch offices and 17 R&D facilities around the world. In addition to domestic centers in Shenzhen, Shanghai, Beijing, Nanjing, Xi'an, Chengdu, and Wuhan, Huawei has also established research facilities in Stockholm, Sweden; Dallas and Silicon Valley, United States; Bangalore, India; Ferbane in Offaly, Ireland; Moscow, Russia; Jakarta, Indonesia; and the Netherlands.<sup>36</sup> Its presence in the North American market has increased rapidly in recent years: From 2006 to 2010, Huawei has grown from 180 employees to more than 1,000.<sup>37</sup>

<sup>34</sup> Matthew Dalton, "Europe Raises Cry Over China Tech Exports," *Wall Street Journal*, October 5, 2010.

<sup>35</sup> Jonathan Stearns, "China Modem Makers May Face EU Anti-Subsidy Tariff," *Bloomberg*, September 16, 2010.

<sup>36</sup> Huawei Technologies Co., Ltd., the largest networking and telecommunications equipment supplier in the People's Republic of China. <http://www.huawei.com>.

<sup>37</sup> *Huawei Technologies (North America Region) Corporate Social Responsibility Report 2009-2010*, p. 19. <http://www.huawei.com/na/en>.

**Figure 1: Huawei Technologies Offices in North America**

Source: Huawei Technologies (North America Region),  
Corporate Social Responsibility Report 2009-2010, p. 19. <http://www.huawei.com/na/en>.

Huawei operates as an employee-owned company; however, its management structure is opaque, and media sources have raised questions about the true nature of the company's ownership. Huawei Technologies Co., Ltd., is itself a wholly owned subsidiary of Shenzhen Huawei Investment & Holding Co., Ltd. The company's employee shareholding program is managed by a shareholder body called the Union of Shenzhen Huawei Investment Holdings Co., Ltd., whose governing board is made up entirely of senior company officials. The company's shares are not freely traded but rather allocated to employees annually as incentives. Only employees within China can hold shares, and they must sell them back to the company if they leave Huawei's employ.<sup>38</sup>

## Controversies Surrounding the Activities of Huawei

### Allegations of Intellectual Property Piracy

Although Huawei has emerged as a highly successful company, it has been troubled by controversy over the years. Huawei has been accused in the past by its international competitors of extensive piracy and intellectual property theft: In one example, Cisco Systems, Inc., filed suit against Huawei and its American subsidiaries in 2003, alleging "wholesale infringement of Cisco's copyrights and misappropriation of Cisco's trade secrets... [to include] blatant and systematic copying of Cisco's router technology... [and] theft of Cisco's intellectual property by misappropriating and copying Cisco's source code, duplicating Cisco's user interface, and plagiarizing extensively from Cisco's user manuals."<sup>39</sup> The lawsuit was dropped in July 2004 after Huawei pledged to modify aspects of its computer products line.<sup>40</sup>

<sup>38</sup> Juha Saarinen, "Analysis: Who Really Owns Huawei?" *ITNews (Australia)*, May 28, 2010.

<http://www.itnews.com.au/News/175946.analysis-who-really-owns-huawei.aspx>.

<sup>39</sup> United States District Court for the Eastern District of Texas (Marshall Division), Civil Action #2:03-CV-027 TJW, *Cisco Systems, Inc., and Cisco Technology, Inc. (Plaintiffs) vs. Huawei Technologies Co., Ltd., Huawei America, Inc., and Futurewei Technologies, Inc. (Defendants)*, "Cisco's Motion for Preliminary Injunction," dated February 5, 2003. [http://newsroom.cisco.com/dlls/Cisco\\_Mot\\_for\\_PI.pdf](http://newsroom.cisco.com/dlls/Cisco_Mot_for_PI.pdf).

<sup>40</sup> Cisco, Inc., press release, "Cisco Comments on Completion of Lawsuit Against Huawei," July 28, 2004. [http://newsroom.cisco.com/dlls/2004/hd\\_072804.html](http://newsroom.cisco.com/dlls/2004/hd_072804.html).

*Allegations of Threats to Communications Security*

Huawei has also been the subject of questions regarding the nature of the company's management and its alleged close ties to the Chinese military. Some analysts have challenged the assertion that Huawei is an actor operating independently of the Chinese government. Noting that "both the [Chinese] government and the military tout Huawei as a national champion," an analysis by the RAND Corporation states that:

*"...one does not need to dig too deeply to discover that [many Chinese information technology and telecommunications firms] are the public face for, sprang from, or are significantly engaged in joint research with state research institutes under the Ministry of Information Industry, defense-industrial corporations, or the military... Huawei was founded in 1988 by Ren Zhengfei, a former director of the PLA [People's Liberation Army] General Staff Department's Information Engineering Academy, which is responsible for telecom research for the Chinese military. Huawei maintains deep ties with the Chinese military, which serves a multi-faceted role as an important customer, as well as Huawei's political patron and research and development partner."<sup>41</sup>*



*Huawei founder Ren Zhengfei*  
Source: Google Images.

Aside from the controversy in the United States over the abortive effort by Huawei to purchase 3Com (see pp. 28-30), media reports from other countries have also indicated concerns on the part of government security agencies in regard to Huawei's activities. British intelligence officials have reportedly warned government ministers of potential infrastructure threats emerging from communications equipment provided by Huawei to networks operated by British Telecom.<sup>42</sup> In Australia, intelligence officials have reportedly investigated alleged links between Chinese military officials and employees of Huawei's Australian offices.<sup>43</sup> In May 2010, Indian press reports revealed concern among intelligence officials about Huawei's activities in India, and the Indian communications ministry has placed limitations on the role of Huawei in India's communications networks.<sup>44</sup> In Taiwan, representatives of the opposition Democratic Progressive Party have also expressed concern over the expansion of Huawei into the island's telecom and network equipment markets, identifying this as a threat to Taiwan's security.<sup>45</sup>

<sup>41</sup> Evan Medeiros et al., *A New Direction for China's Defense Industry* (Arlington, VA: RAND Corporation, 2005), pp. 217-218.

<sup>42</sup> See Michael Smith, "Spy Chiefs Fear Chinese Cyber Attack," *Sunday Times (London)*, March 29, 2009; and Alastair Jamieson, "Britain Could Be Shut Down by Hackers from China, Intelligence Experts Warn," *Telegraph (UK)*, March 29, 2009.

<sup>43</sup> Cameron Stewart, "Huawei in ASIO's Net," *Australian*, September 5, 2009.

<sup>44</sup> Bharti Jain, "Huawei Part of Chinese Spy Network, Says R&AW," *Economic Times (India)*, May 7, 2010.

<sup>45</sup> "Taiwan – Opposition Voices Concern over Huawei's Inroads," Open Source Center Report, June 10, 2010.



Huawei company officials have steadfastly rejected all such alleged security concerns related to the company's operations. Huawei officials have asserted the private nature of the company, calling it a Chinese embodiment of the "American Dream" and stressing the positive advantages of job creation at its facilities in the United States.<sup>46</sup> They also continue to maintain that "Huawei is privately held and 100 per cent owned by its employees" and that "[n]o other organizations, including the government, army or business hold stakes in Huawei."<sup>47</sup>

### Allegations of Industrial Espionage

In July 2010, Motorola Inc. filed suit against Huawei in the U.S. District Court for the Northern District of Illinois, alleging a multiyear plot by Huawei's senior management to steal proprietary trade secrets from Motorola. The case had been in the making for some time but reportedly had been placed on hold while Motorola considered selling its network infrastructure business to Huawei.<sup>48</sup> However, on the heels of the July 19, 2010, announcement that Motorola was selling the majority of its wireless network infrastructure assets to Nokia Siemens Networks for \$1.2 billion USD,<sup>49</sup> there was no longer any commercial incentive for Motorola to refrain from filing the lawsuit.

The lawsuit alleges that multiple Motorola employees – with two identified by name, Shaowei Pan and Hanjuan Jin – colluded with representatives of Huawei, including Huawei's founder Ren Zhengfei, to steal proprietary technology and pass it to Huawei. The alleged vehicle for some of these transfers was Lemko, a company founded by Shaowei Pan and other Motorola employees in 2002 while they were still employed by Motorola.<sup>50</sup> The matters in dispute in the civil case follow from a criminal case that first came to light in February 2007, when, according to allegations by U.S. government investigators:

*"...one day after quitting Motorola, [Ms. Hanjuan] Jin was stopped at O'Hare airport with over 1,000 Motorola documents in her possession, both in hard copy and electronic format. A review of Motorola computer records showed that [Ms.] Jin accessed a large number of Motorola documents late at night. At the time she was stopped, Jin was traveling on a one-way ticket to China... [the charges against her] are based on evidence that Jin intended that the trade secrets she stole from Motorola would benefit the Chinese military."*<sup>51</sup>

Mr. Pan allegedly held multiple meetings with Huawei officials from 2001 onwards, discussing Motorola's operations in international markets and his plans to establish Lemko as a company "independent of Motorola, Inc." Among the technology allegedly transferred was information about a Motorola base station – labeled "Motorola Confidential Property" – which Mr. Pan allegedly e-mailed to Huawei executives from his personal e-mail account in March 2003.<sup>52</sup>

<sup>46</sup> Statements made by Huawei representatives to staff of the U.S.-China Economic and Security Review Commission, July 7, 2009.

<sup>47</sup> Renai Lemay, "Huawei Denies 'Ludicrous' Espionage Claims," *ZDNet News Online*, December 18, 2008. <http://www.zdnet.com.au/huawei-denies-ludicrous-espionage-claims-339293911.htm>.

<sup>48</sup> Loretta Chao, "Motorola Suit Poses Challenges to Huawei's Success," *Wall Street Journal*, July 23, 2010.

<sup>49</sup> Motorola Inc. press release, "Nokia Siemens Networks to Acquire Certain Wireless Network Infrastructure Assets of Motorola for US \$1.2 Billion," July 19, 2010.

<http://mediacenter.motorola.com/content/detail.aspx?ReleaseID=13055&NewsAreaId=2>.

<sup>50</sup> Jamil Anderlini, "Motorola Claims Espionage in Huawei Lawsuit," *Financial Times*, July 22, 2010.

<sup>51</sup> U.S. Department of Justice, "Recent Espionage-Related Prosecutions Involving China," July 20, 2010.

<http://media.washingtonpost.com/wp-srv/politics/documents/spyprosecutions072010.pdf>.

<sup>52</sup> Christopher Rhoads, "Motorola Claims Huawei Plot," *Wall Street Journal*, July 22, 2010.

Representatives of both Huawei and Lemko have denied the allegations, and the case is unadjudicated as of the writing of this report.

### Concerns about Huawei Expressed by Members of the U.S. Congress

Members of the U.S. Congress have weighed in on some of the controversies surrounding Huawei and have expressed concerns regarding the potential national security impacts of Huawei's efforts to purchase stakes in U.S. telecommunications companies. As one example, in October 2007 Representative Ileana Ros-Lehtinen (Florida, 18<sup>th</sup> District), along with 12 co-sponsors, introduced a draft House resolution (H.Res.730) that would have expressed opposition to Huawei's moves to acquire a stake in 3Com.<sup>53</sup> *(For further details on the abortive 3Com / Huawei deal, see pp. 28-30.)*

More recently, in August 2010 eight Members of the U.S. Senate (Sen. Jon Kyl, Arizona; Sen. Christopher Bond, Missouri; Sen. Richard Shelby, Alabama; Sen. James Inhofe, Oklahoma; Sen. Jim Bunning, Kentucky; Sen. Jeff Sessions, Alabama; Sen. Richard Burr, North Carolina; and Sen. Susan Collins, Maine) addressed a letter to senior officials of the Obama Administration (Secretary of the Treasury Timothy Geithner; Secretary of Commerce Gary Locke; Director of National Intelligence James Clapper; and Administrator of General Services Martha Johnson) that expressed concern over a pending deal by Huawei to supply equipment to Sprint Nextel (see following page). The letter expressed concern that "Huawei's position as a supplier of Sprint Nextel could create substantial risk for U.S. companies and possibly undermine U.S. national security." The letter further offered a list of several questions about Huawei and its business activities and requested that the addressees provide responses to these questions.<sup>54</sup>

<sup>53</sup> H.Res.730, "Expressing the Sense of the House of Representatives Regarding the Planned Acquisition of a Minority Interest in 3Com by Affiliates of Huawei," 110<sup>th</sup> Cong., 1<sup>st</sup> sess., introduced October 10, 2007. Text available at <http://thomas.loc.gov/cgi-bin/query/z?c110:H.RES.730>.

<sup>54</sup> Letter from Sen. Jon Kyl, Arizona, Sen. Christopher Bond, Missouri, Sen. Richard Shelby, Alabama, Sen. James Inhofe, Oklahoma, Sen. Jim Bunning, Kentucky, Sen. Jeff Sessions, Alabama, Sen. Richard Burr, North Carolina, and Sen. Susan Collins, Maine, addressed to Secretary of the Treasury Timothy Geithner, Secretary of Commerce Gary Locke, Director of National Intelligence James Clapper, and Administrator of General Services Martha Johnson, dated August 18, 2010. The eleven specific questions directed to the addressees are as follows:

- Does the United States government have unclassified information regarding Huawei's affiliation, if any, with the PLA? What does that information say about the affiliation/relationship, e.g., what control, if any, is exerted by the PLA on Huawei's operations?
- Is there any concern that Huawei, if it gained any measure of control over a U.S. contractor involved with sensitive U.S. government contracts, would present a national security threat for technology leakage or enhanced espionage against the United States? Please provide an unclassified response.
- Is the U.S. Treasury Department discussing or negotiating a deal to allow Huawei to acquire or invest in U.S. companies? What is the status of the negotiations? Will you agree to provide a briefing to Senators and their staffs on the present status?
- Has the Treasury Department included members of the intelligence community (IC) in its negotiations, if any, with Huawei? If yes, does the IC have a veto over any final negotiated product? Will you share with us and our staffs any IC analysis concerning the potential threat of Huawei obtaining any measure of control over a U.S. firm with sensitive contracts?
- What contracts with the Department of Defense (DOD) and the IC does Sprint Nextel have?
- Does Huawei currently supply companies with U.S. government contracts? If so, what are they?
- Have any goods provided to a U.S. government supplier by Huawei ever been found to contain suspect technology, such as intentional defects or "back doors" allowing remote entry?
- Please describe what, if any, a priori security review the General Services Administration conducts on technology (software or hardware) that the United States government purchases from overseas suppliers.
- Have U.S.-based employees of Huawei been granted security clearances by the U.S. government for access to classified information?

## Recent Unconsummated Huawei Deals, and Potential Huawei Deals on the Horizon

Huawei emerged into the spotlight of telecom industry analysts once again in spring and summer 2010, with speculation of potential new deals by Huawei in the U.S. telecom sector. In April 2010, an article in the *Financial Times* indicated that Huawei might be preparing a bid for the network infrastructure unit of Motorola, the U.S. mobile phone manufacturer. In an apparent attempt to head off the concerns surrounding the abortive 3Com deal, Huawei indicated that it would consider a “mitigation agreement,” which would “show its willingness to co-operate with the US, [as] Alcatel of France did when it bought Lucent in 2006.”<sup>55</sup> This came only two months after Motorola announced that it would be restructuring itself in 2011 into two separate companies—one that would operate its network infrastructure business, and one to handle its mobile phone and television set-top box business, with Huawei reportedly to pursue the former.<sup>56</sup> However, speculation on any such deal was ended in July 2010, when Motorola announced the purchase of its network infrastructure business by Nokia Siemens and filed suit against Huawei for alleged industrial espionage (*see text box on pp. 17-18*).

It was also reported in spring 2010 that Huawei might be a potential suitor to buy into Harbinger Capital’s planned Long-Term Evolution (LTE) network, which is likely to become a 4G (4<sup>th</sup> generation) technology standard.<sup>57</sup> (*See more on Huawei and LTE technology issues on pp. 45-46.*) Speculative reports have indicated that the hedge fund Harbinger Capital, which owns spectrum rights in the United States, could be looking for the cost efficiencies that Huawei can offer.<sup>58</sup> Huawei’s known desire to expand in the smart phone business could also be satisfied by Harbinger’s potentially expansive technology in a developed market.

In late July 2010, Huawei lost out in a bid to acquire the firm 2Wire. 2Wire, a U.S.-based broadband technology firm, was acquired by the British firm Pace for a reported \$475 million, with the buyer reportedly interested in 2Wire’s business in the residential broadband services market.<sup>59</sup> Huawei had reportedly offered a higher bid than Pace, but concerns over its ability to receive approval for the deal from the Committee on Foreign Investment in the United States (CFIUS) played a role in its failure to secure the deal.<sup>60</sup> (*For more on the committee and its review process, see pp. 30-33.*)

- 
- Please describe in detail any export licenses currently in review, or approved in the past five years, between any U.S. firm and Huawei.
  - Has the Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), or National Security Agency (NSA) communicated with foreign intelligence agencies regarding their concerns, and vice versa, about Huawei’s operations, affiliations and relationships?

<sup>55</sup> Stephanie Kirchgaessner, “Huawei Tries To Calm US Fears,” *Financial Times*, April 4, 2010. <http://www.ft.com/cms/s/2/44e5e210-400d-11df-8d23-00144feabdc>.

<sup>56</sup> Trading Markets, “Huawei Emerges As Potential Buyer of Motorola’s Mobile Network, Report,” March 17, 2010. [http://www.tradingmarkets.com/news/stock-alert/mot\\_huawei-emerges-as-potential-buyer-of-motorola-s-mobile-network-report-851479.html](http://www.tradingmarkets.com/news/stock-alert/mot_huawei-emerges-as-potential-buyer-of-motorola-s-mobile-network-report-851479.html).

<sup>57</sup> C114, “Harbinger Pioneers Open-Access LTE Network US,” April 1, 2010. <http://www.cn-c114.net/575/a495001.html>.

<sup>58</sup> Stephanie Kirchgaessner, “Security Concerns Hold Back Huawei,” *Financial Times*, July 8, 2010. <http://www.ft.com/cms/s/0/6fd9f072-8aba-11df-8e17-00144feab49a.html>.

<sup>59</sup> Paul Sandle, “Pace Buys U.S. Broadband Co 2Wire for \$475 Mln,” Reuters, July 26, 2010. <http://www.reuters.com/article/idUSTRE66P1UL20100726>.

<sup>60</sup> Stephanie Kirchgaessner and Helen Thomas, “US Divided on How to Tackle Huawei,” *Financial Times*, July 29, 2010.



Finally, in what arguably has emerged as Huawei's most high-profile deal of 2010, media reports first disclosed in July 2010 that Huawei was bidding to sell equipment for an expansion of the wireless broadband network of Sprint Nextel, America's third-largest mobile operator.<sup>61</sup> Huawei's leading partner in this proposed deal is Amerilink Telecom Corporation, a company staffed largely by former employees of Sprint Nextel. To date, Amerilink is acting primarily as a distributor for equipment made by Huawei and as a consultant for Huawei's efforts further to penetrate the U.S. market.<sup>62</sup> These efforts have been the subject of controversy: In August 2010, eight Members of the U.S. Senate addressed a letter to senior officials of the Obama Administration that expressed concern over the pending deal by Huawei to supply equipment to Sprint Nextel (*see text box on page 18*).<sup>63</sup>

A trio of prominent public figures is associated with Amerilink: its founder, William Owens, is a retired U.S. Navy admiral and a former vice chairman of the U.S. Joint Chiefs of Staff;<sup>64</sup> and in 2010, the company recruited former U.S. House of Representatives Democratic Leader Richard Gephardt and former World Bank President James Wolfensohn to serve as members of its board of directors.<sup>65</sup> Amerilink representatives have been active in engaging U.S. officials about the proposed deal with Sprint Nextel; they reportedly have also sought to mitigate concerns about Huawei's hardware by offering that Amerilink certify it for network security purposes.<sup>66</sup>

Security concerns expressed by government officials are believed to be a factor in Sprint Nextel's decision in November 2010 to exclude Huawei Technologies Ltd. and ZTE Corporation from final consideration as equipment suppliers for upgrades to its cellular networks, a deal worth billions of dollars.<sup>67</sup>

#### **Concerns Regarding Potential Network Penetration by PRC Intelligence Agencies**

The *Washington Post* has reported that representatives of the National Security Agency (NSA) contacted senior executives of AT&T late in 2009 to warn them against purchasing equipment from Huawei. According to the *Post* article, "The NSA called AT&T because of fears that China's intelligence agencies could insert digital trapdoors into Huawei's technology that would serve as secret listening posts in the U.S. communications network."<sup>68</sup> At the time, AT&T was taking bids from potential suppliers for its planned next-generation LTE phone network. AT&T has not made any public comment about the reported messages from the NSA, but it did announce in

<sup>61</sup> Paul Taylor and Stephanie Kirchgaessner, "Huawei in Drive to Land Big US Deal," *Financial Times*, July 8, 2010; and Reuters, "China's Huawei Bids for Sprint Equipment Deal: Report," July 8, 2010.

<http://www.reuters.com/article/idUSTRE6680E920100709>.

<sup>62</sup> Loretta Chao and Paul Ziobro, "Huawei Enlists an Ex-Sprint Team," *Wall Street Journal*, August 24, 2010.

<sup>63</sup> Letter from Sen. Jon Kyl, Arizona, Sen. Christopher Bond, Missouri, Sen. Richard Shelby, Alabama, Sen. James Inhofe, Oklahoma, Sen. Jim Bunning, Kentucky, Sen. Jeff Sessions, Alabama, Sen. Richard Burr, North Carolina, and Sen. Susan Collins, Maine, addressed to Secretary of the Treasury Timothy Geithner, Secretary of Commerce Gary Locke, Director of National Intelligence James Clapper, and Administrator of General Services Martha Johnson, dated August 18, 2010.

<sup>64</sup> Team." *Prometheus*. <http://prometheusasia.com/team.html>; and Loretta Chao and Paul Ziobro, "Huawei Enlists an Ex-Sprint Team," *Wall Street Journal*, August 24, 2010.

<sup>65</sup> Spencer Ante and Shayndi Raice, "Dignitaries Come on Board to Ease Huawei Into U.S.," *Wall Street Journal*, September 21, 2010.

<sup>66</sup> John Pomfret, "Between U.S. and China, a Trust Gap," *Washington Post*, October 8, 2010.

<sup>67</sup> Joann S. Lublin and Shayndi Raice, "Security Fears Kill Chinese Bid in U.S.," *Wall Street Journal*, November 5, 2010.

<sup>68</sup> John Pomfret, "Between U.S. and China, a Trust Gap," *Washington Post*, October 8, 2010.

February 2010 that it had selected Ericsson and Alcatel-Lucent as its equipment and service suppliers for the network upgrade.<sup>69</sup>

Assuming that the account of the NSA warning is true, the PRC intelligence entity of greatest concern would likely be the Third Department of the People's Liberation Army General Staff Department, China's leading signals intelligence agency. The Third Department is reportedly the largest of all of China's intelligence services,<sup>70</sup> offering the PRC:

*"by far, the most extensive SIGINT capability of any nation in the Asia-Pacific region. The Chinese operate several dozen SIGINT ground stations deployed throughout China. There they monitor signals from Russia, Taiwan, Japan, South Korea, India, and Southeast Asia. Signals from U.S. military units located in the region are of significant interest to these monitoring stations, and a large SIGINT facility at Hainan Island is principally concerned with monitoring U.S. naval activities in the South China Sea."*<sup>71</sup>

Aside from the collection of communications information, the Third Department also likely bears primary responsibility within the PLA for computer network exploitation (i.e., "cyber espionage") operations. The Third Department is also assessed to have a complementary relationship with the Fourth Department of the PLA General Staff Department, which takes a leading role in computer network attack operations.<sup>72</sup> *(For further discussion of PRC intelligence agencies and their functions, see the Commission's 2009 Annual Report to Congress, chapter 2, section 3, "China's Human Espionage Activities that Target the United States, and the Resulting impacts on U.S. National Security.")*

## ZTE CORPORATION



ZTE Company Logo

<sup>69</sup> Ruth Bender and Gustav Sandstrom, "2nd UPDATE: Ericsson, Alcatel Get 4G Network Deal From AT&T," *Foxbusiness.com*, February 10, 2010. <http://www.foxbusiness.com/story/markets/industries/telecom/nd-update-ericsson-alcatel-g-network-deal-att/>.

<sup>70</sup> U.S.-China Economic and Security Review Commission, *Annual Report to Congress 2009* (Washington, DC: U.S. Government Printing Office, November 2009), p. 153. A firm open-source estimate on the number of personnel in the Third Department is not available. For two sources, see Howard DeVore, *China's Intelligence and Internal Security Forces* (Alexandria, VA: Jane's Information Group, 1999), p. 48; and Nicholas Eftimiades, *Chinese Intelligence Operations* (Annapolis, MD: Naval Institute Press, 1994), p. 46. A figure of 20,000 personnel is provided by Mr. DeVore. A figure of 130,000 is provided in Kan Chung-kuo, "Intelligence Agencies Exist in Great Numbers, Spies Are Present Everywhere; China's Major Intelligence Departments Fully Exposed," *'Chien Shao'* (Frontline), January 1, 2006. OSC ID: CPP20060110510011. [www.open-source.gov](http://www.open-source.gov).

<sup>71</sup> Interagency OPSEC Support Staff, *Intelligence Threat Handbook* (2004), p.75. <http://www.fas.org/irp/threat/handbook/supplement.pdf>.

<sup>72</sup> U.S.-China Economic and Security Review Commission, *Annual Report to Congress 2009* (Washington, DC: U.S. Government Printing Office, November 2009), pp. 153 and 172. James Mulvenon, "PLA Computer Network Operations," in *Beyond the Strait: PLA Missions Other Than Taiwan*, eds. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2009); Northrop Grumman Corporation, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" (contracted research paper for the U.S.-China Economic and Security Review Commission, June 2009), p. 19. <http://www.uscc.gov/researchpapers/2009/NorthropGrumman/PRC/Cyber/Paper/FINAL/Approved%20Report/16Oct2009.pdf>.

Another major player in the Chinese networking market is ZTE Corporation [*Zhongxing Tongxun Gufen Youxian Gongsi* /中兴通讯股份有限公司], a telecommunications company based in Shenzhen. One of the first Chinese telecom equipment providers to pursue business in overseas markets, ZTE now has about 62,000 employees, about 107 representative offices around the world, and 15 research labs throughout North America, Europe, and Asia. ZTE states that 34 percent of its workforce and 10 percent of its revenues are dedicated to R&D.<sup>73</sup> Since 1996, the company has provided products and services to 135 countries and regions, serving major telecom operators in the Asia Pacific region, South Asia, North America, Europe, Latin America, Africa, and the Commonwealth of Independent States.<sup>74</sup>

ZTE was established in 1985 from “a handful of state-owned companies affiliated with the Ministry of Aerospace Industry.”<sup>75</sup> Though the company is publicly listed on the Shenzhen stock exchange and the Hong Kong stock exchange, government-affiliated entities appear to retain a majority share of its stock.<sup>76</sup> Over the last decade, ZTE has steadily increased its global market share among telecom equipment makers.<sup>77</sup> This increase is mostly due to the company’s ability to focus on networking gear, as opposed to phones, and its dedication to delivering equipment that is low cost but reliable. By 2007, ZTE had already become one of the world’s top ten mobile phone makers, joining the ranks of telecom giants Nokia and Samsung. ZTE’s annual income in 2009 was US \$486.4 million<sup>78</sup> and, despite the global downturn, the company’s growth is projected to be strong.

Among western countries, ZTE is a quiet giant, supplying handsets to operators without branding them under its own name. ZTE also has focused mainly on customers in developing countries who require cost-effective telecom solutions and whose countries lack sophisticated infrastructure. ZTE is highly specialized in CDMA [code division multiple access] technology and is willing to customize products for clients. As a result, ZTE’s export sales account for a majority of its revenues.

ZTE has established strategic cooperation agreements with leading telecom giants such as Portugal Telecom, France Telecom, Alcatel-Lucent, Ericsson, and Nortel in next generation network and mobile systems, with Hutchison in 3G (3<sup>rd</sup> generation), and with Marconi in optical transmission systems. The company has also established joint laboratory partnerships with Texas Instruments, Intel, Agere Systems, HHNEC, IBM, Microsoft (China), Qualcomm, Huahong NEC, and Tsinghua University.<sup>79</sup> As Chinese products achieve greater acceptability

<sup>73</sup> ZTE- Corporate information. <http://zte.com.cn>.

<sup>74</sup> Zhong Xing Telecommunication Equipment Company Limited, “ZTE Corporation,” a publicly owned Chinese corporation that designs and manufactures telecommunications and networking equipment and systems. <http://www.zte.com.cn/en>.

<sup>75</sup> *Bloomberg Business Week*, “A Global Telecom Titan Called... ZTE?” March 7, 2005. [http://www.businessweek.com/magazine/content/05\\_10/b3923071.htm](http://www.businessweek.com/magazine/content/05_10/b3923071.htm).

<sup>76</sup> A press clipping from 2006 posted on a ZTE company website states that “Although a listed company, [ZTE] is still very much a state-owned enterprise (SOE), with more than 69 percent of its shares owned by government-affiliated entities.” See China Online News, “Why Zhongxing is the CDMA Leader in China,” September 13, 2006. Posted on the ZTE “Press Center” webpage at [http://www.zte.com.cn/en/press\\_center/press\\_clipping/200106/t20010622\\_156932.html](http://www.zte.com.cn/en/press_center/press_clipping/200106/t20010622_156932.html).

<sup>77</sup> *Economist*, “Silent Mode; ZTE,” October 16, 2008.

<sup>78</sup> [http://ezproxy.library.nyu.edu:2076/us/Inacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T9664351210&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29\\_T9664351222&cisb=22\\_T9664351221&treeMax=true&treeWidth=0&csi=7955&docNo=7](http://ezproxy.library.nyu.edu:2076/us/Inacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9664351210&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9664351222&cisb=22_T9664351221&treeMax=true&treeWidth=0&csi=7955&docNo=7).

<sup>79</sup> “Company Description: ZTE Corporation,” Hoovers Inc., July 1, 2010.

<sup>79</sup> ZTE Corporation. [http://www.zte.com.cn/en/about/corporate\\_information](http://www.zte.com.cn/en/about/corporate_information).

with American consumers – just as Japanese products began to be accepted in the 1960s and 1970s – price points and dependability tend to mute country-of-origin concerns.

## THE ROLE OF HUAWEI AND ZTE IN THE U.S. MARKET

The telecommunications sector may be one of the most interconnected sectors of business between U.S. companies and Chinese companies, and this trend is continuing. For example, Huawei has expanded its facilities in Plano, Texas, to become its new North American headquarters,<sup>80</sup> and press reports in 2009 indicated that Huawei plans to expand its workforce to nearly 1,100 people within the United States and Canada.<sup>81</sup>

Huawei and ZTE are now among the top six global wireless equipment manufacturers, eclipsing, in some product categories, Alcatel-Lucent, Nortel (now in bankruptcy and being sold off in pieces), Cisco, and Motorola.<sup>82</sup> (*For more on Huawei's dealings with Nortel, see pp. 54-56.*) In many product classes, Huawei and ZTE rank in the top three of manufacturers, with Huawei rapidly moving toward number one in providing a full range of wireless networking equipment and handsets (often relabeled under other wireless network manufacturer brand names).

Huawei and ZTE have developed, manufactured, and sold technologically savvy, lower-cost, good-quality products in market niches.<sup>83</sup> While Huawei has had many product entries in the wireless market, its extraordinary range of product offerings supports almost every meaningful segment of telecommunications network architecture. Both Huawei and ZTE have typically introduced their mobile phones into the United States and other new market spaces through relabeling for companies like Verizon Wireless and T-Mobile.

Along with other technology equipment, as the manufacture of mobile phone handsets and associated software moves to offshore outsourcers, security could be compromised. Although there are no readily available case studies where this has actually happened, there is a potential risk of jeopardizing one of the most widely used forms of communications in the United States. Of most interest are Huawei's product uses that have deep vertical penetrations across all aspects of wireless, long haul, deep sea fiber, software, security, and cable networks.

### **Examples of U.S. Market Penetration by Chinese Telecom Companies**

- **July 2007:** An infrastructure agreement between Huawei and Leap Wireless was announced.<sup>84</sup>
- **March 2009:** Huawei became a supplier to Cox Communications for its wireless network, giving the company a major foothold in cable and wireless<sup>85</sup> in the United States.

<sup>80</sup> "Huawei to Add Hundreds of Tech Jobs," *Texas Business Journal*, May 1, 2009.

<sup>81</sup> "Huawei to Add Hundreds of Tech Jobs," *Texas Business Journal*, May 1, 2009.

<sup>82</sup> The original research for this report was performed in 2009, therefore some data have changed. The website "Seeking Alpha" recently reported that Huawei's expansion into the international router market is eating into Cisco's core router business and that "Huawei is currently the 2<sup>nd</sup> largest telecom equipment supplier globally with a share of 20% as of Q3 2009." See "China's Huawei: Margins, Market Share and Cisco's Router Business," *SeekingAlpha.com*, April 12, 2010. <http://seekingalpha.com/article/198323-china-s-huawei-margins-market-share-and-cisco-s-router-business>.

<sup>83</sup> *Wall Street Journal*, "China's Telecom Gear Makers, Once Laggards at Home, Pass Foreign Rivals," April 10, 2010.

<sup>84</sup> Fierce Wireless, "Huawei to deploy CDMA 2000 infrastructure for Cricket Communications," July 11, 2007.

- **March 2009:** Announcement was made that Huawei had deployed a 3G wireless network in Chicago for Cricket Communications, a subsidiary of Leap Wireless.<sup>86</sup>
- **August 2009:** Clearwire, LLC, announced a partnership with Huawei for its wireless communications network.<sup>87</sup> (Clearwire and Sprint Nextel merged in 2008.<sup>88</sup>)
- **March 2010:** ZTE, Chinese manufacturer of mobile phone handsets and infrastructure, announced its expectation to sell phones through major U.S. operators in the second half of the year.<sup>89</sup>

In 2008, Huawei announced a joint venture with Symantec, a U.S. manufacturer of network security products. The Huawei Symantec joint venture is likely complementary to Huawei's continued range of product offerings for telecommunications and network services.<sup>90</sup> It is natural for communications manufacturers to gravitate to the network security space. However, as foreign companies occupy a greater role in this field, there is an increased risk for compromised network security products to be implemented unnoticed in sensitive infrastructures. *(For more on the Huawei Symantec joint venture, see p. 47.)*

On September 29, 2008, a press release posted on Nokia's website announced that the Nokia Siemens Networks and Huawei, with its affiliates, had agreed upon a patent license for standards-essential patents. This will cover the worldwide use of all standards-essential patents of all parties, including GSM (global system for mobile communications), WCDMA (wideband code division multiple access), CDMA2000, optical networking, datacom, and WiMAX, and will affect mobile devices, infrastructure, and services.<sup>91</sup> On March 30, 2009, the Huawei website announced that Huawei had been selected to provide end-to-end cellular solution and services to Cox Communications. Cox, the third-largest cable provider in the United States, will launch its 3G wireless network utilizing Huawei's LTE (3GPP [partnership project] 4G technology)-ready SingleRAN solution and industry-leading 3900 Series base stations.<sup>92</sup> In 2008, Huawei offered its handset unit for sale to private equity firms including Bain Capital, Blackstone, TPG (formerly Texas Pacific Group), Kohlberg Kravis Roberts, Warburg Pincus, and Carlyle Group for \$4 billion.<sup>93</sup> The offer was later pulled, reportedly due to the condition of financial markets.

## THE MAJOR CHINESE DOMESTIC TELECOM CORPORATIONS

While Huawei and ZTE have been among the most active Chinese telecoms in their overseas investments and business activities, China also has other telecom companies, which primarily service the domestic market. The three most prominent, which are all state owned, are listed below.

<sup>85</sup> Light Reading, Cable Digital News, "Cox, Huawei Make Wireless Connection," March 30, 2009.

<sup>86</sup> Huawei Press Release, March 2009.

<sup>87</sup> Light Reading Mobile, "Clearwire Confirms Huawei Deal," August 11, 2009.

<sup>88</sup> *InformationWeek*, "FCC Approves Sprint Clearwire Merger," November 5, 2008.

<sup>89</sup> Fierce Wireless, March 29, 2010.

<sup>90</sup> Symantec Press Release, "Huawei and Symantec Commence Joint Venture," February 5, 2008.

<sup>91</sup> "Nokia Siemens Partners with Huawei," September 29, 2008. The agreement covers worldwide use of all standards essential patents of all parties. <http://news.softpedia.com/news/Nokia-Siemens-Partners-With-Huawei-94374.shtml>.

<sup>92</sup> Huawei website, March 20, 2009. <http://www.huawei.com/news/view.do?id=10799&cid=42>.

<sup>93</sup> Michael Flaherty and Vinicy Chan, "Private Equity Firms Line Up for Huawei Unit Sale," Reuters, June 5, 2008. <http://in.reuters.com/article/idINHKG31043120080605>.



## **China Mobile**

China Mobile Ltd. [*Zhongguo Yidong Tongxin* - 中国移动通信] is currently the world's largest mobile telephone operator.<sup>94</sup> China Mobile provides cellular and value-added mobile services to 31 provinces of mainland China and Hong Kong. With approximately 548 million subscribers (as of May 31, 2010) and over 70 percent of the Chinese cellular market, China Mobile is considered a central state-owned enterprise by the Chinese government.<sup>95</sup> The company has historically operated on a GSM network, but in 2009 it rolled out its home-grown 3G network operating on a time division synchronous code division multiple access (TD-SCDMA) network.<sup>96</sup> China Mobile is currently listed on both the New York Stock Exchange (NYSE:CHL) as well as the Hong Kong stock exchange (941:HKG). Its operating revenue in 2009 was renminbi (RMB) 518.08 billion.<sup>97</sup>

Founded in 1988 as Guangdong Mobile, the commercial mobile telephone network was initially operated by the provincial government of Guangdong for use by high-level officials of state-owned enterprises and high-ranking government officials.<sup>98</sup> By 1997, the Chinese government sought to restructure the telecommunications industry by consolidating provincial telecom corporations. In 2000, the government merged Guangdong Mobile and the telephone operator of Zhejiang into a subsidiary of China Telecom Hong Kong BVI, called China Mobile Ltd. To date, the company is still directly controlled by the government, which has a 74.22 percent equity stake through China Mobile (Hong Kong) Limited, which is wholly owned by the government as an arm of China Mobile Communications Corporation, also government owned.<sup>99</sup>

## **China Telecom**

China Telecom [*Zhongguo Dianxin* / 中国电信] is the largest fixed-line telecommunications operator and broadband service provider in the world.<sup>100</sup> It is one of the leading providers of broadband access services in the Chinese market and has a strong foothold in the residential market.<sup>101</sup> Considered one of the top three state-backed telecommunications companies in

<sup>94</sup> China Mobile Limited, "Operation Data," <http://www.chinamobileltd.com/about.php?menu=1>.

<sup>95</sup> Bruce Einhorn, "China Mobile Is Counting on Android," *Business Week*, August 20, 2009.

[http://www.businessweek.com/globalbiz/content/aug2009/gb20090820\\_505265.htm](http://www.businessweek.com/globalbiz/content/aug2009/gb20090820_505265.htm).

<sup>96</sup> *New York Times*, "China Mobile's 2<sup>nd</sup> Quarter Profit Slips," August 21, 2009.

[http://ezproxy.library.nyu.edu:2076/us/Inacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T9769608077&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29\\_T9769608080&cisb=22\\_T9769608079&treeMax=true&treeWidth=0&selRCNodeID=37&nodeStatId=411en\\_US,1,36&docsInCategory=5&csi=6742&docNo=1](http://ezproxy.library.nyu.edu:2076/us/Inacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9769608077&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9769608080&cisb=22_T9769608079&treeMax=true&treeWidth=0&selRCNodeID=37&nodeStatId=411en_US,1,36&docsInCategory=5&csi=6742&docNo=1).

<sup>98</sup> *Financial Times*, "China Mobile Ltd.," July 19, 2010.

<http://markets.ft.com/tearsheets/businessProfile.asp?s=941:HKG>.

<sup>99</sup> *Business & Company Resource Center: Novel NY*, "China Mobile Ltd."

[http://ezproxy.library.nyu.edu:2081/servlet/BCRC?rsic=PK&rcp=CO&vrsn=unknown&locID=nysl\\_me\\_nyuniv&srchtp=cmp&cc=1&c=1&mode=c&ste=74&tbst=tsCM&tab=4&ccmp=China+Mobile+Ltd.&tcp=china+mobile&n=25&docNum=12501313383&bConts=13119](http://ezproxy.library.nyu.edu:2081/servlet/BCRC?rsic=PK&rcp=CO&vrsn=unknown&locID=nysl_me_nyuniv&srchtp=cmp&cc=1&c=1&mode=c&ste=74&tbst=tsCM&tab=4&ccmp=China+Mobile+Ltd.&tcp=china+mobile&n=25&docNum=12501313383&bConts=13119).

<sup>100</sup> *Economist*, "Strait Deals; Chinese Investment," May 9, 2009.

[http://ezproxy.library.nyu.edu:2076/us/Inacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T9769089916&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29\\_T9769089925&cisb=22\\_T9769089924&treeMax=true&treeWidth=0&selRCNodeID=26&nodeStatId=411en\\_US,1,23&docsInCategory=5&csi=7955&docNo=2](http://ezproxy.library.nyu.edu:2076/us/Inacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9769089916&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9769089925&cisb=22_T9769089924&treeMax=true&treeWidth=0&selRCNodeID=26&nodeStatId=411en_US,1,23&docsInCategory=5&csi=7955&docNo=2); and Doug Young, "China Mobile Growth Prospects Improve," *Reuters*, March 18, 2010.

<http://www.reuters.com/article/idUSTRE62H0IU20100318>.

<sup>101</sup> China Telecom, "Company Overview," [http://www.chinatelecom-h.com/eng/company/company\\_overview.htm](http://www.chinatelecom-h.com/eng/company/company_overview.htm).

<sup>102</sup> Frederick Yeung, "China Telecom Challenges Leader," *South China Morning Post* (Hong Kong), November 18, 2008.

[http://ezproxy.library.nyu.edu:2076/us/Inacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T97707883](http://ezproxy.library.nyu.edu:2076/us/Inacademic/results/docview/docview.do?docLinkInd=true&risb=21_T97707883)

China, China Telecom is the leader in fixed-line networks but is currently the third-largest wireless operator (behind China Mobile and China Unicom), with only 56 million subscribers.<sup>102</sup> The company was listed on the New York Stock Exchange (NYSE:CHA) and the Hong Kong Stock Exchange (HK:728) in November 2002, with an initial public offering of approximately USD \$1.3 billion.

China Telecom was established in 1994 by the Chinese government to oversee the nation's public telecommunications operations. By 1997, China Telecom had become the second-largest fixed-line telephone network in the world, with over 100 million subscribers.<sup>103</sup> In 2008, China Telecom acquired the CDMA network of China Unicom, the third-largest telecommunications firm in China, a move intended to boost the mobile phone operations of China Telecom.<sup>104</sup> The company is still largely subject to policy changes in the Chinese government: China Telecommunications Corporation, a state-owned enterprise, owns a 70.89 percent stake in China Telecom.

### **China Unicom**

China Unicom [*Zhongguo Liantong* / 中国联通] is China's second-largest telecom company, after China Mobile. It is an integrated telecommunications operator offering mobile voice, value-added, fixed-line voice, and broadband services. In 2008, the company had over 273 million subscribers and total assets of around RMB 500.09 billion.<sup>105</sup> China Unicom is the only Chinese telecom to be traded on the New York Stock Exchange (NYSE:CHU), the Hong Kong Stock Exchange (SEHK:0762), and the Shanghai Stock Exchange (SSE:600050). Even so, the company is a state-owned enterprise, with China Netcom Group Corporation (BVI) Limited and China Unicom (BVI) Limited, both state-owned firms, as the two largest shareholders.

Created in 1994 with the permission of the State Council, China Unicom was part of a government reform aimed at the domestic telecom industry to discourage monopolies.<sup>106</sup> For many years, the company mainly operated in northern China and eventually became the official partner of the 2008 Beijing Olympic Games for fixed communications services. In 2009, China Unicom sold its CDMA mobile assets to China Telecom and merged with China Netcom. The merger resulted in an acquisition of fixed-line businesses in 21 provinces in southern China for RMB 4.63 billion.<sup>107</sup> In recent years, it has formed strategic alliances with such companies as

---

[63&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29\\_T9770788366&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29\\_T9770788366&treeMax=true&treeWidth=0&csi=11314&docNo=2](http://ezproxy.library.nyu.edu:2076/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9770788366&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9770788366&treeMax=true&treeWidth=0&csi=11314&docNo=2)

<sup>103</sup> Toh Han Shih, "China Telecom Expects Earnings Rebound," *South China Morning Post* (Hong Kong), March 23, 2010.

[http://ezproxy.library.nyu.edu:2076/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T9770564060&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29\\_T9770564065&treeMax=true&treeWidth=0&csi=11314&docNo=9](http://ezproxy.library.nyu.edu:2076/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9770564060&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9770564065&treeMax=true&treeWidth=0&csi=11314&docNo=9)

<sup>104</sup> Business & Company: Resource Center, "China Telecom Corporation Ltd."

[http://ezproxy.library.nyu.edu:2081/servlet/BCRC?vrsn=unknown&locID=nysl\\_me\\_nyuniv&srchtp=qlbc&cc=2&c=1&mcode=c&ste=74&tbst=tsCM&tab=4&ccmp=China+Telecom+Corporation+Ltd.&mst=china+telecom&n=25&docNum=12501151876&bConts=9023](http://ezproxy.library.nyu.edu:2081/servlet/BCRC?vrsn=unknown&locID=nysl_me_nyuniv&srchtp=qlbc&cc=2&c=1&mcode=c&ste=74&tbst=tsCM&tab=4&ccmp=China+Telecom+Corporation+Ltd.&mst=china+telecom&n=25&docNum=12501151876&bConts=9023)

<sup>104</sup> Economist, "Rewired; Telecoms in China," May 31, 2008.

[http://ezproxy.library.nyu.edu:2076/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T9770429590&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29\\_T9770429596&treeMax=true&treeWidth=0&selRCNodeID=9&nodeStatId=411en\\_US,1.8&docsInCategory=3&csi=7955&docNo=2](http://ezproxy.library.nyu.edu:2076/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9770429590&format=GNBFI&sort=BOOLEAN&startDocNo=1&resultsUrlKey=29_T9770429596&treeMax=true&treeWidth=0&selRCNodeID=9&nodeStatId=411en_US,1.8&docsInCategory=3&csi=7955&docNo=2)

<sup>105</sup> China Unicom, "Corporate Profile."

<sup>106</sup> China Unicom, "Our History." [http://eng.chinaunicom.com/about/Eng\\_qywh/index.html](http://eng.chinaunicom.com/about/Eng_qywh/index.html).

<sup>107</sup> Benjamin Scent, "Unicom in 6.43B Yuan Deal," *Standard* (London), December 17, 2008.



Spanish telecommunications operator Telefónica to swap stock as well as jointly purchase mobile networks and phones.<sup>108</sup>

### **State-Directed Personnel Shuffling and Restructuring at PRC Telecom Corporations**

While questions may circulate about the extent of PRC state influence over the nominally private companies Huawei and ZTE, there is far less ambiguity regarding China's major domestic telecom corporations, all of which are directly state controlled. With these companies, the controlling hand of the state is very clear. The Chinese government exercises extensive command over the management and operations of these companies, as illustrated in the examples below:

#### **2004**

In October 2004, the Chinese government abruptly shuffled the senior management of the three "China" telecoms: a senior executive from China Unicom was made the new head of China Mobile, a former China Mobile vice president was appointed to head China Telecom, and the head executive of China Telecom was moved to China Unicom.<sup>109</sup> The sudden personnel moves had been directed by the Central Organization Department of the Chinese Communist Party,<sup>110</sup> and ignored the nominal legal and fiduciary responsibilities of the corporate boards to select the managing officials of each company.<sup>111</sup> It shocked many shareholders and industry analysts and even drew criticism from the business journal *Caijing*, one of the bolder voices in the Chinese media.<sup>112</sup> It was, as one author has said, "the equivalent of the CEO [chief executive officer] of AT&T being moved without notice to head its domestic US competitor, Verizon, with the Verizon chief being appointed to run Sprint, at a time when the three companies were locked in a bruising battle on price and industry standards."<sup>113</sup>

#### **2008**

Another dramatic shuffle of personnel, and an accompanying state-mandated restructuring of the telecom sector, occurred in May 2008. At that time, new appointments were made to (1) the positions of company president and party secretary at both China Mobile and China Telecom; (2) the president of China Tietong [*Zhongguo Tietong Gongsi* / 中国铁通公司], the vice president of China Unicom, and the vice president of China Unicom were all transferred to China Mobile; and (3) the vice president of China Unicom, and the head of the CCP Discipline Inspection Team of China Unicom, were transferred to China Telecom.<sup>114</sup> The restructuring also mandated the merging of China Mobile and the smaller China Tietong and for China Unicom to be divided, with its CDMA network sold off to China Telecom and its GSM network business merged into China Netcom.<sup>115</sup>

<sup>108</sup> Kevin O'Brien, "Telefónica and China Unicom Deepen Links," *International Herald Tribune*, September 7, 2009.

<sup>109</sup> Kathrin Hille, "China Mobile in Board Shake Up," *Financial Times*, May 31, 2010.

<sup>110</sup> Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: Harper Collins, 2010), pp. 84-89; and Kathrin Hille, "China Mobile in Board Shake Up," *Financial Times*, May 31, 2010.

<sup>111</sup> Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: Harper Collins, 2010), p. 85.

<sup>112</sup> *Caijing*, "The Telecoms Reshuffle: More Harm Than Good," November 15, 2004.

<sup>113</sup> Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: Harper Collins, 2010), p. 84.

<sup>114</sup> ChinaTechNews.com, "China's Telecom Restructuring Plan Finally Announced," May 26, 2008.

<http://www.chinatechnews.com/2008/05/26/6787-chinas-telecom-restructuring-plan-finally-announced>.

<sup>115</sup> Wang Xing, "Jury Out on Dramatic Telecom Restructure," *China Daily*, May 24, 2008.

**2010**

Another government-directed management shake-up in the telecom sector was seen in May 2010, when Wang Jianzhou, the chief executive of China Mobile, was removed from his position as general manager and appointed to chair a newly established board of directors for the company. Mr. Wang was also appointed party secretary of China Mobile's Communist Party committee. He was succeeded as general manager by Li Yue, the company's vice president. China Mobile indicated that the move had been directed once again by the Central Organization Department, and in phraseology evocative of internal CCP discourse, indicated that it was part of a plan to "make the company's management strategy more scientific and regulated." The *Financial Times* commented that the sudden reshuffle at China Mobile "left observers confused... underscoring the opaque nature of China's state enterprises."<sup>116</sup>

## **HUAWEI AND 3-COM: A CLASSIC EXAMPLE OF CHINA'S FORAYS INTO THE U.S. MARKET VIA JOINT VENTURE AND ACQUISITION**

3Com Corporation was a major American telecommunications company that invented, manufactured, integrated, and implemented network infrastructure products and developed supporting service models throughout the small, medium, and (to a lesser degree) large enterprise markets of North America.<sup>117</sup> 3Com Corporation and Huawei formed a joint venture in 2003 for the purpose of developing data communications products. In 2006, 3Com bought out the Huawei stake in the joint venture. In 2007, Bain Capital and Huawei made a \$2.2 billion dollar bid for 3Com, which was eventually abandoned due to security concerns on the part of the U.S. government.<sup>118</sup> (See *more below*.) In November 2009, 3Com announced its acquisition by Hewlett-Packard for \$2.7 billion.<sup>119</sup>

As a manufacturer of routers, switches, and hubs, 3Com had equipment that was often found in the heart of telecommunications networks and that provided connectivity to some of the most secure areas of infrastructures. Nevertheless, despite being a pioneer in the technology of Internet protocol (IP) communications and networking, 3Com lacked brand identity and penetration into the large enterprise market segment due to the presence of more well-established vendors. Strategic decisions to avoid affiliation with IP telephony technology platforms by some companies, such as Microsoft, further constrained 3Com's ability to penetrate further into its chosen markets.

Within two weeks after announcing a net loss of \$18.7 million for its first quarter 2008 revenues, 3Com said that it was being acquired by Bain Capital Partners LLC. Bain had previously handled numerous large technology-based buyouts, to include the takeover of Texas Instruments Inc.'s sensors and controls division.<sup>120</sup> Bain's offer for the deal was \$2.2 billion, with Huawei Tech Investment Co. Ltd. (Hong Kong) to acquire a minority 16.5 percent interest worth \$363 million. Huawei Tech Investment Co. Ltd. is a wholly owned subsidiary of Huawei Technologies Co. Ltd. (Hong Kong), 3Com's former joint venture partner in the H3C venture.

<sup>116</sup> Kathrin Hille, "China Mobile in Board Shake Up," *Financial Times*, May 31, 2010.

<sup>117</sup> 3-Com website section on corporate history. <http://www.3-Com.com>.

<sup>118</sup> Reuters, "Opposition Leads Bain to Call Off 3Com Deal," March 21, 2008.

<http://www.nytimes.com/2008/03/21/technology/21com.html>; and *Cajing China (English version)*, "The 3Com Deal, Behind the Security Flap," October 23, 2007.

<sup>119</sup> Bloomberg.com, "3-Com Agrees to \$2.2 billion dollar purchase," September 28, 2007.

<sup>120</sup> Texas Instruments press release, "TI Completes Sale of Sensor Control Business to Bain Capital," April 26, 2006.

However, the intended deal between Huawei and 3Com fell afoul of the U.S. government interagency Committee on Foreign Investment in the United States (CFIUS), which investigated the deal on national security grounds. (*For further information on the CFIUS process, see pp. 30-33.*) Among the alleged concerns were (1) that Huawei had links to the Chinese military; and (2) that Tipping Point, a subordinate unit of 3Com, provides network security products and services to the Department of Defense (DOD) and a number of other federal agencies.<sup>121</sup> Following failure to negotiate a “mitigation agreement” to answer government concerns, Bain announced in March 2008 that it was backing out of the deal.<sup>122</sup>

### **A Timeline History of 3Com**<sup>123</sup>

- 1979: Founded by Robert Metcalfe (inventor of Ethernet) in 1979.
- 1984: Goes public.
- 1987: Acquires Bridge Communications.
- 1997: Acquires U.S. Robotics (modem manufacturer and owner of Palm, Inc.).
- 1999: 3Com acquires NBX and achieves much progress in initial validation and adoption of VOIP (Voice Over Internet Protocol).
- 2000: Reaches its peak market value of \$25.8 billion listed on the NASDAQ.<sup>124</sup>
  - Exits the high-end router business due to strong competition from Cisco; many of 3Com's larger customers feel abandoned by their vendor of choice.
  - Buys Kerbango and attempts new business entry into Internet radio market but abandons the initiative in less than a year.
  - U.S. Robotics & Palm are spun off and become separate again.
- 2003: Joint venture with Huawei to create H3C. Combined research on routers, switches, wireless networking, security, VOIP, network management systems, and other enterprise and small office home office SOHO (small office home office) -level solutions. 3Com gains access to Asian markets, and Huawei gains access to U.S. and European markets.
  - Sells ComWorks Corporation to UT StarCom.<sup>125</sup>
- 2005: After the DotCom bust, shares of stock fall in value from an adjusted record of \$21.89 to \$2.96 per share.
- 2006: Generates nearly 37.6 percent of revenues from Europe, Middle East, and Africa; 31.3 percent from North America; 22.1 percent from Asia/Pacific; and 9 percent from Central and South America.
- 2007: Juniper Networks (carrier-level telecom and network hardware manufacturer) expresses an interest in buying the H3C joint venture.

<sup>121</sup> Reuters, “Opposition Leads Bain to Call Off 3Com Deal,” March 21, 2008.

<http://www.nytimes.com/2008/03/21/technology/21com.html>; and Steven R. Weisman, “Sale of 3Com to Huawei is Derailed by U.S. Security Concerns,” *New York Times*, February 21, 2008.

<http://www.nytimes.com/2008/02/21/business/worldbusiness/21iht-3com.1.10258216.html>. See also Tipping Point website, “U.S. Federal Government Solutions,” [http://www.tippingpoint.com/solutions\\_federal.html](http://www.tippingpoint.com/solutions_federal.html).

<sup>122</sup> Reuters, “Opposition Leads Bain to Call Off 3Com Deal,” March 21, 2008.

<http://www.nytimes.com/2008/03/21/technology/21com.html>.

<sup>123</sup> Bloomberg.com press release data/public filings/multiple press reports, September 28, 2007.

<sup>124</sup> Bloomberg.com, “3-Com Agrees to \$2.2 billion dollar purchase,” September 28, 2007.

<sup>125</sup> Mobile Monday.Net, “UT Starcom Buys 3Com's Operator Assets,” March 5, 2003. Quote from the article: “Acquiring the CommWorks assets will allow UT Starcom to add to its base of tier-one customers and accelerate its geographic diversification outside of China,” said Hong Lu, president and chief executive officer of UT Starcom. “We are already the largest vendor to China Telecom and sell to major customers such as China Netcom.”

- 2007: 3Com sees the H3C venture as an option for reversing its multiyear unprofitable trend and decides to acquire and keep total ownership of H3C. Huawei sells 3Com its 49 percent share of the H3C joint venture.
- 2007: 3Com announces its acquisition by Bain Capital Partners and Huawei for \$2.2 billion.
- 2008: 3Com acquisition by Bain and Huawei falls through due to regulatory opposition.<sup>126</sup>
- 2009: In November, 3Com announces acquisition by Hewlett-Packard for \$2.7 billion.

Many industry analysts viewed the attempted acquisition of 3Com in concert with Bain as another example of Huawei's efforts to expand its products to overseas markets that it had not yet penetrated, as well as a way of competing directly against global leaders such as Cisco. Huawei was particularly interested in penetrating the North American marketplace at the enterprise solution level.<sup>127</sup>

## DEALS IN THE TELECOM SECTOR, AND THE ROLE OF CFIUS

The Committee on Foreign Investment in the United States is a U.S. government interagency committee chaired by the Treasury Department. Its role is "to review transactions that could result in control of a U.S. business by a foreign person ('covered transactions'), in order to determine the effect of such transactions on the national security of the United States."<sup>128</sup> The CFIUS process is usually initiated when parties to a proposed or pending transaction of potential concern jointly file a voluntary notice with CFIUS.<sup>129</sup>

Membership in CFIUS includes the secretaries of seven federal departments (the Treasury, Justice, Homeland Security, Commerce, Defense, State, and Energy), and the heads of two executive offices (U.S. Trade Representative, Science & Technology Policy). The director of National Intelligence and the secretary of Labor are also nonvoting, ex officio members of CFIUS; and five additional federal offices (Office of Management & Budget, Council of Economic Advisors, National Security Council, National Economic Council, and Homeland Security Council) also participate as observer members of CFIUS.<sup>130</sup>

CFIUS investigates only a limited number of cases each year. It officially blocks only a very small number, although some deals are withdrawn by the filing companies if problems appear likely to crop up in the CFIUS review. In the three-year period from 2006 to 2008, CFIUS received a total of 404 notices (in all industrial sectors) and investigated 36 of them; 57 of these

<sup>127</sup> Reuters, "Opposition Leads Bain to Call Off 3Com Deal," March 21, 2008.

<http://www.nytimes.com/2008/03/21/technology/21com.html>; and *Caijing China* (English version), "The 3Com Deal, Behind the Security Flap," October 23, 2007.

<sup>128</sup> Funding Universe.com/histories; 10Ks, public filings.

<sup>129</sup> United States Department of the Treasury website, "Office of Investment Security -- Committee on Foreign Investment in the United States." <http://www.ustreas.gov/offices/international-affairs/cfius>. CFIUS operates pursuant to section 721 of the Defense Production Act of 1950, as amended by the Foreign Investment and National Security Act of 2007 (section 721) and as implemented by Executive Order 11858, as amended, and regulations at 31 C.F.R. Part 800.

<sup>130</sup> United States Department of the Treasury website, "Office of Investment Security -- Committee on Foreign Investment in the United States -- Overview of the CFIUS Process." <http://www.ustreas.gov/offices/international-affairs/cfius/overview.shtml>.

<sup>130</sup> United States Department of the Treasury website, "Office of Investment Security -- Committee on Foreign Investment in the United States -- Composition of CFIUS." <http://www.ustreas.gov/offices/international-affairs/cfius/members.shtml>.

proposed deals were subsequently withdrawn after filing, but none were formally rejected.<sup>131</sup> In the same period, CFIUS reviewed a total of 133 cases classified as “information” sector deals (one-third of the total number); of these, 22 cases were in the telecommunications industry.<sup>132</sup> Three out of the total 133 “information sector” deals involved investors based in China.<sup>133</sup>

Huawei, in particular, has been a focus of great attention and controversy in association with CFIUS reviews of potential telecom deals. As stated by the *Financial Times*:

*US government agencies charged with reviewing sensitive acquisitions are engaged in a debate over how to handle Huawei... There are two schools of thought within the US government. One pragmatic view holds that [CFIUS] should approve a future transaction [with Huawei] because it would allow the government to negotiate what is known as a mitigation agreement, a set of strict conditions and security-related requirements that could give the US valuable insight into the inner workings of a company that some allege has close ties to the Chinese military...*

*But there are strong arguments against such a move that support keeping Huawei at bay. One former official close to the [CFIUS] process said the government engaged in a similar debate during its review of Huawei's joint bid for 3Com... 'At the time, most of the national security agencies concluded that the window into Huawei would not be useful enough and that it would be very difficult to write procedures that would ensure [network security]...'*<sup>134</sup>

#### **CFIUS and the Abortive Emcore / Caofeidian Deal**

Aside from the abortive deal between Huawei and 3Com, another recent Chinese-related telecommunication deal that encountered difficulties with CFIUS was the cancelled 2010 deal between Emcore Corporation and China's Tangshan Caofeidian Investment Corporation [Tangshan Caofeidian Touzi Jituan / 唐山曹妃甸投资集团], or TCIC. Emcore Corporation, a New Mexico-based manufacturer of components for fiber optic equipment and solar panels, had agreed to sell a 60 percent stake in its fiber optics business to TCIC for \$27.75 million USD.<sup>135</sup>

There is little known about TCIC; the company has no website, and only limited information regarding the investment firm is readily available. It is possible that TCIC is a subsidiary of the Tangshan Caofeidian Infrastructure Investment Corporation [Tangshan Caofeidian Jichu Sheshi Jianshe Touzi Jituan Youxian Gongsi / 唐山曹妃甸基础设施建设投资集团有限公司], a state-owned conglomerate created by the Caofeidian Ministry of Investment. The company is a key

<sup>131</sup> Committee on Foreign Investment in the United States, *Annual Report to Congress 2009* (Washington, DC: November 2009), p. 3. <http://www.ustreas.gov/offices/international-affairs/cfius/docs/2009%20CFIUS%20Annual%20Report.pdf>.

<sup>132</sup> Committee on Foreign Investment in the United States, *Annual Report to Congress 2009* (Washington, DC: November 2009), pp. 4 and 7. <http://www.ustreas.gov/offices/international-affairs/cfius/docs/2009%20CFIUS%20Annual%20Report.pdf>.

<sup>133</sup> Committee on Foreign Investment in the United States, *Annual Report to Congress 2009* (Washington, DC: November 2009), p. 15. <http://www.ustreas.gov/offices/international-affairs/cfius/docs/2009%20CFIUS%20Annual%20Report.pdf>.

<sup>134</sup> Stephanie Kirchgaessner and Helen Thomas, “US Divided on How to Tackle Huawei,” *Financial Times*, July 29, 2010.

<sup>135</sup> Emcore Corp. Press Release, “EMCORE and Tangshan Caofeidian Investment Corporation (‘TCIC’) Pursue Alternative Means of Cooperation to Address Regulatory Concerns,” June 28, 2010. [http://www.emcore.com/news\\_events/release?y=2010&news=249](http://www.emcore.com/news_events/release?y=2010&news=249).



player in the financial and economic development of Caofeidian, an industrial zone on a man-made island in the Gulf of Bohai. The Caofeidian project was initiated at the direction of the PRC State Council in 2004 and is administered by Tangshan City, Hebei Province.<sup>136</sup>

Tangshan Caofeidian Infrastructure Investment Corporation claims 28 subsidiaries and several equity affiliates. These subsidiaries and affiliates are reportedly involved in a wide variety of industries, to include real estate, hotels, railroads, logistical services, construction, petrochemicals, and even electric vehicle development.<sup>137</sup>

Figure 2: Location of Caofeidian Island



Source: <http://www.caofeidian.us/index.html>.

Figure 3: Artist Conception of Caofeidian Island



Source: <http://hy.csm.org.cn/icsr10/en/110.htm>.

Although it is unconfirmed, the TCIC involved in the Emcore deal may be associated with Tangshan Caofeidian Financial Investment, Ltd., [*Tangshan Caofeidian Touzi Youxian Zeren Gongsi* 唐山曹妃甸投资有限责任公司], a state-owned investment bank based in Caofeidian. The bank is involved in private equity investment, direct investment, consulting, and financial advisory services.<sup>138</sup> Tangshan Caofeidian Investment, Ltd., has invested in a plethora of domestic and foreign firms and funds, to include the China-Africa Development Fund, the China-Belgium Equity Investment Fund, the Bohai Industry Investment Fund, the China-ASEAN Investment Fund, China Aluminum Corporation, Mandarin Capital Partners [*Zhong-Yi Mandalin Jijin* / 中意曼达林基金, a joint investment project between Chinese and Italian banks],<sup>139</sup> as well as other "major projects that are in the interest of shareholders."<sup>140</sup>

<sup>136</sup> Caofeidian promotional website. <http://www.caofeidian.us/index.html>.

<sup>137</sup> "Tangshan Caofeidian Infrastructure Construction Dynamic Management Platform" [Tangshan Caofeidian Jichu Sheshi Jianshe Dongtai Guanli Pingtai / 唐山曹妃甸基础设施建设动态管理平台], "Company Introduction." Translation by USCC staff. <http://www.cfdjt.com/Integration/ProjectIntro.aspx>.

<sup>138</sup> *Daily Economic News* [Mei Ri Jingji Xinwen / 每日经济新闻], "National Development Bank Goes Through Tangshan Caofeidian to March into City Development" [Guojia Kaifa Yinhang Jiedao Tangshan Caofeidian Zhijie Jinjun Chengshi Kaifa / 国家开发银行借道唐山曹妃甸直接进军城市开发], March 10, 2010. Translation by USCC staff. [http://finance.ce.cn/rolling/201003/10/t20100310\\_15590232.shtml](http://finance.ce.cn/rolling/201003/10/t20100310_15590232.shtml).

<sup>139</sup> Mandarin Capital Partners website. <http://www.mandarinpc.com/index.html>.

<sup>140</sup> *Daily Economic News* [Mei Ri Jingji Xinwen / 每日经济新闻], "National Development Bank Goes Through Tangshan Caofeidian to March into City Development" [Guojia Kaifa Yinhang Jiedao Tangshan Caofeidian Zhijie Jinjun Chengshi Kaifa / 国家开发银行借道唐山曹妃甸直接进军城市开发], March 10, 2010. Translation by USCC staff. [http://finance.ce.cn/rolling/201003/10/t20100310\\_15590232.shtml](http://finance.ce.cn/rolling/201003/10/t20100310_15590232.shtml).

The proposed deal between Emcore and TCIC was withdrawn in late June 2010.<sup>141</sup> As is its usual practice, CFIUS has not made any public statement about the matter. Emcore has stated only that CFIUS communicated “certain regulatory concerns about the transaction” and that “EMCORE and TCIC remain willing to explore alternative means of cooperation that would address regulatory concerns and meet the parties’ objectives.”<sup>142</sup>

## THE GROWTH STRATEGY OF CHINESE TELECOM FIRMS

An apparent strategy for Chinese companies has been to pursue developing markets first and then move on to developed markets, as seen in the involvement of Chinese companies in telecom infrastructure markets in the 1980s and 1990s.<sup>143</sup> Their product strategy was to provide broad-scale telecommunications and network products for low procurement and implementation costs.<sup>144</sup>

Within China’s domestic market, the government appears to have strongly favored domestically produced telecommunications products and services.<sup>145</sup> This protected environment allowed domestic firms such as Huawei and ZTE to gain strength and size while also being able to compete against world-class solutions providers such as Cisco, 3Com, Avaya, Nortel, Alcatel-Lucent, Ericsson, IBM, and others across a wide range of solution sets that may have been unsustainable in the face of free and open competition.

Huawei’s initial forays into the global marketplace were into other Asian nations in China’s economic near abroad.<sup>146</sup> This was the initial arena where some Chinese companies may have refined their strategy of “developing markets first, developed markets second” before moving forward with a strategy for global competition.<sup>147</sup>

Huawei has competed very successfully worldwide and is often in the number one or two slot in developing markets.<sup>148</sup> Its aggressive strategy and pricing have a major economic impact for both large and small service providers, and its market prospects appear positive. Nevertheless, if a company wants to ascend to the top tier of global telecommunications and networking equipment companies, historically it has been essential that it gain access to the U.S. marketplace. The North American market appears to have been one of Huawei’s last target markets, as penetrating the U.S. marketplace promised to pose one of the toughest challenges and could remain a weaker market for Huawei for some time.<sup>149</sup> This may have driven much of

<sup>141</sup> Stephanie Kirchgaessner, “US Blocks China Fibre Optics Deal Over National Security,” *Financial Times*, June 30, 2010; and Emcore Corp. Press Release, “EMCORE and Tangshan Caofeidian Investment Corporation (‘TCIC’) Pursue Alternative Means of Cooperation to Address Regulatory Concerns,” June 28, 2010. [http://www.emcore.com/news\\_events/release?y=2010&news=249](http://www.emcore.com/news_events/release?y=2010&news=249).

<sup>142</sup> Emcore Corp. Press Release, “EMCORE and Tangshan Caofeidian Investment Corporation (‘TCIC’) Pursue Alternative Means of Cooperation to Address Regulatory Concerns,” June 28, 2010. [http://www.emcore.com/news\\_events/release?y=2010&news=249](http://www.emcore.com/news_events/release?y=2010&news=249)

<sup>143</sup> NPR.org, “Chinese Telecom Companies Look to Global Markets,” August 16, 2005.

<sup>144</sup> Voice & Data Online, India, “ZTE Right Pricing,” September 3, 2008.

<sup>145</sup> *Asia Times*, “3G is Key to a Foreign Telecom Role in China,” December 6, 2006, and “Voice & Data Online, India, “ZTE Right Pricing,” September 3, 2008.

<sup>146</sup> Voice & Data Online, India, “ZTE Right Pricing,” September 3, 2008.

<sup>147</sup> RCR Wireless, “Huawei’s Aggressive Push Pays Off,” September 24, 2008.

<sup>148</sup> Del Oro Group Press Release, “Chinese Vendors Huawei and ZTE Gain Ground on Leaders Ericsson and Nokia Siemens,” April 26, 2008.

<sup>149</sup> *Forbes*, “Huawei’s U.S. coming out Party,” March 27, 2009; and *Forbes*, “Huawei Buys Back Into 3Com,” October 1, 2007.



Huawei's joint venture strategy with 3Com, which may be considered the company's first large, strategic attempt to move into U.S. markets.

The abortive deal with 3Com would have offered Huawei an opportunity to establish the beachhead for a stronger presence in the North American marketplace. It was also an opportunity for Huawei to jump on the mergers and acquisitions (M&A) bandwagon that was gaining momentum in the telecommunications industry. Huawei's statements indicated a desire to use its H3C joint venture with 3Com as a means of refining the focus of its product strategy to telecommunications service providers. However, its actions may have also indicated a more ambitious strategy for the North American market.<sup>150</sup> After 3Com bought out the H3C venture, it appears that Huawei may have used the resulting cash to turn back around and pursue 3Com in acquisition mode. Although its efforts in this regard were opposed by regulators (*see pp. 28-30*), this still serves as a useful example of the way in which Huawei's direct market entry was attempted.

Huawei can be expected to learn both from experience and from studying other companies as it refines its global business model and presence. As it expands into new areas of business and employs new marketing strategies, Huawei can be expected to evolve continually in ways that will facilitate penetration into the United States and other target global markets. After sufficient globalization of its business model, Huawei may continue to move from being an equipment and solution manufacturer/provider to being a foundational shaper of markets. By no longer merely competing within market space boundaries, Huawei may overcome market models that compete with its own in order to redefine the way telecommunications and networking technologies are consumed and perhaps even redefine the market spaces by itself.

Investments take many more forms than simply financial investments or acquisitions. Chinese companies have made thoughtful investments in leading-edge financial practices, management talent, expertise, global engineering, R&D, and training facilities. Consistent with industry practices, many Chinese companies have successfully recruited executives from other major telecommunications companies for decades in an effort to conform to or drive best global management practices.<sup>151</sup> These companies apparently have gone to great efforts to manage, compensate, and retain top talent for expanding market share and achieving corporate earnings growth: for example, Huawei recently recruited a former Nortel executive to run its European operations.<sup>152</sup>

## EXPANSION INTO DEVELOPING MARKETS

China has made its mark in wireless networking products. It is postured potentially to become the global leader in wireless networking worldwide as its networking products become part of infrastructure contributions to developing nations. Developing nations have certain advantages when acquiring technology and communications infrastructures, principally because they are not encumbered by legacy infrastructure. In many cases, they will not need to invest in ground-based infrastructure for telecommunications and can go straight to wireless networks.

<sup>150</sup> *Forbes*, "Nortel's China Syndrome," January 12, 2009.

<sup>151</sup> Kevin Maney, "The New Face of IBM" - "China's biggest IT brand wants to go global. So it bought the PC division - and the world-class management - of an American icon. Who says being 'oceans apart' is a bad thing?" *Wired*, July 2005. <http://www.wired.com/wired/archive/13.07/lenovo.html>.

<sup>152</sup> Cellular News, "Huawei Taps Former Nortel Exec to European Job," July 13, 2009.

Outside of China, Chinese telecom companies have been aggressive in purchasing networks in the developing world. This expansion into emerging markets may have been facilitated in part by western investments in China, which have freed Chinese capital to reach outward for acquisitions in other parts of the world.<sup>153</sup> However, the main driver behind these acquisitions appears to be the PRC's "going out" strategy, intended to encourage China's selected "national champions" to compete in international markets. In regions that may have been underserved for telecommunications products and services, the lower-cost options offered by Chinese firms can be a natural fit.

U.S. corporate investments in China's telecom infrastructure and technical capabilities may be allowing Chinese companies to redirect a very large amount of their investment capital to purchase assets and networks in emerging markets – thereby effectively degrading U.S. competitive postures in these same growth markets when they find themselves competing directly against Chinese firms. In addition, as foreign firms increasingly have their technologies developed and manufactured in China, this provides unique insights to Chinese firms that they are able to use to improve their own products, a trend that will strengthen China's competitive position in both U.S. and global markets.

Recently, China has continued its acquisition approach to building market share in emerging markets.<sup>154</sup> For example, in 2006, China Mobile acquired Millicom International Cellular, which operated mobile telephone services in some of the world's least-developed regions, to include parts of Central America, South America, Africa, and the Asia-Pacific region.<sup>155</sup> As China Mobile expands successfully into emerging markets, other Chinese telecom providers such as Huawei and ZTE also seem likely to displace western suppliers. Developments of this nature can be increasingly negative for western wireless network equipment providers.<sup>156</sup>

Likewise, in February 2007, China Mobile acquired a 100 percent stake in Paktel and renamed the company China Mobile Pakistan. At that time, "[a]ccording to China Mobile Pakistan's COO [chief operating officer] Zafar Usmani, China Mobile had invested \$1.66 billion USD in Pakistan, creating 41,700 job opportunities for the country."<sup>157</sup> Following up on this investment, in February 2009 China Mobile Pakistan announced an additional investment of \$500 million to construct networks and infrastructures in Pakistan under its "Zong" brand.<sup>158</sup>

Other recent deals have continued the pattern of Chinese telecom expansion. In October 2008, China announced a planned investment of \$50 million USD to develop telecommunications facilities in Guinea-Bissau's national post and telecom operator (PTO) Guinea Telecom,

<sup>153</sup> Jason Singer and Jason Dean, "China Mobile Nears \$5.3 Billion Deal For Millicom; Beijing's Biggest Purchase Overseas Would Intensify Push Into Emerging Markets," *China Daily*, May 25, 2006. [http://www.chinadaily.com.cn/world/2006-05/25/content\\_600127.htm](http://www.chinadaily.com.cn/world/2006-05/25/content_600127.htm).

<sup>154</sup> CNNMoney.com, "China's New Frontier, Chinese Telecom gear maker Huawei and ZTE have already conquered Africa and Asia. Next stop: Latin America." June 23, 2009.

<sup>155</sup> Jason Singer and Jason Dean, "China Mobile Nears \$5.3 Billion Deal For Millicom Beijing's Biggest Purchase Overseas Would Intensify Push Into Emerging Markets," *China Daily*, May 25, 2006. [http://www.chinadaily.com.cn/world/2006-05/25/content\\_600127.htm](http://www.chinadaily.com.cn/world/2006-05/25/content_600127.htm).

<sup>156</sup> David Jackson, "China Mobile - Millicom Deal Threatens Ericsson, Nokia, Lucent, Motorola, Qualcomm," SeekingAlpha.com, May 25, 2006. <http://seekingalpha.com/article/11224-china-mobile-millicom-deal-threatens-ericsson-nokia-lucent-motorola-qualcom>.

<sup>157</sup> China Tech News, "Pakistan Welcomes More Chinese Telecom Investment," February 18, 2009. <http://www.chinatechnews.com/2009/02/18/8855-pakistan-welcomes-more-chinese-telecom-investment>.

<sup>158</sup> China Tech News, "Pakistan Welcomes More Chinese Telecom Investment," February 18, 2009. <http://www.chinatechnews.com/2009/02/18/8855-pakistan-welcomes-more-chinese-telecom-investment>.

including the installation of a fiber-optic network to span the entire country, from the border with Senegal in the north to Guinea in the south.<sup>159</sup> Chinese telecoms are also reaching into wealthier nonwestern markets. In April 2009, China Mobile announced its desire to pursue an investment in the Taiwanese telecommunications company Far EasTone.<sup>160</sup> Instead, China Mobile gained approval to set up a subsidiary under its “Zong” brand, which will be used to source telecommunications handsets and equipment.<sup>161</sup>

A clear model has emerged: Chinese companies leverage their inexpensive and plentiful engineers, designers, contractors, and any others needed to build new networks or to upgrade existing networks in these emerging markets.<sup>162</sup> As western markets become saturated, these emerging markets become the growth areas and enable government-influenced telecommunication companies to find attractive new areas for expansion.<sup>163</sup> Where fixed-line infrastructure is poor or limited, cellular networks are much cheaper to roll out and are used as the primary means of communication.<sup>164</sup> As China expands its network influence and infuses its supply chains with propriety standards and equipment, China builds its global influence in the overall standards processes and becomes a much stronger player in developing global standards. By influencing these global standards, China may increase the overall value of its own proprietary intellectual property.

## THE EAST-WEST FLOW OF INVESTMENTS IN THE COMMUNICATIONS SECTOR

Investments between China and the United States have become symbiotic, with results that may not have been immediately apparent at the outset. Chinese and American companies have shared in both the risks and the rewards in their capitalist ventures.<sup>165</sup> While the events cataloged in this report lead to the eventual conclusion that American network security could *potentially* be imperiled, our national security also depends upon how we manage our business relationships with China and how we deal with the successive companies that have been born out of our broad trading framework. National security will not be effectively maintained without economic security.

Through the use of mergers and acquisitions, the aggressive application of sovereign wealth funds, joint ventures, and many other business mechanisms, China is rapidly gaining the

<sup>160</sup> PriMetrica, Inc., “Guinea Telecom to receive USD50m in Chinese investment” (Carlsbad, CA: October 21, 2008). [http://www.telegeography.com/cu/article.php?article\\_id=25675](http://www.telegeography.com/cu/article.php?article_id=25675).

<sup>161</sup> Dow Jones & Company, Inc., “Taiwan stocks on fire on China Mobile-Far EasTone Deal Plan,” *Wall Street Journal* Digital Network, MarketWatch, Inc., Asia Markets, April 29, 2009. <http://www.marketwatch.com/story/china-mobiles-taiwan-plan-could-change-everything>.

<sup>162</sup> Chinmei Sung and Janet Ong, “Taiwan Opens 100 Industries to Chinese Investment (Update2),” Bloomberg, June 30, 2009. <http://www.bloomberg.com/apps/news?pid=20601080&sid=aFeN1SK55G7U>; and NetworkWorld, “China Mobile Wins Approval for Taiwan Subsidiary,” May 11, 2010.

<sup>163</sup> Jason Singer and Jason Dean, “China Mobile Nears \$5.3 Billion Deal For Millicom Beijing's Biggest Purchase Overseas Would Intensify Push Into Emerging Markets,” China Daily Information Co. (CDIC), May 25, 2006. [http://www.chinadaily.com.cn/world/2006-05/25/content\\_600127.htm](http://www.chinadaily.com.cn/world/2006-05/25/content_600127.htm).

<sup>164</sup> Jason Singer and Jason Dean “China Mobile Nears \$5.3 Billion Deal For Millicom Beijing's Biggest Purchase Overseas Would Intensify Push Into Emerging Markets,” China Daily Information Co. (CDIC), May 25, 2006. [http://www.chinadaily.com.cn/world/2006-05/25/content\\_600127.htm](http://www.chinadaily.com.cn/world/2006-05/25/content_600127.htm); and Reuters, “Russia's MTS (WHAT IS MTS?) picks Huawei for 3G Armenia Network,” January 16, 2009.

<sup>165</sup> Jason Singer and Jason Dean “China Mobile Nears \$5.3 Billion Deal For Millicom Beijing's Biggest Purchase Overseas Would Intensify Push Into Emerging Markets,” China Daily Information Co. (CDIC), May 25, 2006. [http://www.chinadaily.com.cn/world/2006-05/25/content\\_600127.htm](http://www.chinadaily.com.cn/world/2006-05/25/content_600127.htm).

<sup>166</sup> *Wall Street Journal*, “China Ready to Place Bets on Hedge Funds,” June 19, 2009.

potential for establishing global dominance in the telecommunications sector. Significant investments have been made in the communications sector over the last two decades, with substantial escalation occurring over the last ten years and increasing escalation over the most recent five years. These investments parallel the overall growth of Chinese investments in the United States and U.S. investments in China.

Some U.S. venture funds and hedge funds have targeted China exclusively in an effort to generate both growth and higher yields in their portfolios and to take advantage of China's burgeoning infrastructure build-out.<sup>166</sup> Many major venture capital and private equity firms have looked toward China for growth. Billions of dollars from firms such as Draper Fisher, Sycamore Ventures, The Carlyle Group Asia, Intel Capital (the venture arm of Intel), Softbank Asia, JP Morgan Asia – all firms with strong U.S. roots or investment ties – have been invested in Chinese telecommunications ventures since the early 2000s. Many of these companies are now publicly traded on exchanges like the NASDAQ, NYSE, FTSE, and NIKKEI.<sup>167</sup>

China has announced continued network investment at home on next-generation wireless technologies, potentially reaching 280 billion RMB (~\$44B USD) in 2009.<sup>168</sup> Faced by an ongoing financial crisis in the United States, some U.S. venture firms have announced a renewed investment strategy in China's infrastructure.<sup>169</sup> Networks of investment, venture capital, hedge funds, other financial instruments, and management entities seem almost as interconnected today as the technologies themselves.

China has also moved forward aggressively on an array of European partnerships that allow rapid growth in space-based communications markets.<sup>170</sup> This is due to the fact that companies from China are not only investors in foreign firms but are also investors in China's own "home-grown" manufacturing talent and capabilities base. Chinese companies have used mergers, acquisitions, and international partnerships to steadily and rapidly increase China's home-grown technologies – which, in many cases, might be more accurately identified as "grafted foreign hybrids."

Chinese companies have also made considerable investments through sovereign wealth funds in numerous hedge funds and investment banks. For example, Beijing Wonderful Investments/The China Investment Corporation recently took an expanded 12.5 percent stake in Blackstone Group.<sup>171</sup> Blackstone's private equity group has, over the years, taken stakes in companies like T-Mobile (one of the largest wireless cellular carriers in the global market, including the United States), TDC Telecom, Sungard (provider of backup, disaster recovery, and storage solutions – provider of critical disaster recovery services to the U.S. government), Global Tower (an operator of towers for wireless networks), NewSkies (a broadband satellite communications company), TRW Automotive, Charter Communications, Adelphia Communications (cable), iPCS (wireless communications provider), and StorageApps (provider of storage area networking solutions).<sup>172</sup>

<sup>166</sup> *New York Times*, "Silverlake Eyes Asia Tech Investments," November 28, 2008.

<sup>167</sup> Asia Private Equity Review, April 2006; China C SR [corporate social responsibility], May 27, 2008.

<sup>168</sup> *China Daily*, "China Finally Awards Telecom Operators 3G Wireless," January 7, 2009.

<sup>169</sup> Annual Reports and 10K filings, Carlyle Group website. [www.carlyle.com](http://www.carlyle.com).

<sup>170</sup> Alcatel Alenia Press Release, "Alcatel Alenia Space Wins New Communication and Broadcast Satellite Contract Chinasat 6B From ChinaSatcom, Bolstering Cooperation With China," redOrbit.com, December 5, 2005.

<sup>171</sup> Blackstone 10K Filing 2009. Annual Report and consolidated financial statements.

<sup>172</sup> The Blackstone Group. <http://www.blackstonegroup.com>.

Patterns of these investments suggest the potential for a continual increase of Chinese investments in global business markets, which might also provide deep access by PRC government-influenced or controlled actors to both influential foreign companies and to sensitive communications networks. However, as with any investment, it is also possible that investments and relationships such as these continually will open doors to new opportunities to expand business lines and portfolios constructively. Many American businesses have embraced strong ties with Asian companies over the last few decades, and the American consumer less frequently associates negative brand identity with Chinese technology products, particularly when they are paired with major American, Japanese, or European brand identities.

## SECTION 2

# POTENTIAL VULNERABILITIES IN COMMUNICATIONS INFRASTRUCTURE AND PRODUCTS, AND CHINESE INVESTMENTS IN THESE SECTORS

*Note: This report mentions only a few actors and fields of technology, representing a fraction of the various actors, technologies, and relationships present in the communications sector. They were selected because references are often more readily available or particularly noteworthy. Although valid examples, they may not be fully representative of the overall sector environments themselves.*

Efforts to analyze potential technological risks are often plagued by a failure to account for the continuous nature of technological innovation, difficulties associated with “control dilemmas,”<sup>173</sup> and faulty assumptions of a continuity of currently prevailing trends. New technologies are constantly evolving, and U.S. technological competitiveness will be challenged frequently in the future and from many quarters. As applies to this analysis, U.S. policymakers and industry officials cannot fully understand and appreciate the risks of China’s rising influence in the communications sector until that influence has become somewhat manifest. Nevertheless, working continually toward reasonable forecasts of risks is necessary in light of the potential national security stakes involved.

## INVESTMENTS IN LONG-HAUL FIBER

Fiber is being used extensively worldwide as the primary means of high-bandwidth communication, to include advanced digital video and data and high-speed Internet and telephony applications. In the past few years, the number of new fiber connections has outpaced the number of new copper cable connections, principally due to the superior performance of fiber technology.<sup>174</sup> Fiber has become the transport technology of choice because it has thousands of times the bandwidth of copper wire and can carry signals hundreds of times farther before needing a repeater. Most carrier-level or business network backbones are fiber-based using Ethernet standards.<sup>175</sup>

Insofar as sensitive U.S. data are transported across global undersea networks, the data are vulnerable to interception or interference by hostile actors but perhaps only by degrees more so than before. Hacking into optical networks is not overly difficult. Perhaps the easiest and consequently most undetectable means is simply bending a cable, as this will allow a small (but sufficient amount) of light to leak from the cable without actually breaking connections – something that operations engineers try to be very quick to notice and investigate. A “tap” is completed by using commercially available couplers to place a microbend in the cable to allow light to radiate through the cladding and be exposed to a photodetector. The photodetector is connected to an electro-optical converter that acts as an interface to a network interface card. This tap allows the data being transmitted through the cable to be intercepted and “sniffed” for

<sup>173</sup> A “control dilemma” relates to the fact that the catastrophic risks of new changes and technologies often cannot be known until they have been implemented to the degree necessary for the risks to be incurred.

<sup>174</sup> InfoTech News, “Research and Markets: Gigabit Ethernet Fiber and Copper Cabling Systems,” TMCNET.com, April 15, 2010.

<sup>175</sup> Cisco website. <http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Ethernet.pdf>.



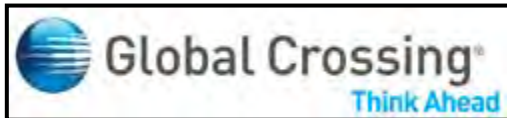
desired information in much the same way as any network data may be compromised.<sup>176</sup>

Splicing is another method for tapping fiber optic cables but is much more difficult to perform successfully, as it usually results in briefly breaking the connection, which may lead to detection. When millions of connections are severed, even momentarily, this is noteworthy and will possibly lead to an investigation of the event by affected carriers.<sup>177</sup>

The potential for disruption of communications through undersea cables was seen in December 2006 when an earthquake broke cables in the South China Sea between Taiwan and the Philippines, disabling 90 percent of the region's telecommunications capacity. It was demonstrated again in January and February 2008 when cables in Middle Eastern waters were reportedly broken by stray ship anchors. The cable outages disrupted a wide variety of communications, to include the ability of the U.S. military's Central Command to communicate with facilities and units in Iraq and Afghanistan.<sup>178</sup>

Whether fiber is cut by accident, by design to disrupt communications, or hacked to intercept sensitive data, the threat to national security can be significant. All fiber networks consist of complex electronic components, many of which are manufactured outside of the United States. These components could form another source of insecurity, as they can be infected with malicious code such as kill switches, Trojan horses, worms, or many other harmful features during the manufacture process. Repair parts<sup>179</sup> and diagnostic tools also can be a source of malware exposing fiber communications to third-party eavesdropping. The United States has placed itself in a position of relying on other countries for much of its technology infrastructure, a set of circumstances with serious implications for network security. (For more on this subject, see sec. 3 of this report, "Supply Chain Integrity, and the Impact on Government/Defense Contracting.")

**The Security of Optical Fiber Networks,  
and the Case of Global Crossing and Hutchison-Whampoa**



Global Crossing Company Logo  
Source: Global Crossing.com.



Hutchison Whampoa Company Logo  
Source: Hutchison-Whampoa.com.

In late 1999, an aggressive global fiber optic build-out was in progress as the Internet boom pushed the development of optical fiber networks to carry greater traffic loads at increasing speeds. This spurred increased construction of an undersea fiber to bridge high-density points in Asia and Europe. Global Crossing, a holding company based in Bermuda with significant U.S. and global interests, made significant investments in high-capacity undersea fiber routes, ultimately establishing a "\$20 billion global fiber optic network [that] crosses both the Atlantic and Pacific Oceans and connects twenty-seven countries in Asia, North and South America and

<sup>176</sup> Sandra Kay Miller, "Hacking at the Speed of Light," SecuritySolutions.com, April 1, 2006.

<sup>177</sup> Sandra Kay Miller, "Hacking at the Speed of Light," SecuritySolutions.com, April 1, 2006.

[http://securitysolutions.com/mag/security\\_hacking\\_speed\\_light](http://securitysolutions.com/mag/security_hacking_speed_light).

<sup>178</sup> James Geary, "Who Protects the Internet?" *Popular Science*, March 13, 2009.

<sup>179</sup> Reperi - Integrated circuits (ICs) can be altered to introduce malware into the hardware. That includes replacement parts that consist of ICs. Specifically, fiber uses transceivers and multiplexers along with other equipment. Any of these devices can be sources of malware.



Europe.”<sup>180</sup> Global Crossing’s interests have been strategically significant because of the depth of its holdings in undersea cable connecting key strategic transport routes and its exposure to U.S. government communications traffic through substantial holdings and the holdings of subsidiaries.

*Figure 4: Global Crossing Networks in 2010*



*Source: Global Crossing, "Carrier Overview," 2010.*

Overestimating demand and timing caused a telecommunications bust cycle in the early 2000s, resulting in bankruptcy filings by long-haul fiber carriers. Hutchison Whampoa had a \$400 million convertible bond stake in Global Crossing at the time Global Crossing entered bankruptcy in 2002. In early 2002, Singapore Telecom (ST Telemedia) and Hutchison Whampoa of Hong Kong attempted to acquire a majority stake in Global Crossing’s network assets at a price of \$750 million).<sup>181</sup> Hutchison Whampoa subsequently withdrew from the purchase agreement and ST Telemedia exercised its option under the purchase agreement to assume all of Hutchison’s rights and obligations, purchasing a 61.5 percent stake in Global Crossing (reorganized following bankruptcy) for \$250 million.<sup>182</sup> These actions were taken due to ongoing CFIUS objections to the potential role of Hutchison Whampoa.<sup>183</sup> *(For more on telecom deals that ran afoul of CFIUS, see pp. 30-33.)*

Hutchinson Whampoa is Hong Kong’s largest multinational conglomerate, operating in 54 countries worldwide. The company holds a broad range of investments, from health and beauty products to port operations, property development, and telecommunications.<sup>184</sup> To date, Hutchison Whampoa is the largest company traded on the Hong Kong Stock Exchange, with a

<sup>180</sup> James Lewis, “CFIUS - The Committee on Foreign Investment in the United States” (Washington, DC: Center for Strategic and International Studies, February 2006). [http://csis.org/files/media/csis/pubs/060212\\_cfius.pdf](http://csis.org/files/media/csis/pubs/060212_cfius.pdf).

<sup>181</sup> Global Crossing Press Release, “Hutchison Whampoa Limited and Singapore Technologies Telemedia Pte. Ltd. Plan to Invest \$750 Million in Global Crossing,” January 8, 2002.

<sup>182</sup> Global Crossing Press Release, “ST Telemedia Increases Proposed Stake in Global Crossing,” April 30, 2003; and Global Crossing 2003, 2004 10K SEC [Securities and Exchange Commission] filings.

<sup>183</sup> James Lewis, “New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure, and Communications Interception,” *Federal Communications Law Journal* (June 2005).

<http://www.law.indiana.edu/fcli/pubs/v57/no3/Lewis.pdf>.

<sup>184</sup> Hutchison Whampoa Limited, About HWL. <http://www.hutchison-whampoa.com/eng/about/overview.htm>.

total market capitalization of HKD \$205.7 billion.<sup>185</sup> The company was British owned until 1979, when Hong Kong and Shanghai Banking Corporation (HSBC) sold its controlling 22 percent stake to Cheung Kong Holdings, owned by Hong Kong tycoon Li Ka-Shing, for HKD \$639 million.

Commonly referred to in Hong Kong as “Superman,” Li Ka-Shing is the 11th richest man in the world, with a net worth of USD \$23.1 billion, making him the richest man in Asia.<sup>186</sup> Mr. Li maintains close ties to the Chinese government. He is a director of the China International Trust and Investment Corporation (CITIC), a state investment arm operated by the China government, and also serves on several state advisory bodies.<sup>187</sup> According to James Lewis, a research fellow with the Center for Strategic and International Studies:

*“The crux of the opposition to Hutchison was the company’s alleged connections to the Chinese government. Senior Chinese government officials are reputedly among Hutchison’s stockholders. The Department of Defense and others feared that China could use this investment relationship to influence Hutchison and particularly to obtain access to Global Crossing’s communications networks... Hutchison is clearly a legitimate, commercial, publicly-traded entity with a long history of business success, but Chinese intelligence entities have used their ownership stake in foreign companies as a means to obtain controlled technology. The fear that the Chinese government, if given the opportunity, would extend the use of this technology to collect communications is not an unreasonable fear.”<sup>188</sup>*

## ROUTERS, SWITCHES, AND HUBS

Routers are used to connect users between networks, while switches and hubs are used to connect users within a network. With advances in technology, many routers are now designed to perform the functions of switches and hubs as well as other security services such as intrusion detection/prevention and antivirus scanning. Routers have become the “Swiss army knife” of networking. Most networks are designed for redundancy and have multiple routers so that the failure of a few will not cause a complete network outage. In the case of an outage, routing tables of the remaining routers are reconfigured, and the network continues functioning, although at a reduced level until faulty routers can be repaired or replaced.

Typically, network customers subscribe with an Internet service provider (ISP) or carrier to transport their traffic between networks. When traffic is destined for a network using a different ISP as their carrier, some means must be provided to hand the traffic off to the other carrier for final delivery to the destination. Carriers may enter into their own teaming or peering

<sup>185</sup> *Bloomberg Businessweek*, HUTCHISON WHAMPOA LTD (13: Hong Kong).

<http://investing.businessweek.com/research/stocks/snapshot/snapshot.asp?ticker=13:HK>.

<sup>186</sup> Michael Schuman, “The Miracle of Asia’s Richest Man,” *Forbes*, February 24, 2010.

<http://www.forbes.com/2010/02/24/li-ka-shing-billionaire-hong-kong-richest-opinions-book-excerpt-michael-schuman.html?boxes=HomepageLighttop>.

<sup>187</sup> Stephen Vines, “The Other Handover,” *TIMEasia*, August 6, 2005.

[www.time.com/time/asia/2005/journey/hutchison.htm](http://www.time.com/time/asia/2005/journey/hutchison.htm).

<sup>188</sup> James Lewis, “New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure, and Communications Interception,” *Federal Communications Law Journal* (June 2005).

<http://www.law.indiana.edu/fclj/pubs/v57/no3/Lewis.pdf>. Others have also voiced concerns about Hutchison Whampoa: for example, former Senate Majority Leader Trent Lott once went so far as to allege that Hutchison Whampoa is “an arm of the People’s Liberation Army.” See *Economist*, “Keeping Out Li Ka-Shing,” May 3, 2003. However, a detailed examination of these allegations, or a deeper study of the background of Hutchison Whampoa, is beyond the scope of this report.

arrangements to handle such traffic or use an Internet exchange point (IXP) that has been set up for this specific purpose. An Internet exchange point is the physical infrastructure that allows ISPs to exchange Internet traffic between their networks by means of mutual peering arrangements that allow traffic to be exchanged without cost. These IXPs use a host of networking equipment, including sophisticated routers and switches to enable traffic to be properly routed.

This equipment is comprised of integrated circuits that can be severely impacted through malicious circuits that modify functionality or include backdoors and/or kill switches. Although a hostile actor manufacturing such products could conceivably target all integrated circuits to be used in routers, they might instead target integrated circuits used in the most sophisticated equipment, thus assuring the maximum amount of damage per individual attack. Following this line of reasoning, the Internet in the United States could theoretically be brought down or severely disrupted because the routers and switches serving the IXPs were disabled and traffic could no longer be routed between networks, except where carriers had their own private peering arrangements. Generally, the larger the network, the more sophisticated the equipment (such as routers and switches) becomes. Arguably, by focusing on the larger classes of routers and switches, a potential enemy could disrupt the most traffic and cause the greatest amount of harm with the fewest resources expended in an attack.<sup>189</sup>

However, this does not preclude strategies based on attacking large numbers of lower-end equipment components. Cyber attacks can be shaped in many different ways and attack the full spectrum of systems and networks. Depending on which effects are desired and tools that are available, cyber attackers may use old techniques to attack new systems effectively or may find that the massive effects of attacks based on using multitudes of smaller compromised components (workstations, access points, low-end routers, smart phones, etc.) can easily outweigh the effects of attacking higher-end systems or networks.

One of the central reasons that the proposed purchase of 3Com by Bain Capital and Huawei proved so controversial was the prominent position of 3Com in the router market. As a manufacturer of routers, switches, and hubs, 3Com had equipment that was often found in the heart of telecommunications networks and provided connectivity into some of the most secure areas of critical infrastructures. 3Com was also a significant provider of data communications equipment to the U.S. federal government.<sup>190</sup> (*For a fuller account of the abortive deal between 3Com and Huawei, see pp. 28-30.*) The U.S. companies Cisco and Juniper still hold a large share of the global high-end router market; however, Huawei is growing quickly and expanding worldwide, causing U.S. companies to lose ground.<sup>191</sup>

<sup>189</sup> Reperi – nonpublic research - there are numerous vectors for attacks intended to have a large-scale impact, and the possibility of massive attacks at large numbers of smaller routers is very real. However, some consider striking at large routers to be more attractive.

<sup>190</sup> Reuters, "Opposition Leads Bain to Call Off 3Com Deal," March 21, 2008.

<http://www.nytimes.com/2008/03/21/technology/21com.html>; and *Cajing China* (English version), "The 3Com Deal, Behind the Security Flap," October 23, 2007.

<sup>191</sup> "Cisco and Juniper's combined market share fell from 69% in 2008 to 59% in 2009. Huawei and Alcatel-Lucent gained much of the share these companies lost." See TelecomsEurope.net, "Cisco, Juniper Lose Routing Market Share in 2009," February 22, 2010. <http://www.telecomseurope.net/content/cisco-juniper-lose-routing-market-share-2009>.

## WiMAX/WiFi – NETWORK AND NETWORK CONTROL DEVICES AND PROTOCOLS FOR WIRELESS NETWORKING

Over the past decade, WiFi (wireless fidelity) has significantly raised the amount of interest in the wireless market. It is quickly becoming a replacement for or addition to wireline Ethernet in the business community and the access method of choice in the home. The creation of WiFi hot spots in locations such as airports, hotels, and coffee houses offers greater user mobility in connecting to service providers for data and voice transmissions. There are multiple standards in widespread use today, including 802.11a, 802.11b, 802.11g, and fairly recent developments such as 802.11n. The difference in each is in the frequency spectrum and modulation technology use, and the transmission rates available.

Worldwide Interoperability for Microwave Access (WiMAX) is a relatively new standard approved in January 2003 that will offer a last-mile alternative to digital subscriber line (DSL) and cable modem service, promising to lead to ubiquitous, continuous, mobile wireless connectivity. Huawei makes this type of equipment and will become a vendor to Clearwire Communications as the company rolls out 4G services at multiple locations in the United States. WiMAX can provide broadband on demand or last-mile wireless access to speed the deployment of IEEE 802.11 WiFi hotspots and wireless LANs. Public safety trials among various network providers in the United States have included utilizing WiMAX combined with Land Mobile Radio (LMR) applications to deliver public safety communications between multiple law enforcement and emergency responders. Clearwire has been quoted in the press regarding its intent to offer public safety solutions over its network.<sup>192</sup> Sprint Nextel is a major equity investor in Clearwire.<sup>193</sup>

Understanding China's internal domestic telecommunications market is essential to understanding Chinese communications investments in U.S. companies and around the world. China's own market for wireless communications has made it an attractive target for U.S. investment and an inexpensive development and manufacturing hub for wireless technologies. In the wireless world, it presents the mass market of mass markets, where manufacturing for wireless equipment can more easily cultivate economies of scale.

China began issuing 3G licenses for its internal spectrum in January 2009. The first three companies receiving licenses were China Mobile (TD-SCDMA - the domestically developed 3G standard), China Telecom (CDMA2000 - U.S. developed), and China Unicom (WCDMA - Europe developed).<sup>194</sup> The Chinese Ministry of Industry and Information Technology provided regulatory oversight for 3G network operation, dealing with competition, consumer rights, security, telecom charges management, and facilities.<sup>195</sup>

---

<sup>192</sup> WiMAX is a telecommunications technology providing wireless transmission of data using a variety of transmission modes, from point-to-multipoint links to portable and fully mobile Internet access. Based on the IEEE 802.16 standard (Broadband Wireless Access), WiMAX can be thought of as a more powerful relative of WiFi. For directional use, under ideal conditions WiMAX can reach between line-of-sight points for as far as 20 miles or more to connect local hotspots into a larger wireless wide-area network. Meanwhile, WiMAX hotspots can be as much as five or six miles across. A user may have a WiFi hotspot in their home that talks to a WiMAX hotspot in their neighborhood, which is connected to a WiMAX backbone that connects to the Internet at a distant location.

<sup>193</sup> Clearwire Press Release, May 7, 2008.

<sup>194</sup> *China Daily*, "China's telecom sector gets 3G licenses," January 7, 2009.  
[http://www.chinadaily.com.cn/bizchina/2009-01/07/content\\_7375721.htm](http://www.chinadaily.com.cn/bizchina/2009-01/07/content_7375721.htm).

<sup>195</sup> *China Daily*, "China's telecoms sector gets 3G licenses," January 7, 2009.  
[http://www.chinadaily.com.cn/bizchina/2009-01/07/content\\_7375721.htm](http://www.chinadaily.com.cn/bizchina/2009-01/07/content_7375721.htm).



At the same time, China has been making massive investments in 4G technology. The “Next-Generation Broadband Wireless Mobile Communications Network” began in 2008 and will stretch over 15 years, with total spending expected to reach 70 billion RMB (close to \$10 billion USD).<sup>196</sup> China has been trying to promote its own standards for international adoption but has yet to achieve this goal. The network standard LTE is considered to be the next standard for replacing and upgrading 3G/4G systems and includes both frequency division and time division duplexes.<sup>197</sup> TeliaSonera, a Scandinavian telecom company, launched the first live LTE 4G services in Norway and Sweden in December 2009 using Huawei infrastructure in the Norway deployment. China Mobile launched the world’s first TD (time division) LTE network recently providing download speeds ten times faster than 3G networks.<sup>198</sup> A significant number of LTE trials are already underway worldwide with Huawei having premier product entries in this market segment.

### **Huawei and the Development of LTE Standards**<sup>199</sup>

Long-Term Evolution (LTE) is a “high performance air interface for cellular mobile telephony,”<sup>200</sup> and many of the world’s leading telecommunications firms (including Verizon Wireless and AT&T) are working on potentially converting their networks to LTE technology.<sup>201</sup> The emergence of the LTE standard is the result of collaboration between telecommunications industry associations in Europe, Japan, China, South Korea, and North America. A number of international corporations are competing or collaborating in this market space, to include Cisco (United States), Ericsson (Sweden), Huawei (China), LG Technologies (Korea), Motorola (United States), Nokia Siemens Networks (Finland), Samsung (Japan), and ZTE (China).

Huawei has set for itself a strategic goal to become an industry leader in fixed wireline networks, wireless networks, and network switch segments worldwide. By spring of 2009, Huawei had become number two globally in the fixed wireline and network switch segment and number three in the wireless segment. Within the wireless segment, Huawei is investing considerable resources in the development of LTE technology.<sup>202</sup> Huawei has been involved with LTE research and development since 2004 and as of July 2010 had “been awarded 14 LTE commercial contracts and more than 60 LTE trials, including the world’s first commercial LTE network in Oslo, Norway... [Huawei] intends to remain ahead of the industry curve by providing leading edge and customer-specific LTE solutions to allow operators around the world to establish and maintain long-term, competitive LTE leadership.”<sup>203</sup>

Interlocutors speaking on behalf of Huawei have cited the company’s superior position in LTE technology as a compelling reason for western telecom companies to adopt its products. Huawei’s products are not necessarily superior to those of other suppliers worldwide: they are comparable in some ways and inferior or superior in others, depending on relative product development strategies. However, Huawei is competing fiercely in the entire LTE business model, to include services and management, and it might be able to position its product

<sup>196</sup> Kaiser Kuo, “China’s 4G Master Plan,” February 26, 2008. <http://digitalwatch.ogilvy.com.cn/en/?p=205>.

<sup>197</sup> Kaiser Kuo, “China’s 4G Master Plan,” February 26, 2008. <http://digitalwatch.ogilvy.com.cn/en/?p=205>.

<sup>198</sup> CNET News, “TeliaSonera Launches First LTE 4G Network,” December 14, 2009; and Richard Wilson, “China Goes for 4G LTE in a Big Way,” Electronicsweekly.com, July 29, 2009.

<sup>199</sup> The information in this section is based primarily on analysis provided to the Commission by Reperi LLC.

<sup>200</sup> See the entry for “LTE” in the glossary of this report, p. 97.

<sup>201</sup> Wireless Industry News, “AT and T Starts Building its LTE Network,” February 11, 2010.

<http://www.wirelessindustrynews.org/news-feb-2010/1836-021110-win-news.html>.

<sup>202</sup> Analysis provided to the Commission by Reperi LLC.

<sup>203</sup> Huawei website, “LTE Overview.” [http://www.huawei.com/radio\\_access\\_network/lte.do](http://www.huawei.com/radio_access_network/lte.do).

offerings to be less expensive than those of its competitors. U.S. telecommunications companies are under intense pressure to control costs, which may be forcing them to elevate pricing as a higher consideration than might otherwise have been the case.

The United States is currently faced by an accelerating technology paradigm shift in certain sectors, particularly telecommunications, in which foreign companies are moving into the position of being gatekeepers of standards in advanced technologies. Current-day decisions made by telecommunications companies regarding infrastructure build-outs will affect their business for years to come, and the question of which technology provider is likely to emerge as the industry leader is significant: "These telecom companies cannot afford (in a practical business sense) to choose a horse that won't win... *If current trends continue... going with products from someone like Huawei might be viewed as a business survival decision, regardless of [any] potential security risks.*"<sup>204</sup>

## APPLICATIONS SOFTWARE

### Software/Controllers/Drivers

Networking equipment relies on controllers and/or drivers with associated software to deliver the functionality for which the equipment was designed. Since controllers may be embedded as integrated circuits in computer motherboards, routers, expansion cards, printer interfaces, or USB (universal serial bus) devices, they are subject to malicious actors inserting vulnerabilities that can render a device useless upon activation of a "kill" switch or changing the functionality in a way that reduces security by leaking or corrupting sensitive data. Controllers and drivers implemented through software are also potential sources of security vulnerabilities. Well-positioned actors with malicious intent can easily add viruses and other malware such as Trojans, worms, rootkits, spyware, and other malicious and unwanted software.

Applications software in wireless handsets, smart phones, and other network devices is one of the crucial components of overall wireless telecommunications solutions. TechFaith Wireless is a joint venture between Qualcomm and China's Techfaith to produce inexpensive software for wireless handsets.<sup>205</sup> Qualcomm is a manufacturer of wireless airlink technologies, chipsets, consumer electronics, hardware, mobile content services, secure phones, satellite phones (Globalstar), repeaters, wireless charging, and other devices.

## NETWORK SECURITY PRODUCTS

### Security Software

A trend is emerging of Chinese investment in network security companies and network security software and device manufacturing. In 2008, Huawei announced a joint venture with Symantec, a U.S. manufacturer of network security products best known for its popular antivirus software.<sup>206</sup> (See *text box on the following page.*) It is natural for communications manufacturers to gravitate to the network security space. However, as foreign companies gravitate to these parts of the supply chain, foreign network security products gain the potential

<sup>204</sup> Analysis provided to the Commission by Reperi LLC.

<sup>205</sup> AllBusiness.Com, "Qualcomm, China TechFaith Create Wireless Company," March 27, 2009.

<sup>206</sup> Symantec Press Release, "Huawei and Symantec Commence Joint Venture," February 5, 2008. "...the company will develop and distribute world-leading security, and storage appliances to global telecommunications carriers and enterprises, and the transaction has satisfied all closing conditions received all required government and regulatory approvals..."

ability to be implemented in sensitive infrastructures unnoticed. China's technology manufacturers are increasingly moving into this security realm to meet their own growing needs, and their products therefore are appearing in global networks more frequently.

### **The Creation of Huawei Symantec**



**Huawei  
Symantec**

*Huawei Symantec Company Logo*

In February 2008, Huawei Technologies and the U.S.-based network security firm Symantec announced the creation of a joint venture to “develop and distribute world-leading security and storage appliances to global telecommunications carriers and enterprises.” The resulting joint venture, “Huawei Symantec,” was created with Huawei owning a 51 percent share of the company and Symantec owning a 49 percent share. John W. Thompson, chairman and chief executive officer of Symantec, serves as chairman of the board; Ren Zhengfei, chief executive officer of Huawei, serves as chief executive officer.

According to the company's website, it employs over 4,000 people and has expanded from its Chengdu headquarters into R&D centers in Chengdu, Beijing, Shenzhen, and Hangzhou. The company describes its mission as “combin[ing] Huawei's expertise in telecom network infrastructure and Symantec's leadership in security and storage software to provide world-class solutions” for network security and storage.<sup>207</sup>

The lack of transparency surrounding the operations and management of Huawei Technologies,<sup>208</sup> as well as the role of Symantec in designing and marketing network security products, could raise concerns in some quarters regarding potential national security issues associated with the joint venture. However, no specific allegations have been made against the company, and it has emerged as a significant competitor in the network security field.<sup>209</sup>

An important consideration in the market space for network security products is “technology refresh.” If network protocols advance beyond the technical capabilities of security hardware, there are dangers of networks having traffic that is unmonitored passing through security zones undetected. An example would be IPv6 packets being tunneled through an IPv4 capable-only firewall. Theoretically, some elements of the IPv6 traffic could breach security without notice.<sup>210</sup>

Protecting telecommunications networks and the equipment and data that comprise these networks is essential to national security. Protection may be in the form of antivirus software

<sup>207</sup> Huawei Symantec website, “About Huawei Symantec.”

[http://www.huaweisymentec.com/en/About\\_Us/Company\\_Information/Company\\_Introduction](http://www.huaweisymentec.com/en/About_Us/Company_Information/Company_Introduction).

<sup>208</sup> See discussion of Huawei's management structure on page 15 of this report. See also Kevin O'Brien, “Upstart Chinese Telecom Company Rattles Industry as It Rises to No. 2,” *New York Times*, November 29, 2009; and Kevin Eagles, “Huawei Needs To Be More Open on Security If It Is To Become a Global Player,” *SC Magazine (UK)*, November 6, 2009.

<sup>210</sup> For a list of the company's products and services, see Huawei Symantec website, “Products & Solutions.”

[http://www.huaweisymentec.com/en/Product\\_Solution](http://www.huaweisymentec.com/en/Product_Solution).

<sup>210</sup> Network World, “Invisible IPv6 Traffic Poses Serious Network Threat,” July 13, 2009.



and the hardware/software comprising the various security appliances discussed above. Computer security is enhanced through the use of three processes: prevention, detection, and response. A failure in any of these processes could leave systems open to intrusion, with serious consequences. In the current environment of technology outsourcing, the opportunities for hostile nations to compromise U.S. security through the manipulation of security software or hardware used in critical infrastructure has increased dramatically. Reacting only when the threat materializes may prove to be far too late. The selection of sources for network security software and hardware begs careful consideration.

## HANDSETS AND SMART PHONES

As the manufacture of mobile phone handsets and associated software moves to offshore outsourcers along with other technology equipment, security potentially could be compromised by actors with hostile intentions, thereby placing at risk one of the most widely used forms of communications in the United States.

Both of China's two largest telecom equipment companies, ZTE and Huawei, are amassing significant market share in the handset sector. Many of these handsets are made to work with 4G technologies (next-generation wireless). The Asian market has been an early adopter of standards that would allow 4G wireless technologies to expand rapidly; having the ability to roam freely across many types of networks is an essential element of handset compatibility. Many developing nations in South America, Africa, and Europe have followed suit.<sup>211</sup>

Huawei and ZTE's product lines compete with Motorola, Ericsson, LG, Samsung, and Apple. As markets shift, competition forces market participants to change relationships in order to adapt to new or emerging conditions. Most of these companies have agreements with one another to work together and develop certain product applications in order to stay competitive. According to press reports, Huawei and ZTE have been focused on developing, manufacturing, and selling technologically savvy, lower-cost products as Huawei moves to occupy market niches.<sup>212</sup> Both Huawei and ZTE have typically introduced their mobile phones into the United States and other markets through relabeling for companies like Verizon Wireless and T-Mobile. Huawei's new Android smart phone, manufactured for T-mobile, is a touch screen and Android-powered hand set. (The Android operating system and application technology model was initially developed by Google and then shifted to an open source alliance.) Android has an open software standard that moves easily between networks and protocols and features Google search, utilities, and applications capabilities. These features make the Huawei Android phone a competitive new entrant into the U.S. wireless market.

*Figure 5: A T-Mobile UK "Pulse" Smartphone with Huawei Android Technology*

<sup>211</sup>Firoze Manji and Stephen Marks, "African Perspectives on China in Africa," Fahamu--Network for Social Justice, 2007.

<sup>212</sup>CNNMoney.com, "China's New Frontier," June 25, 2009.



Source: Google Images.

There were some indications in early 2010 that the computer firm Lenovo might be taking steps to consider further acquisitions in the North American market. Speculation also appeared in the business press in spring 2010 that Lenovo might make a bid for Palm, with an eye toward getting into the smartphone market.<sup>213</sup> However, no confirmed action has occurred on such a deal as of the writing of this report. *(For further discussion of the controversy surrounding the sales of Lenovo equipment to the U.S. government, see pp. 66-68 of this report.)*

## HANDSETS AND SMART PHONES: POTENTIAL VULNERABILITIES

How telephones/handsets are attacked is a useful study for understanding the vulnerabilities of communications equipment to malicious activity. From botnets<sup>214</sup> to SMiShing (SMS phishing) to battery draining,<sup>215</sup> the wireless handset is one of the latest and most favored vectors for

213 Kit Eaton, "Lenovo Wants in on Smartphone Biz, Acquiring Palm Could be the Ticket," *Fast Company*, April 19, 2010. <http://www.fastcompany.com/1620623/lenovo-mobile-internet-smartphones-finances-growth-palm-palm-os-pre-pixi?#>.

214 Fox News Network LLC, "Experts: Zombie Cell-Phone Hack Attacks May Be Next," October 16, 2008. <http://www.foxnews.com/story/0,2933,438481,00.html> : "[S]ome of the most vicious Internet predators are hackers who infect thousands of PCs [personal computers] with special viruses and lash the machines together into 'botnets' to pump out spam or attack other computers. Now security researchers say cell phones, and not just PCs, are the next likely conscripts into the automated armies. The mobile phone as zombie computer is one possibility envisioned by security researchers from Georgia Tech in a new report coming out Wednesday. The report identifies the growing power of cell phones to open a new avenue of attack for hackers. Of particular concern is that as cell phones get more computing power and better Internet connections, hackers can capitalize on vulnerabilities in mobile-phone operating systems or web applications. Botnets, or networks of infected or robot PCs, are the weapons of choice when it comes to spam and so-called 'denial of service attacks,' in which computer servers are overwhelmed with Internet traffic to shut them down."

215 ScienceDaily LLC, "Stealth Attack Drains Cell Phone Batteries," August 30, 2006: "Cell phones that can send or receive multimedia files could be targeted by an attack that stealthily drains their batteries, leaving cellular communications networks useless, according to computer security researchers at the University of California-- Davis (UC Davis). 'Battery power is the bottleneck for a cell phone,' said Hao Chen, assistant professor of computer science at UC Davis. 'It can't do anything with a dead battery.' Cell phones are designed to conserve battery life by spending most of their time in standby mode. Chen, and graduate students Denys Ma and Radmilo Racic, found that the MMS [Microsoft Media Server] protocol, which allows cell phones to send and receive pictures, video and audio files, can be used to send packets of junk data to a cell phone. Every time the phone receives one of these packets, it 'wakes up' from standby mode, but quickly discards the junk packet without ringing or alerting the user. Deprived of sleep by repeated pulses of junk data, the phone's batteries run down up to 20 times faster than in regular use. The attacker needs to know the number and Internet address of the victim's cell phone, but those are easy to obtain, Chen said. The computer used to launch the attack could be anywhere on the Internet. Chen and his students have tested the concept in the laboratory. They have also found other vulnerabilities in the MMS protocol -- one, for example, would allow users to circumvent billing for multimedia services and send files for free. As cell phone

cyber attack. Viewing SMiShing<sup>216</sup> as an example, this is a mobile device attack that seeks to dupe the recipient of an SMS (short message service – text) message into downloading malware onto their handset.<sup>217</sup> Once the handset is infected, it can be turned into a “zombie,” allowing attackers to control the device.<sup>218</sup> If the mobile device communicates with any computers, they too can be infected and become nodes on a “zombie botnet.”<sup>219</sup>

Analysts predict these and other threats of various types to cell phones and other mobile devices will eventually outnumber malware-laden e-mail messages.<sup>220</sup> In addition, these attacks can be used to expand their own scope to personal computers (PCs) and other networks when unsuspecting users forward these messages to their PCs.<sup>221</sup> Researchers have been able to demonstrate this style of attack scenario with no user involvement or action at all using only SMS messages.

These types of attacks on our cell phone infrastructure require very little in the way of resources, making them ideal candidates for malicious actors. The primary vehicle for the attack is the software that links the cell phones to their network, as the hardware is industry standard and already in most cell phones. These attacks illustrate the enormous impact that standards play vis-à-vis vulnerabilities that may affect communications security. If certain specific hardware and software standards were nationalized and closed, the ability for attackers to exploit specific national networks would be greatly reduced. By utilizing open standards, even in secure applications, it becomes an easier proposition for malicious actors, state affiliated or otherwise, to cripple the wireless communication networks of other countries.

### **The Debate Over “Open” vs. “Closed” Standards**

The question of whether to adopt “open” or “closed” standards has sparked debate in the realm of cyber security. Proponents of closed standards believe their way is most secure because it is most secret; proponents of open standards believe their way is most secure because it allows their vulnerabilities to be identified, for users to be informed, and for systems to be tested quickly and broadly for malware infections.

providers offer more services, such as e-mail, web surfing and file sharing, they become vulnerable to the same attacks as computers, as well as to new types of attack that exploit their specific vulnerabilities. ‘It’s important to evaluate security now, while cell phones are being connected to the broadband Internet,’ Chen said.”

<http://www.sciencedaily.com/releases/2006/08/060829090243.htm>.

<sup>216</sup> Washington State Office of the Attorney General, “Cell Phones Under Attack: How to block text spam and viruses,” December 19, 2007: “Cell phones with Internet access are especially at risk. By clicking on a link in a smishing message, you can unknowingly allow a hacker to steal your personal information, activate your phone’s camera or even listen in on your private cell phone conversations. In some cases, these programs can send fake messages to people in a phone’s contact list. Last year, techies discovered a Trojan horse program that pretended to access Web pages but instead sent SMS messages to premium-rate phone numbers -- costing the cell phone user. Another message offered victims free antivirus software for their phone, supposedly from their mobile service provider. Users that downloaded the software from the link were infected with malware.”

<http://www.sciencedaily.com/releases/2006/08/060829090243.htm>.

<sup>217</sup> TechTarget, “SMiShing,” SearchMobileComputing.com, Definitions.  
[http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40\\_gci1241308,00.html](http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1241308,00.html).

<sup>218</sup> TechTarget, “SMiShing,” SearchMobileComputing.com, Definitions.  
[http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40\\_gci1241308,00.html](http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1241308,00.html).

<sup>219</sup> TechTarget, “SMiShing,” SearchMobileComputing.com, Definitions.  
[http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40\\_gci1241308,00.html](http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1241308,00.html).

<sup>220</sup> TechTarget, “SMiShing,” SearchMobileComputing.com, Definitions.  
[http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40\\_gci1241308,00.html](http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1241308,00.html).

<sup>221</sup> TechTarget, “SMiShing,” SearchMobileComputing.com, Definitions.  
[http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40\\_gci1241308,00.html](http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1241308,00.html).

Current cyber research is revealing that the majority of analyzed cyber intrusions utilize techniques and/or vulnerabilities that are not patchable in the contemporary sense (i.e., updating software to remain current). In other words, there may at times be a likelihood that security software or updates (whether open or closed) will not address the most commonly used vectors of targeted attacks and will offer little or no protection from them. Also apparent is that the majority of analyzed attacks are committed using “old” means based on tools or techniques that have been in the wild for months or years. The duration of cyber attacks also seems to be increasing, with cyber-intruders persistently and dynamically present and undetected on systems for months or years.

Therefore, a flexible, thoughtful, and informed hybrid approach to security that effectively uses simple tools (both open and closed as they demonstrate merit) may be the most meaningful approach to security.<sup>222</sup>

Mainstream wireless communications-based attacks could have significant economic impacts as well as negatively impacting national security by potentially limiting or eliminating the ability of defenders to communicate effectively. In the past, cell phones have generally been regarded as immune from viruses, worms, Trojan horses, or other malware that have threatened PC-based networks for years. However, that has changed with the targeting of high-end phones with fully functional operating systems and the ability to download and install a wide variety of applications. The biggest culprit leading to infection by viruses or Trojans is the downloading of files, applications, ringtones, games, and other related content.

Mobile devices are capable of carrying a virus back to a PC when the two devices synchronize. A mobile user could pick up a virus outside a network perimeter on the mobile device, bring it back inside a firewall, and synchronize it with a system on their network, spreading the virus on an otherwise secure local area network (LAN), then a wide area network (WAN), and beyond. As an example of another potential vulnerability, a Trojan horse application can be installed on a device through memory cards, infrared file transfer, or synchronization. An attacker can send a special text message to the infected phone, signaling the Trojan to commit a hostile act such as stealing the last five minutes of phone conversation stored in the device’s memory.

In a demonstration presented at the Black Hat Security Conference in Las Vegas in July 2009, researchers revealed that an attacker could exploit a software hole to make calls, steal data, send text messages, and do more or less anything a person can do on their iPhone.<sup>223</sup> The attacker needed only to send SMS control messages to the device and could then send SMS messages to anyone in the victim’s address book to spread the attack.<sup>224</sup> This attack required no effort of the part of the user and only looked for the victim’s phone number.<sup>225</sup> The attacker sends SMS messages containing configuration information that is normally found only on network servers.<sup>226</sup> According to reports, Global System for Mobile Communications (GSM)

<sup>222</sup> Reperi LLC, information, technology, and telecommunications security research, supported variously by other sources.

<sup>223</sup> Elinor Mills, “Researchers take control of iPhone via SMS,” ZDNet.com, July 30, 2009.

[http://news.zdnet.com/2100-9595\\_22-326501.html](http://news.zdnet.com/2100-9595_22-326501.html).

<sup>224</sup> Elinor Mills, “Researchers take control of iPhone via SMS,” ZDNet.com, July 30, 2009.

[http://news.zdnet.com/2100-9595\\_22-326501.html](http://news.zdnet.com/2100-9595_22-326501.html).

<sup>225</sup> Elinor Mills, “Researchers take control of iPhone via SMS,” ZDNet.com, July 30, 2009.

[http://news.zdnet.com/2100-9595\\_22-326501.html](http://news.zdnet.com/2100-9595_22-326501.html).

<sup>226</sup> Robert McMillan, “Some SMS Networks Vulnerable to Attack,” July 28, 2009.

[http://tech.yahoo.com/news/pcworld/20090729/tc\\_pcworld/somesmsnetworksvulnerabletoattack](http://tech.yahoo.com/news/pcworld/20090729/tc_pcworld/somesmsnetworksvulnerabletoattack).

networks are susceptible, but CDMA networks are not.<sup>227</sup> Other bugs found in cell phone software have allowed attackers to control the user interface on Windows Mobile devices via the SMS messages to disable keypads, rendering the cell phone unusable.<sup>228</sup>

Prior to this report, another similar type attack was reported by Trust Digital in April 2009.<sup>229</sup> In this type of attack, an SMS message is sent to a phone that opens its browser directing the phone to a malicious website; the website then downloads software to the phone and steals the information on the phone.<sup>230</sup> In a paper written by Penn State University researchers in 2005, various SMS vulnerabilities were identified, details of how the SMS attacks could be accomplished were described, and mitigation recommendations were presented.<sup>231</sup>

Reports have indicated that three China-based entities created the "Sexy Space" Trojan and tried to send it through the Symbian Foundation's digital-signing process.<sup>232</sup> All Symbian Series 60 third-edition phones by Nokia, LG, and Samsung were potential targets of the malware.<sup>233</sup> At the time of original reference, the Symbian platform was in use in just under 50 percent of all smart phones.<sup>234</sup>

Another potential national threat involving the iPhone and the exclusive AT&T wireless network has been dubbed "Jailbreaking."<sup>235</sup> The lighter side of Jailbreaking involves users who want to break free from carrier and manufacturer restrictions to use software they prefer,<sup>236</sup> but it may also have more serious implications. Jailbreaking alters a phone's baseband processor (BBP) that facilitates connections to cell towers,<sup>237</sup> meaning that attackers could potentially disable those towers.<sup>238</sup> Changing the BBP code can also allow the Exclusive Chip Identification (ECID) to be changed, making the device essentially anonymous on the network.<sup>239</sup> These vulnerabilities in cell phones can be easily exploited with a computer, access to a WiFi network,

<sup>227</sup> Robert McMillan, "Some SMS Networks Vulnerable to Attack," July 28, 2009.

[http://tech.yahoo.com/news/pcworld/20090729/tc\\_pcworld/somesmsnetworksvulnerabletoattack](http://tech.yahoo.com/news/pcworld/20090729/tc_pcworld/somesmsnetworksvulnerabletoattack); and also Jim Dalrymple, "Apple Fixes iPhone SMS Flaw," July 31 2009. [http://news.cnet.com/8301-1009\\_3-10301001-83.html](http://news.cnet.com/8301-1009_3-10301001-83.html).

<sup>228</sup> Elinor Mills, "Researchers take control of iPhone via SMS," ZDNet.com, July 30, 2009.

[http://news.zdnet.com/2100-9595\\_22-326501.html](http://news.zdnet.com/2100-9595_22-326501.html).

<sup>229</sup> Elinor Mills, "SMS Messages Could Be Used to Hijack a Phone," April 19, 2009. [http://news.cnet.com/8301-1009\\_3-10222921-83.html](http://news.cnet.com/8301-1009_3-10222921-83.html).

<sup>230</sup> Elinor Mills, "SMS Messages Could Be Used to Hijack a Phone," April 19, 2009. [http://news.cnet.com/8301-1009\\_3-10222921-83.html](http://news.cnet.com/8301-1009_3-10222921-83.html).

<sup>231</sup> William Enck et al., "Exploiting Open Functionality in SMS-Capable Cellular Networks," (Pennsylvania State University, September 2, 2005). <http://www.smsanalysis.org/smsanalysis.pdf>.

<sup>232</sup> Vivian Yeo, "Chinese Firms Behind 'Sexy Space' Trojan," July 22, 2009. [http://news.cnet.com/8301-1009\\_3-10292917-83.html](http://news.cnet.com/8301-1009_3-10292917-83.html).

<sup>233</sup> Vivian Yeo, "Chinese Firms Behind 'Sexy Space' Trojan," July 22, 2009. [http://news.cnet.com/8301-1009\\_3-10292917-83.html](http://news.cnet.com/8301-1009_3-10292917-83.html).

<sup>234</sup> Vivian Yeo, "Chinese Firms Behind 'Sexy Space' Trojan," July 22, 2009. [http://news.cnet.com/8301-1009\\_3-10292917-83.html](http://news.cnet.com/8301-1009_3-10292917-83.html).

<sup>235</sup> Dong Ngo, "Jailbreaking iPhone could pose threat to national security, Apple claims," July 29, 2009.

[http://reviews.cnet.com/8301-19512\\_7-10298646-233.html](http://reviews.cnet.com/8301-19512_7-10298646-233.html); David Kravets, "iPhone Jailbreaking Could Crash Cellphone Towers, Apple Claims," Wired.com, July 28, 2009. <http://www.wired.com/threatlevel/2009/07/jailbreak/>.

<sup>236</sup> David Kravets, "iPhone Jailbreaking Could Crash Cellphone Towers, Apple Claims," Wired.com, July 28, 2009. <http://www.wired.com/threatlevel/2009/07/jailbreak/>.

<sup>237</sup> David Kravets, "iPhone Jailbreaking Could Crash Cellphone Towers, Apple Claims," Wired.com, July 28, 2009. <http://www.wired.com/threatlevel/2009/07/jailbreak/>.

<sup>238</sup> David Kravets, "iPhone Jailbreaking Could Crash Cellphone Towers, Apple Claims," Wired.com, July 28, 2009. <http://www.wired.com/threatlevel/2009/07/jailbreak/>.

<sup>239</sup> David Kravets, "iPhone Jailbreaking Could Crash Cellphone Towers, Apple Claims," Wired.com, July 28, 2009. <http://www.wired.com/threatlevel/2009/07/jailbreak/>.



a couple of cell phones, and a business card.<sup>240</sup> These types of attacks are on the rise and, given the speed with which information moves via the Internet, it becomes a challenge for the industry to close the holes before the next ones are discovered.<sup>241</sup>

From a communications security perspective, government procurement of cell phones might appropriately consider both the hardware and software aspects of devices. Vulnerabilities associated with hardware may relate to overreliance on particular networks, and/or overreliance of supply chains on particular hardware supply models. One potential mitigation strategy is for the Department of Defense and other government organizations to consider the use of cell phones that are flexible in both data transmission standards and physical hardware -- which is to say, easily replaceable and able to function across multiple network types and spectrum bands/frequencies. Reliance on particular hardware designs could have negative impacts if the supplier(s) fail, withhold production, or otherwise undermine systems or services, or if consequent supply chains suffer disruptions or failure.<sup>242</sup>

Reliance on a particular transmission standard would limit the field of use to the range of compatible networks. By using a broad spectrum purchasing approach, security can be enhanced by having utilization capabilities across a wide variety of hardware and data transmission protocols. This would enable the supply chain to adapt to many adverse situations. Mobile devices are relatively inexpensive and easily moved from region to region. However, alternative approaches, consisting of closed networks and proprietary hardware, tend to be costly and ineffective from an economic and mobility standpoint. Manufacturers are often reluctant to dedicate scarce resources to pursue such technology models if they will lack broad market appeal.

From a software perspective, cell phone technology is changing and evolving every day. Attacks from a wide variety of vectors will only increase. The first step to mitigate these attacks should be increased user education and awareness. Comprehensive training on what to look for and how attackers are utilizing new technologies would improve the process of attack identification and prevention. Identifying when a device or network has been compromised is the fastest way of taking evasive action to close the device, move to another device, or utilize a different network. Having immediate access to source code for device operating systems and network software is another tactic to pursue to avoid delay in heading off cellular attacks. In addition to having the source code access, trained personnel are required to make lightning-fast adjustments to source code bases both to defend against and pursue attackers.

Smart phones blend the voice and data features of both phones and personal digital assistants (PDAs) into a single portable device. Many of today's wireless handsets include calendars, alarms, and downloadable applications and typically support e-mail and desktop synchronization so that mobile users have access to their master contact, calendar, and to-do lists. Wireless handsets have evolved into a technology that offers near-constant access for multimedia applications such as global positioning system (GPS), video gaming, stereo FM radio, digital photography, CD (compact disc)-quality music, texting, access to e-mail, Internet browsing, and many other functions. While such functions can contribute greatly to both professional productivity and personal entertainment, the ready connectivity of handset devices opens many more potential doors to malicious network actors.

<sup>240</sup> Joan Goodchild, "3 Simple Steps to Hack a Cell Phone," CSO Online, April 29, 2009.

<sup>241</sup> <http://www.csoonline.com/article/491200/SimpleStepsToHackaSmartphoneIncludesVideo>.

<sup>241</sup> Joan Goodchild, "CISCO: SMS Smartphone Attacks on the Rise," CSO Online, July 14, 2009.

<sup>241</sup> <http://www.csoonline.com/article/497120/CiscoSMSSmartphoneAttacksOnTheRise>.

<sup>242</sup> Reperi LLC, "Trends In Mobile Wireless Communications," 2006.



## WIRELESS HEADSETS, EARPIECES, AND BLUETOOTH

Almost all of China's phone manufacturers make Bluetooth products. ZTE makes Bluetooth accessories to go with its mobile phone products, some of which may have limited market penetration in the United States but which could be part of any larger agreement with major U.S. telecommunications carriers. Bluetooth is an open wireless technology that allows wireless devices to exchange data over short distances. In essence, when Bluetooth devices connect to one another, they create a small wireless personal area network (PAN). Multiple devices can be connected to the same PAN. Bluetooth is a ubiquitous standard today, so most Chinese manufacturers do produce Bluetooth devices. Bluetooth uses frequency-hopping spread-spectrum radio technology, which breaks up data and spreads data out on up to 79 different frequencies, transmitting about a megabit of data per second. Connections can be made and information exchanged between any devices that are Bluetooth capable.

### **Bluetooth: Potential Vulnerabilities**

When Bluetooth is enabled, it generally is configured to broadcast its device's availability for a connection to any and all other devices in range, which makes the device very easy for an attacker to locate and exploit. An attacker need only be equipped with the required software and a portable computer with a Bluetooth adapter. The attacker need only go into an area where they expect to find targetable devices nearby and then perform their attack automatically when vulnerable devices are located. With the attacker's system scanning for targets automatically, the attacker can remain inconspicuous, and the nature of the attacks generally will not alert the victim to the fact that they are under attack.

Once a device is compromised, the attacker can gain access to all data and system functionality. A large number of programs are available that are specifically designed to attack Bluetooth cell phones. "Bluesnarfing" is the common term for an attack that downloads all of the victim's data, while "Bluebugging" is an attack that allows the attacker to turn a compromised wireless phone into a bugging device or to eavesdrop on all calls made on the device.

Compromised phones can be used for a myriad of purposes, from collecting private or sensitive information, diverting long distance charges, and eavesdropping, to rigging them with kill commands or other damaging exploits.

### **Switching Equipment and Other Networking Services – The Nortel Story**



From its founding in 1895 as Northern Electric and Manufacturing, and its early days of manufacturing equipment for Canada's fledgling telephone system,<sup>243</sup> Nortel grew to become a major manufacturer of telecom equipment ranging from carrier-class systems to user equipment (much of it deployed throughout the U.S. government). Beginning in the early 2000s, Nortel started to experience financial difficulties and began exploring deals with other corporations:

<sup>243</sup> Nortel.com website, "Nortel History." <http://www.nortel.com/corporate/corptime/index.html>.

-- In 2004, Nortel and China Putian Corporation<sup>244</sup> agreed to a memorandum of understanding for cooperation on research and development, and manufacture of 3G equipment and products. The two companies cooperated on projects such as 3G field trials sponsored by China's Ministry of Information Industry.

-- In 2005, Nortel and China Putian established a joint venture for research and development, manufacturing, and sale of 3G mobile telecom equipment and products to customers in China. Signing of the Joint Venture Framework Agreement occurred in Beijing and was witnessed by China's Premier Wen Jiabao and Canada's Prime Minister Paul Martin.<sup>245</sup>

-- In February 2006, Nortel and Huawei announced plans to form a joint venture in order to develop IP broadband internet solutions.<sup>246</sup> This venture evidently did not progress beyond the early stages.

-- In 2008 – a year in which the company's stock lost 96 percent of its value and the company was mulling bankruptcy<sup>247</sup> – a possible deal emerged that would have resulted in an infusion of much-needed cash into the company. Huawei bid \$400 million for Nortel's Metro Ethernet Networking business, a bid that some industry observers considered far above its value.<sup>248</sup> However, concerns over Huawei's background appear to have derailed the deal, with some U.S. broadband providers reportedly indicating that they would stop buying Nortel equipment if Huawei acquired a large stake in the firm.<sup>249</sup>

-- On January 14, 2009, Nortel sought bankruptcy protection.<sup>250</sup> Since this time, a general sell-off of Nortel's business units and assets has occurred.<sup>251</sup> Telefonaktiebolaget LM Ericsson ("Ericsson"), Kapsch CarrierCom AG ("Kapsch"), Ciena, GENBAND, Inc., Avaya Inc., and Hitachi Ltd. have each purchased portions of Nortel or its assets and subsidiaries, constituting the bulk of the company.<sup>252</sup>

<sup>244</sup> Hoovers.com reference. [http://www.hoovers.com/company/CHINA\\_PUTIAN\\_CORPORATION/rfjhhif-1.html](http://www.hoovers.com/company/CHINA_PUTIAN_CORPORATION/rfjhhif-1.html).

<sup>245</sup> Press release on the Nortel.com website.

[http://www.nortel.com/corporate/news/newsreleases/2005a/01\\_20\\_05\\_china\\_putian.html](http://www.nortel.com/corporate/news/newsreleases/2005a/01_20_05_china_putian.html).

<sup>246</sup> Nortel.com, "Nortel, Huawei to Establish Joint Venture to Address Broadband Access Market" and "Plan to Jointly Develop Ultra Broadband Products for Delivery of Converged Services," February 1, 2006.

[http://www2.nortel.com/go/news\\_detail.jsp?cat\\_id=-8055&oid=100194923](http://www2.nortel.com/go/news_detail.jsp?cat_id=-8055&oid=100194923).

<sup>247</sup> Andy Greenberg, "Nortel's China Syndrome," *Forbes.com*, January 12, 2009.

[http://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx\\_ag\\_0112nortel.html](http://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx_ag_0112nortel.html).

<sup>248</sup> Andy Greenberg, "Nortel's China Syndrome," *Forbes.com*, January 12, 2009.

[http://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx\\_ag\\_0112nortel.html](http://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx_ag_0112nortel.html).

<sup>249</sup> Andy Greenberg, "Nortel's China Syndrome," *Forbes.com*, January 12, 2009.

[http://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx\\_ag\\_0112nortel.html](http://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx_ag_0112nortel.html).

<sup>250</sup> Lionel Laurent, "Nortel Throws in the Towel," *Forbes.com*, January 14, 2009.

[http://www.forbes.com/2009/01/14/nortel-alcatel-technology-markets-equity-cx\\_0114markets11.html?partner=whiteglove\\_google](http://www.forbes.com/2009/01/14/nortel-alcatel-technology-markets-equity-cx_0114markets11.html?partner=whiteglove_google).

<sup>251</sup> Nortel.com, "Nortel Obtains Court Orders for Creditor Protection," January 14, 2009.

[http://www2.nortel.com/go/news\\_detail.jsp?cat\\_id=-8055&oid=100251347&locale=en-US](http://www2.nortel.com/go/news_detail.jsp?cat_id=-8055&oid=100251347&locale=en-US); and Nortel.com, "Nortel Business and Financial Restructuring," <http://www.nortel.com/corporate/restructuring.html>; and Nortel's U.S. claims agent, Epiq Bankruptcy Solutions, LLC.

<http://chapter11.epiqsystems.com/NNI/Project/default.aspx?DMWin=dcd9aa35-e94e-418b-84a3-d769f095df78>.

<sup>252</sup> Based on data available from the Nortel.com website, restructuring section.

<http://www.nortel.com/corporate/restructuring.html>.

**The Nortel Story as a Possible Sign of Things to Come**

In the example of the abortive Huawei/Nortel deal, we see what is likely to become a repeating pattern in both the telecom and other industries:

1. A western telecom company with a very strong and deep business posture in the U.S. marketplace in general (and the U.S. government in specific) begins to experience distress related to prevailing economic conditions;
2. The company accepts research and development ties with Chinese companies in an effort to gain large-scale entry into China's lucrative new market but finds that the benefits of entering the Chinese market fail to provide the new lease on life that is hoped for;
3. A Chinese company flush with investment capital (Huawei) steps in to purchase portions of the distressed company's (Nortel) business in which it is interested (also giving the distressed company an infusion of much-needed cash);
4. However, push-back from the distressed company's customers (due to security concerns) can be sufficient to discourage the deal. Numerous restructuring efforts may then fail to achieve sufficient positive traction, and the distressed company may subsequently wind up in bankruptcy.

At present, Nortel is being sold in parts to the highest bidders.

**TABLE 1: WHERE CHINA'S PRODUCTS ARE FOUND IN THE U.S. COMMUNICATIONS MARKET**

WHAT IT IS: PRODUCT	WHO MAKES IT: MANUFACTURER	WHAT IT IS USED FOR, AND WHAT IT CAN DO	PRESENT OR FUTURE USE	SOURCE
<b>ZTE EV-DO Modem/USB</b>	ZTE, relabeled by Verizon and other companies	Connecting wirelessly to 3G, GSM, EDGE, and HSDPA (High-Speed Downlink Packet Access)	Compatible with wireless networks like Verizon, AT&T	<a href="http://engadgetmobile.com">engadgetmobile.com</a>
<b>ZTE Smartphones/3G, 4G with Qwerty keyboards, LTE devices</b>	ZTE USA; planned partnership with Verizon Wireless	Competes with other wireless handset providers	Competes with Apple, Blackberry (RIM), Motorola, and other handset providers, Nokia, Ericsson, and Samsung	<a href="http://fiercewireless.com">fiercewireless.com</a>
<b>Application Software for Wireless Devices – TechSoft Mobile Solutions Suite</b>	QualComm/China TechFaith joint venture wireless company – each put in up to ~\$35 million, according to reports. The new company is China-based TechSoft. TechFaith was Qualcomm's first independent design house partner	Operating software for CDMA mobile handsets <a href="http://www.techfaithwireless.com/english/products/products_ApplicationSoftware.htm">http://www.techfaithwireless.com/english/products/products_ApplicationSoftware.htm</a>	3G CDMA mobile handset software applications	Electronics News, 03/27/2008
<b>Base Station and equipment for HSDPA (high-speed downlink packet access)</b>	Huawei – Provider to T-Mobile – <i>in Europe – working on a deal for U.S.</i>	Base station for wireless networks allowing maximized use of towers/cabinets in rolling out HSDPA, reducing build-out costs for T-Mobile. HSDPA is a packet-based mobile telephony protocol used in 3G UMTS (universal mobile telecommunications system) radio networks to increase data capacity and speed up transfer rates.	Deployment in cellular, GSM, and wireless networks, provides access to data packets	Network World
<b>Patent for WiMAX wireless patents</b>	Nokia Siemens Network/Nokia parent company and Huawei – patent deal	Deal covers standards relating to GSM, WCDMA, CDMA, optical networking, datacom, and WiMAX	Standards control	<a href="http://telecoms.com">telecoms.com</a>
<b>Huawei E583 X Modem</b>	3G to WiFi Huawei	It is what T-Mobile and other network providers would like to offer	Mobile network connectivity for individual users	CNET SlashGear
<b>3G Network Equipment/LTE Ready</b>	Huawei	4G and 3G networks – wireless. Cox wireless network	Deployment in U.S. cities	<i>Wall Street Journal</i> Network World

## TABLE 2: WHERE CHINA'S INVESTMENTS ARE FOUND IN THE U.S. COMMUNICATIONS MARKET

The table below highlights significant Chinese investments in the U.S. telecommunications sector. This table also lists some attempted deals that failed to obtain CFIUS approval. Even though some of the deals noted below did not go through, it is important to note that these investment attempts had the potential for impacting key network traffic important to U.S. national security interests.

INVESTOR	INVESTMENT	WHAT IT IS/PART OF SUPPLY CHAIN	WHAT IT DOES/CAN DO	INVESTMENT AMOUNT	DATE	SOURCE
<b>Hutchison Whampoa</b>	Joint venture with Global Crossing 50/50. <sup>253</sup> Total: both partners \$1.2 billion	Fiber routes. Fixed line telecommunications. Internet, fiber optic, international cable. Web hosting.	Provide international telecom transport – network monitoring.	Aggregate joint venture value of \$1.2 billion.	2000	Highbeam.com Hutchison Whampoa Press Release
<b>Hutchison Whampoa – Singapore Telecom STT</b>	Assets of Global Crossing (Asian Crossing). <sup>254</sup>	Undersea cable traffic to U.S.	Carry traffic between U.S., Asia, Europe, and some continental U.S. routes	\$250 Million *Deal went forward with Singapore Telecom Only	2002	SEC 10K
<b>Huawei Bain Capital Partners and Huawei jointly</b>	Acquisition attempt. 51/49 percent majority in Huawei 3-Com (H3C). 3-Com later bought out the joint venture. <sup>255</sup>	Wireless routers, voice, data, networking products. Proposed buyout for \$2.2 billion of 3Com in 2007 – U.S. government objected; acquisition failed. 3Com revenues have spiraled downward since.	Wireless data traffic transport.  Routers for DOD and federal government.	Unknown.	2003 - 2007.	Press Releases
<b>Cox Com</b>	Huawei	LTE and wireless base stations.	Broadband communications.	Undisclosed	2009	<i>Wall Street Journal</i>
<b>Leap Wireless “Cricket”</b>	Huawei	CDMA / EV-DO networking products. Huawei CDMA2000 network with 1xEV-DO Rev A capable BTS (base transceiver	Wireless broadband modems, routers. Broadband data transmission.	Undisclosed	2009	EETimes Asia.Com

<sup>253</sup> Hutchison Whampoa Limited Press Release, “Hutchison Whampoa and Global Crossing complete telecom joint venture in Hong Kong,” January 12, 2000.

<sup>254</sup> Global Crossing SEC (Securities and Exchange Commission) 10K Filing, 2002.

<sup>255</sup> 3-Com later bought out its portion of the H3C joint venture.

		station). The solutions will include Huawei's SoftX3000-Softswitch, Air Bridge BSC6600, UMG8900-Universal Media Gateway, and high-capacity BTS 3606.				
<b>Clearwire (investors, Intel, Sprint Nextel, Google)</b>	Huawei	WiMAX. 4G networks. WiMAX base stations. LTE.	High-speed broadband wireless.	Undisclosed	2009	<i>Wall Street Journal</i>
<b>Verizon</b>	ZTE	USB modems.	Data Comm.	Unknown	2007	Newswire

Figure 6: Sample Integrated Operational Network Model (Healthy)

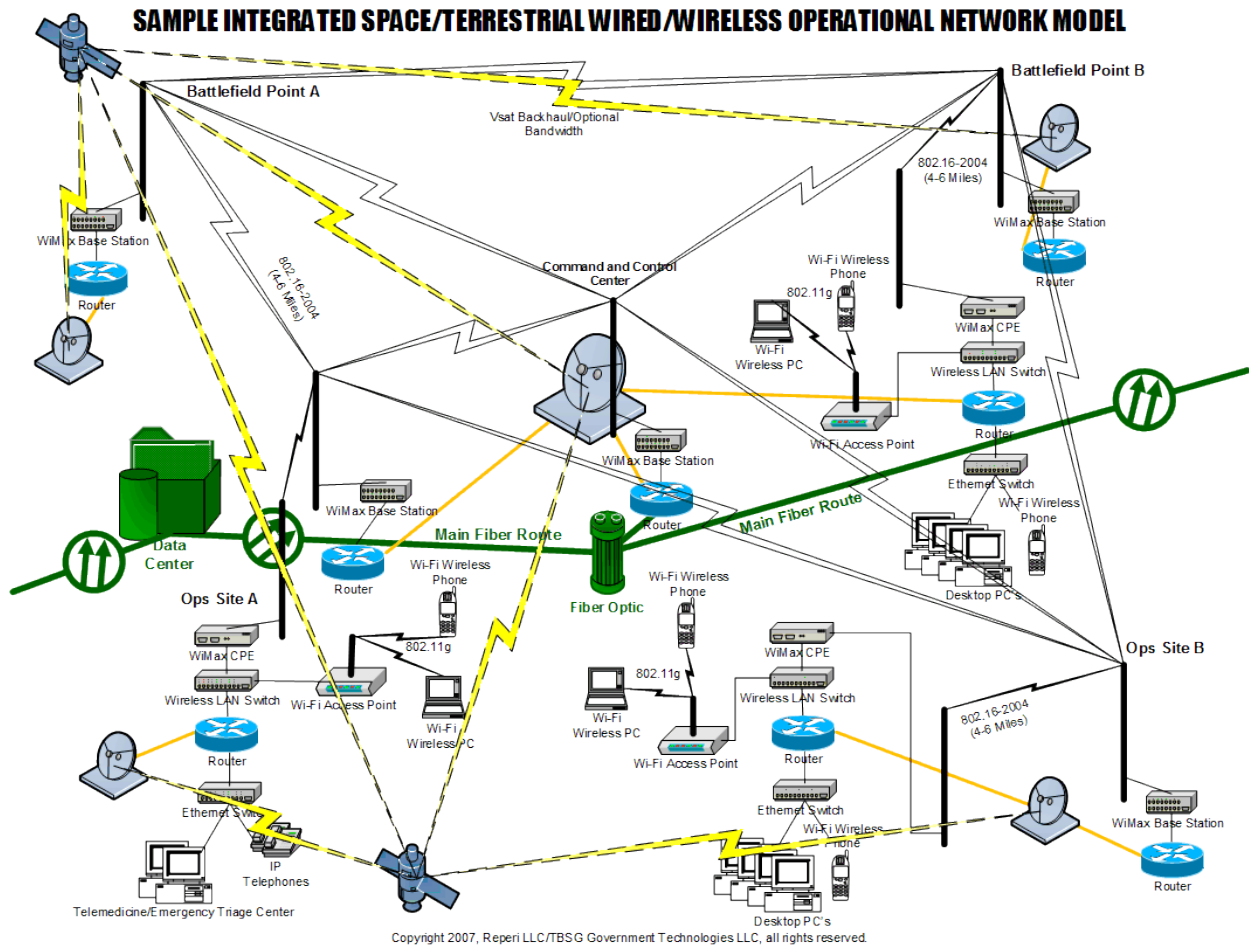




Figure 7: Sample Integrated Operational Network Model (Corrupted)

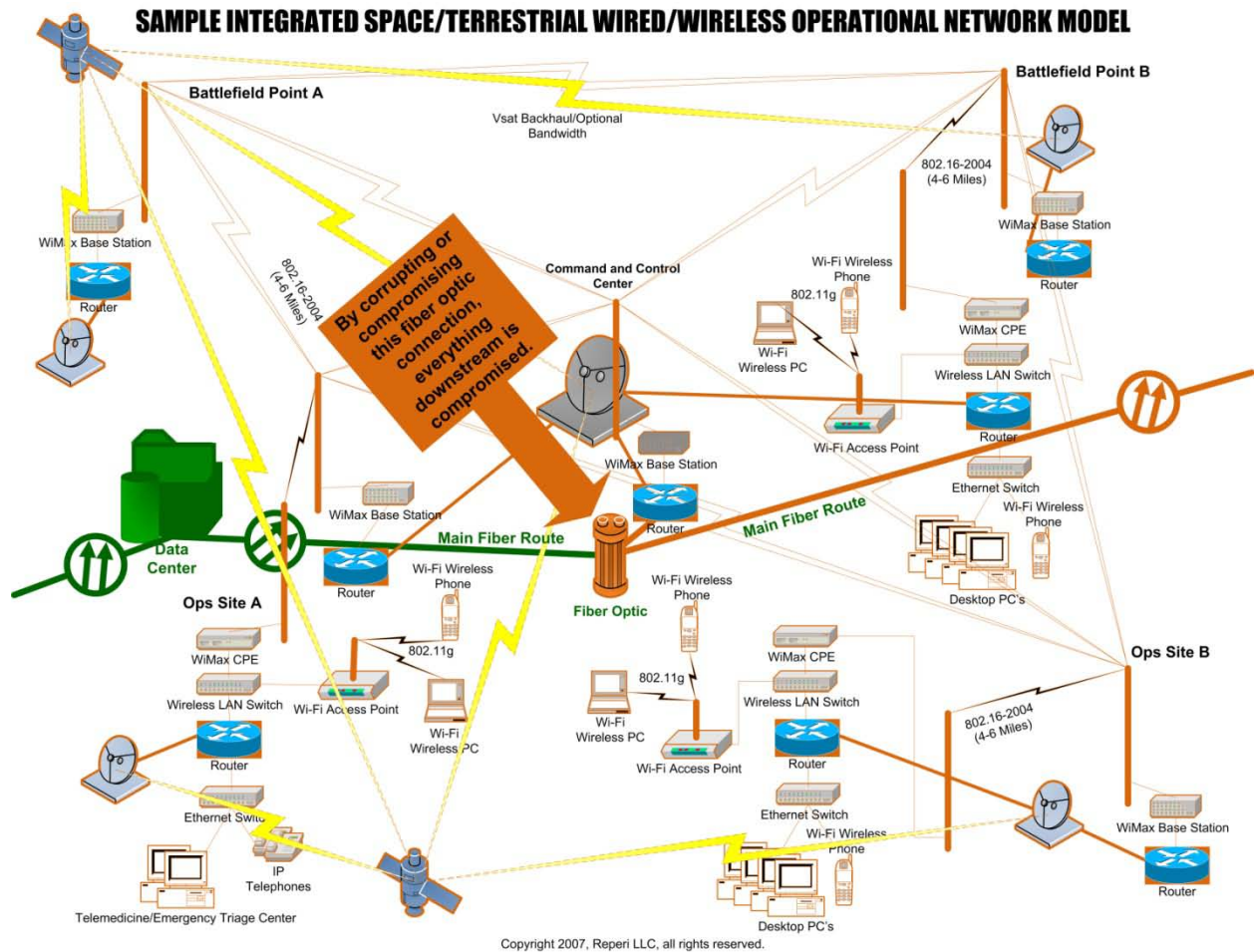
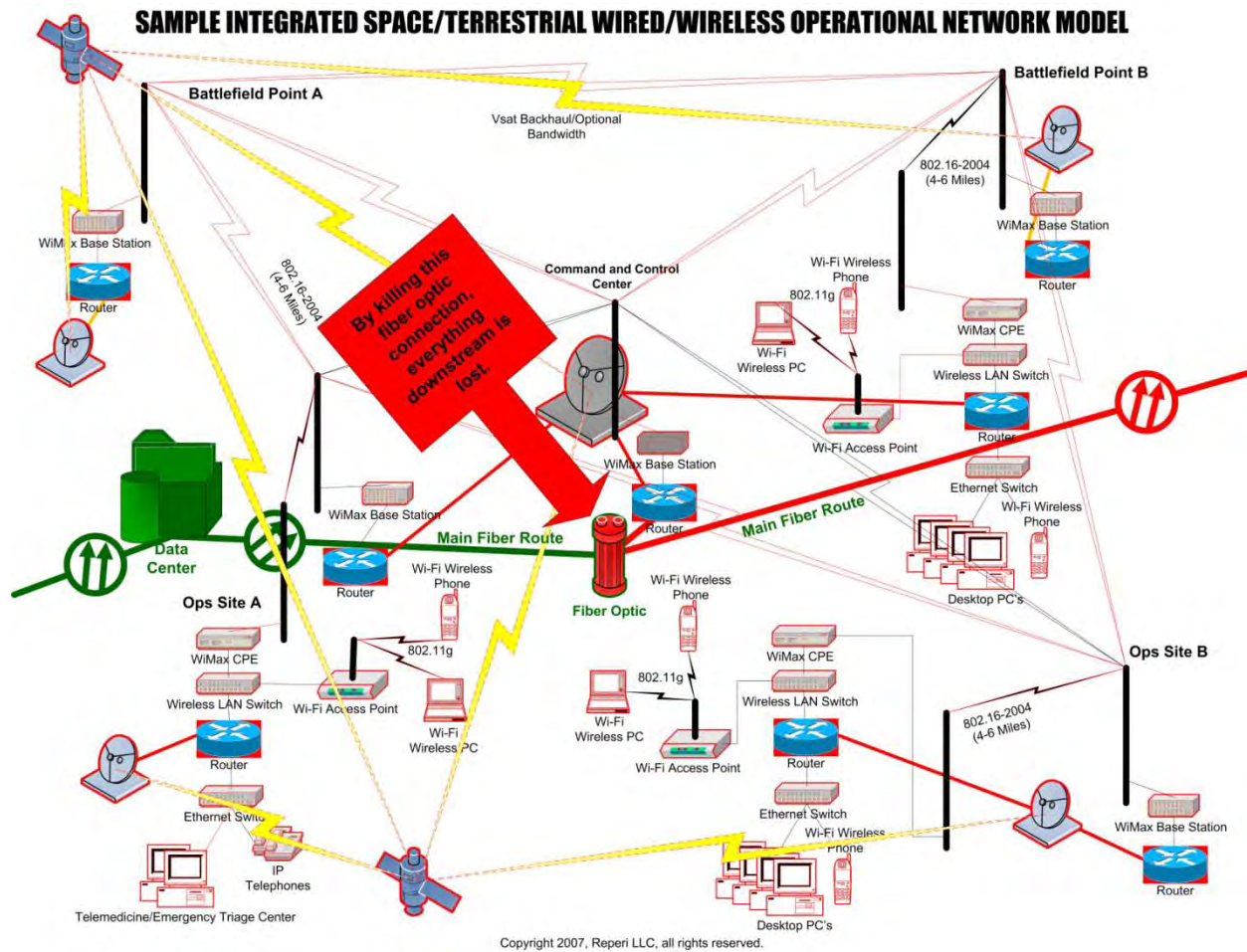


Figure 8: Sample Integrated Operational Network Model (Disabled)<sup>256</sup>

<sup>256</sup> A useful reference for additional perspective is the war impact maps of the Serbian networks during their 1999 conflict, available at <http://www.cheswick.com/ches/map/yu/index.html>.

## SECTION 3

# SUPPLY CHAIN INTEGRITY, AND THE IMPACT ON GOVERNMENT / DEFENSE CONTRACTING

American interests are heavily dependent on cyber space and, in the case of businesses and private individuals, many vital functions are now tied together across private or public networks such as the Internet. In the case of national security and defense enterprises, cyberspace is also now a key enabler. Continuously available secure enterprise networks are indispensable and now reside at the core of national security mission needs.

*The loss of unfettered access to cyberspace would not merely be “game changing” in America, it would be profoundly catastrophic. Cyberspace is a crown jewel at our national core that should be protected with care. American awareness of the critical value of cyberspace is growing, but not at a pace that is commensurate with the rate at which cyber risks are increasing.*

The most pressing critical strategic cyber security issues are the following:

- Recognition by policymakers of the need to adapt quickly to address and fund critical vulnerabilities.
- Substantial security risks posed by critical supply chain vulnerabilities due to dependence on foreign innovation and manufacturing.
- Potentials for permanent loss of critical supply chain elements.

The U.S. Department of Defense has recognized cyber security as a principal issue and is seeking to address it in both policy and practice. Admirable efforts to address culture, management, and technical challenges are being undertaken in the U.S. defense community in response to the growing awareness of the criticality of cyberspace.<sup>257</sup> However, given the context of resources and policy, U.S. military efforts are necessarily focused first on the tremendous challenge of protecting and enabling military cyberspace, while the vast majority of American critical cyberspace existing in the private/commercial realm remains largely unaddressed by government cyber security efforts.

The question of supply chain security is a key element in cyber security. Dependency upon foreign manufacturers for critical products across the telecommunications, communications, and information systems supply chains impacts almost every aspect of voice and data transport. To date, public discussion of the vulnerabilities of electronics components to malicious tampering has been largely theoretical, but historical precedent does exist:

*At the height of the cold war, in June 1982, an American early-warning satellite detected a large blast in Siberia... [It was] an explosion on a Soviet gas pipeline. The cause was a malfunction in the computer-control system that Soviet spies had stolen from a firm in Canada. They did not know that the CIA [Central Intelligence Agency] had tampered with*

<sup>257</sup> House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats, and Capabilities, Statement by Michael E. Krieger, deputy chief information officer/G-6, United States Army, 111th Cong., 2nd sess., May 5, 2009.

*the software so that it would 'go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds,' according to the memoirs of Thomas Reed, a former air force secretary. The result, he said, 'was the most monumental non-nuclear explosion and fire ever seen from space.'...*

*... given that computer chips and software are produced globally, could a foreign power infect high-tech military equipment with computer bugs? 'It scares me to death,' says one senior military source. 'The destructive potential is so great.'*<sup>258</sup>

If agents of the U.S. government could maliciously tamper with electronics components bound for purchase by an adversary, then adversaries of the United States could certainly consider doing the same. This may already have happened in at least one instance: Jim Lewis, an expert on cyber security issues at the Center for Strategic and International Studies, has described a case of sabotaged hardware that may have been used to facilitate a breach of secure systems at the U.S. Central Command in 2008. As stated in an interview with CBS News:

*Last November, someone was able to get past the firewalls and encryption devices of one of the most sensitive U.S. military computer systems and stay inside for several days. 'This was the CENTCOM network,' Lewis explained. '[S]ome foreign power was able to get into their networks. They could see what the traffic was. They could read documents. They could interfere with things. It was like they were part of the American military command.'*

*Lewis believes it was done by foreign spies who left corrupted thumbdrive drives or memory sticks lying around in places where U.S. military personnel were likely to pick them up. As soon as someone inserted one into a CENTCOM computer, a malicious code opened a backdoor for the foreign power to get into the system.*<sup>259</sup>

### **Supply Chain Integrity and Cyber Security**

***Loss of control of telecommunications supply chains could constitute one of the single greatest threats to U.S. cyber and communications security.*** There are many potentially troubling issues surrounding potential corruption and/or tampering with electronics manufacturing supply chains. These include the following:

- Potential increased risk of loss of sensitive data and intellectual property through compromised networks;
- Impacts of a potential adversary's reach into critical infrastructure and weapons systems for sabotage;
- Loss of manufacturing, infrastructure, scientific, and engineering expertise.

*Exposure and national security risks should be evaluated from a variety of factors:*

- The loss of U.S. dominance or competitiveness in the overall context of the national security supply chains or in key individual segments.
- The loss of supply chain components.

<sup>258</sup> *Economist*, "War in the Fifth Domain," July 1, 2010.

<sup>259</sup> CBS News, *60 Minutes*, "Cyber War: Sabotaging the System," November 8, 2009.  
<http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml>.



- The ability of a foreign adversary to impact an element of the supply chain or resultant architectures through controllers and devices.
- The means by which networks and devices move classified and nonclassified information.

Cyber security concern centering on China is a core issue that has created problems for Chinese telecom product suppliers on the global stage. As cited previously, India is selectively barring telecom deals with some foreign providers on this basis. In December 2009, India's Telecommunications Department asked Indian mobile phone operators to suspend deals with foreign equipment companies and told several mobile phone operators that proposed deals with Chinese companies could not proceed due to security concerns.<sup>260</sup> Central to India's concerns is the possibility of foreign malware, hacking, and spying. Restrictions have evidently been lifted on most foreign manufacturers, with those remaining under restriction being "principally Chinese."<sup>261</sup> Similar concerns came to light in the United Kingdom.<sup>262</sup> *(For further discussion of concerns by some governments regarding the alleged activities of Huawei, see p. 16.)*

U.S. concerns in these respects are no less significant; however, American considerations are perhaps even more complex. As previously noted, there are significant, pervasive, and increasing interdependencies between the Chinese and American economies, particularly in the telecommunications sector. Potential U.S. cyber vulnerabilities are profound relative to our cyber defense capabilities. Research by cyber security professionals has illustrated U.S. cyber vulnerabilities and helped define the context of risks in terms of severity, magnitude, time indexes, and potential solutions.<sup>263</sup> Although collaboration with the private sector may be addressed in the Comprehensive National Cybersecurity Initiative,<sup>264</sup> the means of doing so may remain undefined and in need of exploration for some time. A major obstacle to meaningful public-private cooperative efforts is the absence of a common basis of knowledge and dialog to support operational working collaboration between the two sectors.

China's cyber warfare and cyber espionage capabilities are reported as being very substantial (see text box on the following page), with the potential for severe threats to both the integrity of government networks and to commercial intellectual property. Furthermore, with many U.S. business organizations doing business in China, it is no longer sufficient only to consider the circumstances of cyber security within the United States. Careful consideration of the ramifications (including impacts within the United States) of cyber vulnerabilities created by direct exposure to the Chinese marketplace is needed. Perhaps one of the best recent examples to cite is the controversy surrounding alleged penetrations of Google networks by

<sup>260</sup> *China Tech News*, "Indian Government Bans Import of Chinese Telecom Equipment," April 30, 2010.

<sup>261</sup> Heather Timmons, "India Tells Mobile Firms to Delay Deals for Chinese Telecom Equipment," *New York Times*, April 30, 2010. <http://www.nytimes.com/2010/05/01/business/global/01delhi.html>.

<sup>262</sup> Michael Smith, "Spy chiefs fear Chinese cyber attack," *Sunday Times* (London), March 29, 2009. <http://www.timesonline.co.uk/tol/news/uk/article5993156.ece>.

<sup>263</sup> House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, "Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action," testimony of O. Sami Saydjari, president, Professionals for Cyber Defense, and chief executive officer, Cyber Defense Agency, LLC, 110th Cong., 1st sess., April 25, 2007. <http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf>.

<sup>264</sup> The White House: "The activities under way to implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy." *White House.gov*, May 2009.

Chinese hackers. U.S. telecommunications or technology companies with operations abroad may discover they are more vulnerable than expected.<sup>265</sup>

### **Chinese Cyber Espionage Directed vs. the United States**

In a public report released in 2009, analysts with the Northrop Grumman Corporation produced a research report for the U.S.-China Economic and Security Review Commission that stated:

*"China is likely using its maturing computer network exploitation capability to support intelligence collection against the US Government and industry by conducting a long-term, sophisticated, computer network exploitation campaign. The problem is characterized by disciplined, standardized operations, sophisticated techniques, access to high-end software development resources, a deep knowledge of the targeted networks, and an ability to sustain activities inside targeted networks, sometimes over a period of months."*<sup>266</sup>

In early 2010, the computer security firm Mandiant released a report titled *The Advanced Persistent Threat*, which stated that:

*"MANDIANT defines the APT [Advanced Persistent Threat] as a group of sophisticated, determined and coordinated attackers that have been systematically compromising U.S. government and commercial computer networks for years. The vast majority of APT activity observed by MANDIANT has been linked to China."*<sup>267</sup>

## **CONTROL OF MANUFACTURING PROCESSES**

Recent years have seen significant outsourcing of America's traditional manufacturing capacity. The impetus for such outsourcing is generally related to economics or more suitable operating environments (favorable tax treatments, government subsidies, less onerous labor laws, etc.), and these outsourcing opportunities can be very attractive to U.S. companies. Regardless, they can result in potential compromises to national security in a variety of ways, to include malicious intent or unintentional design or fabrication errors.

One of the dilemmas currently facing the American defense establishment is how to maintain both strategic and tactical superiority in an environment where the manufacture and provisioning of critical technology infrastructure is being outsourced rapidly to entities that may not have U.S. national interests foremost in their minds. In some cases, the loyalties of these entities may lie first with other nations, some of whom may have geopolitical goals that run contrary to those of the United States.

<sup>265</sup> Google, Inc., Google Beijing, Google Shanghai, Google Guangzhou, and Google Hong Kong; see also Dambala, Inc., "The Command Structure of the Aurora Botnet, History, Patterns and Findings," March 3, 2010.

<sup>266</sup> Northrop Grumman Corp., "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" (paper produced for the U.S.-China Economic and Security Review Commission, October 2009).

[http://www.uscc.gov/researchpapers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper\\_FINAL\\_Approved%20Report\\_16\\_Oct2009.pdf](http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16_Oct2009.pdf).

<sup>267</sup> Mandiant, "M Trends: The Advanced Persistent Threat," January 2010.



The United States has evolved a growing dependency on foreign suppliers for a number of critical electronics components. As noted earlier, Chinese manufacturers have achieved significant integration into the communications supply chain through varying forms of investment. As a result, they have obtained technological expertise, lower cost capabilities that allow “supply chain dominance,” the ability not only to develop standards but also to dominate standards in many niches, and the ability to develop momentum in advancing development of next-generation technologies.<sup>268</sup>

Much of the U.S. economy and national well-being is irrevocably tied to the extensive system of voice, data, and video networks that tie together almost every fabric of our lives. This includes access to government information and services, contact with business associates, financial transactions, education, health care, management of utilities and other critical infrastructure, and social networking, among other baseline enabling functions. As technologies progress, the network continues to extend its reach to other devices, from the remotely monitored supervisory control and data acquisition (SCADA) systems that control public utilities, to personal electronics that allow remote activation of cell phones or other devices that can be accessed through or controlled by cell phones.<sup>269</sup> Disruptions, whether intentional or unintentional, can and do have profound consequences.



Lenovo Company Logo

**Lenovo's Entry into the U.S. Computer Market,  
and Controversies Surrounding its Government Sales**

Lenovo has emerged as one of the world's largest manufacturers of personal computers. Lenovo is headquartered in Purchase, New York, and manufactures in several locations in China as well as in Raleigh, North Carolina. The company began in 1984 as Legend Group, led by computer scientist Liu Chuanzhi. Legend originally received start-up capital from the Chinese Academy of Sciences, a government agency.<sup>270</sup> To date, Legend Holdings is the largest shareholder of Lenovo, and the Chinese Academy of Sciences owns 65 percent of Legend Holdings. In effect, the Chinese government is the largest shareholder in the company, though the extent of the government's role within the company is unclear.

In the 1990s, Lenovo served as the Chinese distributor for Hewlett-Packard Co. but has since expanded beyond manufacturing to information technology (IT) consulting, systems integration, software and e-commerce, mobile phones and personal digital assistants (PDA's). In 1994, the company listed on the Hong Kong Stock Exchange (HKSE: 0992) and is currently trading with a market capitalization of US\$41.52 billion.<sup>271</sup> The company grew steadily over the last decade

<sup>268</sup> Reperi - General conclusion from the Defense Science Board Task Force on High-Performance Microchips Supply, February 2005, pp. 29-32.

<sup>269</sup> Reperi – It is reasonable to conclude that disruptions of this nature would have a profound and far-reaching detrimental effect.

<sup>270</sup> Lenovo Group Ltd., NOVEL NY Business & Company Resource Center, July 1, 2010.

[http://ezproxy.library.nyu.edu:2081/servlet/BCRC?vrsn=unknown&locID=nysl\\_me\\_nyuniv&srchtp=glbc&cc=1&c=1&mde=c&ste=74&tbst=tsCM&tab=4&ccmp=Lenovo+Group+Ltd.&mst=lenovo&n=25&docNum=I2501310652&bConts=13119](http://ezproxy.library.nyu.edu:2081/servlet/BCRC?vrsn=unknown&locID=nysl_me_nyuniv&srchtp=glbc&cc=1&c=1&mde=c&ste=74&tbst=tsCM&tab=4&ccmp=Lenovo+Group+Ltd.&mst=lenovo&n=25&docNum=I2501310652&bConts=13119).

<sup>271</sup> Yahoo! Finance, Lenovo Group Ltd. HKD0.025 (0992.HK), July 1, 2010. <http://finance.yahoo.com/q?s=0992.HK>.

through acquisition of IT consulting and systems integration systems. Legend was renamed The Lenovo Group in 2003.

Most famously, Lenovo acquired IBM's Personal Computing Division in 2005 for US\$1.75 billion.<sup>272</sup> With the deal, Lenovo also acquired the right to IBM's Think Pad brand name for five years, although the company has focused on promoting its own brand name rather than leveraging the IBM name.<sup>273</sup> Lenovo's purchase of IBM's personal computer division was reviewed by the Committee on Foreign Investment in the United States, which allowed the deal to go through, with certain qualifications.<sup>274</sup>

However, Lenovo's success has also been accompanied by controversy. In spring 2006, concerns were raised by members of the U.S.-China Economic and Security Review Commission regarding a planned State Department purchase of 16,000 Lenovo computers, with 900 of the computers intended for use in a classified network connecting U.S. embassies and consulates.<sup>275</sup> Dr. Larry Wortzel, then chairman of the Commission, stated that "[i]f you're a foreign intelligence service and you know that a [U.S.] federal agency is buying... computers from [a Chinese] company, wouldn't you look into the possibility that you could do something about that?"<sup>276</sup> Another Commissioner, Michael Wessel, added that "[t]his event should trigger a broader review of our procurement policies for all our classified networks and communications."<sup>277</sup>

Representative Frank Wolf (R-Va.), then chairman of the House Appropriations Subcommittee on Commerce, Justice, State and the Judiciary, led the effort to address concerns about this issue. In the face of these objections, the State Department indicated that the Lenovo computers would be used only on unclassified networks. In a statement, Representative Wolf said that "I was deeply troubled to learn that the new computers were purchased from a China-based company.... This decision would have had dire consequences for our national security, potentially jeopardizing our investment in a secure IT infrastructure."<sup>278</sup>

For their part, Lenovo company officials have steadfastly denied that there are any reasons to worry about the security of the company's computers. Jeffrey Carlisle, vice president of government relations for Lenovo, stated that the computers would be manufactured in "the same places, using the same processes as I.B.M. had," and that "If anything were detected, it would be a death warrant for the company... No one would ever buy another Lenovo PC. It

<sup>272</sup> Kevin O'Brien, "Lenovo Steps Out Onto Global Stage," *International Herald Tribune*, March 9, 2006.  
[http://ezproxy.library.nyu.edu:2076/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T9663556996&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29\\_T9663556999&cisb=22\\_T9663556998&treeMax=true&treeWidth=0&csi=8357&docNo=1](http://ezproxy.library.nyu.edu:2076/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9663556996&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9663556999&cisb=22_T9663556998&treeMax=true&treeWidth=0&csi=8357&docNo=1).

<sup>273</sup> Glenn Rifkin and Jenna Smith, "Quickly Erasing 'I' and 'B' and 'M,'" *New York Times*, April 12, 2006.  
[http://ezproxy.library.nyu.edu:2076/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21\\_T9663910891&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29\\_T9663910894&cisb=22\\_T9663910893&treeMax=true&treeWidth=0&csi=6742&docNo=5](http://ezproxy.library.nyu.edu:2076/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9663910891&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9663910894&cisb=22_T9663910893&treeMax=true&treeWidth=0&csi=6742&docNo=5).

<sup>274</sup> Eric Bangeman, "Uncle Sam Looking Carefully at IBM/Lenovo Deal," *Ars Technica* (January 24, 2005).  
<http://arstechnica.com/old/content/2005/01/4550.ars>.

<sup>275</sup> Grant Gross, "U.S. State Department to Limit Use of Lenovo PCs," *ComputerWorld*, May 19, 2006.  
[http://www.computerworld.com/s/article/9000639/U.S.\\_State\\_Department\\_to\\_limit\\_use\\_of\\_Lenovo\\_PCs](http://www.computerworld.com/s/article/9000639/U.S._State_Department_to_limit_use_of_Lenovo_PCs).

<sup>276</sup> Eric Bangeman, "Lenovo Laptop Deal Draws Scrutiny from Government Agency," *Ars Technica* (March 26, 2006).  
<http://arstechnica.com/old/content/2006/03/6475.ars>.

<sup>277</sup> Grant Gross, "U.S. State Department Limits Use of Lenovo PCs," *PC World*, May 19, 2006.  
[http://www.pcworld.com/article/125802/us\\_state\\_department\\_limits\\_use\\_of\\_lenovo\\_pcs.html](http://www.pcworld.com/article/125802/us_state_department_limits_use_of_lenovo_pcs.html).

<sup>278</sup> Grant Gross, "U.S. State Department Limits Use of Lenovo PCs," *PC World*, May 19, 2006.  
[http://www.pcworld.com/article/125802/us\\_state\\_department\\_limits\\_use\\_of\\_lenovo\\_pcs.html](http://www.pcworld.com/article/125802/us_state_department_limits_use_of_lenovo_pcs.html).

would make no sense to do it."<sup>279</sup> Lenovo Chairman Yang Yuanqing told the Associated Press: "The [Chinese] government isn't involved in any daily operation of the company, including our strategic positions, appointment of our CEO, or our financing.... Our management team is in charge of that. I don't believe because Legend Holdings is our biggest shareholder that this means we are a government-controlled company."<sup>280</sup>

The experience may have left Lenovo executives with a sense that increased engagement with Congressional representatives might head off similar problems in the future, and starting in 2006 Lenovo began to sponsor lobbying efforts on Capitol Hill. From 2006-2009, Lenovo paid a total of \$1,060,000 to lobbying firms, engaging the services of Akin Gump Strauss Hauer & Feld; Capstrat; the Gallagher Group; the Duberstein Group; and Miller and Chevalier. The bulk of this amount was paid to Akin Gump Strauss Hauer & Feld: a total of \$920,000 for services in 2008-2009, for matters centered on "China" and "technology issues." In addition, Lenovo spent another \$2,619,000 in the same period to fund direct lobbying efforts by its own representatives.<sup>281</sup>

## MICROCHIP MANUFACTURING

### Key Cyber Security and National Security Risks

Recent years have seen increasing attention paid by public officials to the potential security vulnerabilities inherent in the offshoring of computer hardware manufacturing. As was stated in 2008 by Secretary of Homeland Security Michael Chertoff:

*A less often focused on [than cyber espionage] but equally significant threat comes from the supply chain. Increasingly when you buy computers they have components that originate from places all around the world. We need to look at the question of how we assure that people are not embedding in very small components or things that go into computers [things] that can be triggered remotely and then become the basis of ways to [steal] information or [that] could become botnets.*<sup>282</sup>

Representatives of private industry have also voiced concerns about the potential for security threats being embedded in computer hardware. As was stated in testimony before the U.S.-China Economic and Security Review Commission by Kevin Coleman, cyber security consultant and senior fellow with the Technolytics Institute:

*Hardware is just as susceptible as software is to hackers through the inclusion of malicious logic....Hidden malicious circuits provide an attacker with a stealthy attack vector. Commercial suppliers are increasingly moving the design, manufacturing, and testing stages of Integrated Circuit (IC) production to a diverse set of countries, which is making the securing of the IC supply chain infeasible. Together, commercial off-the-shelf (COTS) procurement and global production lead to an increasing risk of covert hardware/firmware based cyber attacks. The extraordinary effort required to uncover*

<sup>279</sup> Steve Lohr, "State Department Yields on PCs from China," *New York Times*, May 23, 2006.

<sup>280</sup> Gregg Keizer, "Lenovo Denies Its PCs Are Security Risk," *ChannelWeb*, May 25, 2006.

<sup>281</sup> <http://www.cnn.com/security/188500323;jsessionid=3RJWEDHCIPK0DQE1GHRSKHWATMY32JVN?itc=refresh>.

<sup>282</sup> Calculations performed by staff of the U.S.-China Economic and Security Review Commission based on examination of disclosure documents in the U.S. Senate Lobbying Disclosure Act database. Database available at [http://www.senate.gov/legislative//Public\\_Disclosure/LDA\\_reports.htm](http://www.senate.gov/legislative//Public_Disclosure/LDA_reports.htm).

<sup>282</sup> *Popular Mechanics*, "Homeland Chief Chertoff Gives Security Update," October 1, 2009. <http://www.popularmechanics.com/technology/gadgets/4237823>.

*such high-tech covert acts, combined with the massive number of chips we would have to test and validate from a circuitry and microcode perspective, as well as the need to scan through tens of millions of lines of code and validate each software instance on billions of devices, come together to make ensuring the integrity of our systems nearly impossible. Security must be designed and built in, not tested for after the fact.*<sup>283</sup>

Cyber security expert Jim Gosler<sup>284</sup> has stated that compromised chips and electronics have already been found in DOD systems: "We have found microelectronics and electronics embedded in applications that they shouldn't be there. And it's very clear that a foreign intelligence service put them there."<sup>285</sup>

**The Defense Science Board Task Force**  
**2005 Report on High-Performance Microchip Supply**

The Department of Defense has taken note of potential security concerns related to the outsourcing of microchip manufacturing. In a report released in early 2005 by the Defense Science Board Task Force on High-Performance Microchip Supply,<sup>286</sup> several statements highlight the dangers of relying on foreign sources for integrated circuit components used in military applications:

*"Trustworthiness includes confidence that classified or mission-critical information contained in chip designs is not compromised, reliability is not degraded, and unintended design elements are not inserted in chips as a result of design or fabrication in conditions open to adversary agents."*<sup>287</sup>

*"Defense system electronic hardware, like that used in commercial applications, has undergone a radical transformation. Whereas custom circuits, unique to specific applications, were once widely used, most information processing today is performed by combinations of memory chips (DRAMs, SRAMs, etc.) which store data (including programs), and programmable microchips, such as Structured ASICs [application-specific integrated circuits], Programmable Logic Arrays (PLAs), central processors (CPUs), and digital signal processors (DSPs), which operate on the data. Of the two classes of parts, the latter have more intricate designs, which make them difficult to validate (especially after manufacturing) and thus more subject to undetected compromise."*<sup>288</sup>

<sup>283</sup> U.S.-China Economic and Security Review Commission, *Hearing on China's Propaganda and Influence Operations, Its Intelligence Activities that Target the United States, and the Resulting Impacts on U.S. National Security*, testimony of Kevin Coleman, April 30, 2009.

<sup>284</sup> Jim Gosler is or has been a Sandia fellow, National Security Agency visiting scientist, and the founding director of the Central Intelligence Agency's Clandestine Information Technology Office. See The White House, "The United States Cyber Challenge," May 8, 2009. <http://www.whitehouse.gov/files/documents/cyber/The%20United%20States%20Cyber%20Challenge%201.1%20%208updated%205-8-09%29.pdf>.

<sup>285</sup> CBS News, 60 Minutes, "Cyber War: Sabotaging the System," November 8, 2009. <http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml>.

<sup>286</sup> Department of Defense, *Report of the Defense Science Board Task Force on High-Performance Microchips Supply* (Arlington, VA: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2005). <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.

<sup>287</sup> Department of Defense, *Report of the Defense Science Board Task Force on High-Performance Microchips Supply* (Arlington, VA: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2005), p. 17. <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.

<sup>288</sup> Department of Defense, *Report of the Defense Science Board Task Force on High-Performance Microchips Supply* (Arlington, VA: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2005), pp. 44-45. <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.



*"The semiconductor world can be divided into two broad producer segments – standard (commodity) and custom products. Standard products are sold to many customers for use in many applications; custom products – ASICs – are designed, manufactured and sold to one customer for specific uses. The economic models for suppliers and customers in these two segments are very different. While a great deal of attention is paid to securing trusted ASIC supplies for the DOD community, questions must also be asked about the future sources of standard commercial products."*<sup>289</sup>

*"Since it is clear that the general tendency is to manufacture leading-edge semiconductor products outside the United States and the fixed costs of ASIC design and fabrication are skyrocketing, a clear trend is emerging for designers to use as few custom semiconductor products as possible; instead, they employ programmable standard products. Semiconductor standard products are those whose functionality can be changed by software programming, as in the case of microprocessors (MPUs) and digital signal processors (DSPs), or hardware programmability, as in the case of field programmable products such as field programmable gate arrays. While these standard products will also increasingly be manufactured offshore, their functionality is mostly controlled by the user, [thus] it may be impossible to independently secure that functionality."*<sup>290</sup>

*"Programmable parts have more intricate designs, which make them difficult to validate (especially after manufacturing) and thus more subject to undetected compromise. Thus, it is important that programmable components be "trustable," though only to a degree that is commensurate with their application."*<sup>291</sup>

*"Trustworthiness of custom and commercial systems that support military operations – and the advances in microchip technology underlying our information superiority... ha[ve] been jeopardized. Trust cannot be added to integrated circuits after fabrication; electrical testing and reverse engineering cannot be relied upon to detect undesired alterations in military integrated circuits" (emphasis in original).*<sup>292</sup>

The production and manufacture of customized microchips such as application-specific integrated circuits (ASICs) is a complex process involving three phases: design, mask making, and fabrication. Each phase presents opportunities for an adversary to insert vulnerabilities that can render a device useless upon activation of a "kill" switch or change the functionality in a way that reduces security by leaking or corrupting sensitive data. Since a single device may contain millions of transistors, the ability to identify malicious circuits is almost impossible to accomplish either practically or economically.

<sup>289</sup> Department of Defense, *Report of the Defense Science Board Task Force on High-Performance Microchips Supply* (Arlington, VA: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2005), p. 39. <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.

<sup>290</sup> Department of Defense, *Report of the Defense Science Board Task Force on High-Performance Microchips Supply* (Arlington, VA: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2005), p. 40. <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.

<sup>291</sup> Department of Defense, *Report of the Defense Science Board Task Force on High-Performance Microchips Supply* (Arlington, VA: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2005), p. 40. <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.

<sup>292</sup> Department of Defense, *Report of the Defense Science Board Task Force on High-Performance Microchips Supply* (Arlington, VA: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2005), p. 3. <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.

During the design phase, engineers have direct access to the design database and can, if they so desire, make subtle changes that modify the functionality or insert malicious code such as kill switches, Trojan horses, worms, or many other backdoor features. During the masking phase, ultraviolet (UV) light is used to expose patterns on the layers of the microprocessor in a process similar to photography. Masks used for the chip-making process are called stencils. When these are used with UV light, they create various patterns on each layer of the microprocessor. Similar to the design phase, the masking phase offers a potential malicious actor the opportunity to change the design of the circuit by substituting one mask for another. Changing the mask allows the addition of transistors that can alter functionality or insert malicious code.

The fabrication phase is the final step in the production of ASICs. During manufacture, it is possible to make changes to the design or embed hundreds of additional transistors into each circuit with little probability of being detected. It is also possible to alter the functionality of an integrated circuit after manufacture by using a focused-ion-beam (FIB) etching machine to remove material from the chip and etch new connections between the transistors. While this is a legitimate process for modifying chip design, it can also be used for nefarious purposes in the hands of a skilled technician. This technology can be particularly useful to those wanting to disrupt U.S. systems by focusing on the maintenance and repair chain following the initial production of microchips.

#### **Recent Cases Involving Counterfeited Computer Equipment from China**

Over the past several years there have been a number of law enforcement cases involving counterfeit computer chips of Chinese origin that were sold to U.S. government agencies. Such cases raise concerns for the potential security risk of tampering. However, they also raise concerns of a more prosaic but still serious nature, such as the risk of defective components being installed in critical computer, communications, or weapons systems. Many of these cases have involved the counterfeiting of computer products produced and marketed by Cisco Systems, Inc. Three such examples are the following:

1. In January 2008, Michael and Robert Edman were charged with conspiring with a contact in China to purchase computer equipment and then falsely relabeling and selling the items as Cisco products. Operating under the company name Syren Technology, the two brothers allegedly shipped the counterfeit Cisco products directly to customers, including "the Marine Corps, Air Force, FBI [Federal Bureau of Investigation], Federal Aviation Administration, Department of Energy, as well as defense contractors, universities, school districts and financial institutions." The men entered a partial guilty plea to the charges in September 2009.<sup>293</sup>
2. In January 2010, Yongcai Li, a Chinese citizen, was sentenced in California to 30 months in prison and ordered to pay \$790,683 in restitution to Cisco Systems following from a conviction for trafficking in counterfeit Cisco computer products. Working through his company Gaoyi Technology, located in Shenzhen, China. Mr. Li procured counterfeit Cisco products in China and then shipped the products to the United States.<sup>294</sup>

<sup>293</sup> U.S. Attorney's Office for the Southern District of Texas Press Release, "Brothers Plead Guilty to Selling Counterfeit Cisco Products to Bureau of Prisons," September 9, 2009.  
<http://www.justice.gov/criminal/cybercrime/edmanPlea.pdf>.

<sup>294</sup> U.S. Department of Justice Press Release, "Departments of Justice and Homeland Security Announce 30 Convictions, More Than \$143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware," May 6, 2010. [http://www.fbi.gov/pressrel/pressrel10/convictions\\_050610.htm](http://www.fbi.gov/pressrel/pressrel10/convictions_050610.htm).



3. Also in January 2010, Ehab Ashoor, 49, a Saudi citizen, was sentenced in Texas to 51 months in prison and ordered to pay \$119,400 in restitution to Cisco Systems. A federal jury found Mr. Ashoor guilty of charges related to trafficking in counterfeit Cisco products. Although no specific security threat is alleged, a Department of Justice press release sounded a note of alarm about the case, noting that “Ashoor purchased counterfeit Cisco Gigabit Interface Converters (GBICs) from an online vendor in China with the intention of selling them to the U.S. Department of Defense for use by U.S. Marine Corps personnel operating in Iraq,” to be used on a computer network “used by the U.S. Marine Corps to transmit troop movements [and] relay intelligence.”<sup>295</sup>

Many such investigations into counterfeit computer equipment were conducted by federal authorities under the names of “Operation Cisco Raider” and “Operation Network Raider.” According to a Department of Justice statement made in May 2010:

*“To date, [Immigration and Customs Enforcement--ICE] agents have seized counterfeit Cisco products having an estimated retail value of more than \$35 million. ICE investigations have led to eight indictments and felony convictions... [Customs and Border Patrol--CBP] has made 537 seizures of counterfeit Cisco network hardware since 2005, and 47 seizures of Cisco labels for counterfeit products. In total, ICE and CBP seized more than 94,000 counterfeit Cisco network components and labels with a total estimated retail value of more than \$86 million during the course of the operation.”*<sup>296</sup>

However, the Department of Justice statement immediately above did not clearly indicate to what extent these counterfeit computer components originated in China and/or how many of the arrests and convictions involved linkages to China. Public statements from the Department of Justice have not alleged any negative actions by the Chinese government and have stressed the cooperative nature of these investigations with PRC officials: A Federal Bureau of Investigation (FBI) spokeswoman stated in May 2008 that the bureau “worked very closely with the Chinese government” on such cases,<sup>297</sup> and a May 2010 press release stated that “U.S. law enforcement authorities continue to work with China’s Ministry of Public Security (MPS) to combat the manufacture and export of counterfeit network hardware from China... This ongoing work is being facilitated by the [Intellectual Property] Criminal Enforcement Working Group of the U.S.-China Joint Liaison Group for law enforcement, which is co-chaired by the Criminal Division [of the FBI] and the MPS.”<sup>298</sup>

## TESTING OF INTEGRATED CIRCUITS

Testing of integrated circuits to ensure the integrity of batches and manufacturing processes dealing with physical consistency, authenticity, and materials integrity can be partially done using electric current testing and layer scanning methods currently in industry use. However,

<sup>295</sup> U.S. Department of Justice Press Release, “Departments of Justice and Homeland Security Announce 30 Convictions, More Than \$143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware,” May 6, 2010. [http://www.fbi.gov/pressrel/pressrel10/convictions\\_050610.htm](http://www.fbi.gov/pressrel/pressrel10/convictions_050610.htm).

<sup>296</sup> U.S. Department of Justice Press Release, “Departments of Justice and Homeland Security Announce 30 Convictions, More Than \$143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware,” May 6, 2010. [http://www.fbi.gov/pressrel/pressrel10/convictions\\_050610.htm](http://www.fbi.gov/pressrel/pressrel10/convictions_050610.htm).

<sup>297</sup> John Markoff, “FBI Says the Military Had Bogus Computer Gear,” *New York Times*, May 9, 2008.

<sup>298</sup> U.S. Department of Justice Press Release, “Departments of Justice and Homeland Security Announce 30 Convictions, More Than \$143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware,” May 6, 2010. [http://www.fbi.gov/pressrel/pressrel10/convictions\\_050610.htm](http://www.fbi.gov/pressrel/pressrel10/convictions_050610.htm).

exhaustive preventative testing of the deeply embedded purposes of designs within an integrated circuit is increasingly less possible as densities approach and increase below 20 nanometers. As stated in a March 2008 article from the online journal of the Institute of Electrical and Electronics Engineers:

- *Although commercial chip makers routinely and exhaustively test chips with hundreds of millions of logic gates, they can't afford to inspect everything. So instead they focus on how well the chip performs specific functions. For a microprocessor destined for use in a cell phone, for instance, the chip maker will check to see whether all the phone's various functions work. Any extraneous circuitry that doesn't interfere with the chip's normal functions won't show up in these tests...Nor can chip makers afford to test every chip. From a batch of thousands, technicians select a single chip for physical inspection, assuming that the manufacturing process has yielded essentially identical devices. They then laboriously grind away a thin layer of the chip, put the chip into a scanning electron microscope, and then take a picture of it, repeating the process until every layer of the chip has been imaged. Even here, spotting a tiny discrepancy amid a chip's many layers and millions or billions of transistors is a fantastically difficult task, and the chip is destroyed in the process.*<sup>299</sup>
- *A single plane like the DOD's next generation F-35 Joint Strike Fighter can contain an 'insane number' of chips, says one semiconductor expert familiar with that aircraft's design.*<sup>300</sup> *Estimates from other sources put the total at several hundred to more than a thousand. And tracing a part back to its source is not always straightforward. The dwindling of domestic chip and electronics manufacturing in the United States, combined with the phenomenal growth of suppliers in countries like China, has only deepened the U.S. military's concern.*<sup>301</sup>
- *Recognizing this enormous vulnerability, the DOD recently launched its most ambitious program yet to verify the integrity of the electronics that will underpin future additions to its arsenal. In December, the Defense Advanced Research Projects Agency (DARPA), the Pentagon's R&D wing, released details about a three-year initiative it calls the Trust in Integrated Circuits program. The findings from the program could give the military--and defense contractors who make sensitive microelectronics like the weapons systems for the F-35--a guaranteed method of determining whether their chips have been compromised.*<sup>302</sup>

Even if the military establishment is successful in determining which chips have been compromised in its microelectronics systems, problems with microchips and integrated circuits have the potential to cause significant harm to the entire country through disruptions of nonmilitary systems such as power plants, telephone systems, air traffic control infrastructure, Internet services, and private/public networks. Many, if not all, of these systems will continue to rely on nontrusted sources for technology products and services.

<sup>299</sup> Sally Adee, "The Hunt for the Kill Switch," *IEEE (Institute of Electrical and Electronics Engineers) Spectrum* (May 2008). <http://www.spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>.

<sup>300</sup> Sally Adee, "The Hunt for the Kill Switch," *IEEE (Institute of Electrical and Electronics Engineers) Spectrum* (May 2008). <http://www.spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>.

<sup>301</sup> Sally Adee, "The Hunt for the Kill Switch," *IEEE (Institute of Electrical and Electronics Engineers) Spectrum* (May 2008). <http://www.spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>.

<sup>302</sup> Sally Adee, "The Hunt for the Kill Switch," *IEEE (Institute of Electrical and Electronics Engineers) Spectrum* (May 2008). <http://www.spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>.

### **Kill Switches and Backdoors**

Although a sufficient reserve of trusted critical computer chips for a weapon system such as the F-35 can be identified and stockpiled, this is not the case with more commoditized telecommunications systems and components. The most-expected tampering threats in fabricating integrated circuits are generally assumed to be the inclusion of kill switches or backdoors. Each is defined as follows:

*A kill switch is any manipulation of the chip's software or hardware that would cause the chip to die outright... A backdoor, by contrast, lets outsiders gain access to the system through code or hardware to disable or enable a specific function. Because this method works without shutting down the whole chip, users remain unaware of the intrusion. An enemy could use it to bypass battlefield radio encryption, for instance.*<sup>303</sup>

Most computer users today are well aware of the risks in downloading computer viruses through software vulnerabilities, but few consider the dangers of purchasing a computer or other network devices with security risks already etched into the silicon used to make the microchips. As an example, encryption in today's systems is often done through integrated circuits dedicated to this function.

It is possible to add a code during the manufacture of the integrated circuit that will disable the encryption function when the code is received from an outside source. The circuit could also be altered through the addition of transistors that will disable encryption at a set time. Not knowing that encryption has been disabled, the user could continue to send sensitive or classified messages that would be readable by a hacker representing a hostile nation or a criminal enterprise.<sup>304</sup>

Flash memory could be added to networked printers that result in saving image files of every document printed and forwarding those images to a third party. Kill switches could be embedded into DOD systems to bring the systems down at a predetermined time or upon receipt of external instructions or codes. The potential for harm is enormous, extending from simple identity theft by criminal enterprises to disrupting networks and defense systems vital to national security.

<sup>303</sup> Sally Adey, "The Hunt for the Kill Switch," *IEEE* (Institute of Electrical and Electronics Engineers) *Spectrum* (May 2008). <http://www.spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>.

<sup>304</sup> Sally Adey, "The Hunt for the Kill Switch," *IEEE* (Institute of Electrical and Electronics Engineers) *Spectrum* (May 2008). <http://www.spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>.

## CONCLUSIONS & RECOMMENDATIONS

### SUPPLY CHAIN SECURITY AND POTENTIAL IMPACTS ON GOVERNMENT CONTRACTING FOR SENSITIVE SYSTEMS

The discussion of market segments and products discussed previously in this report demonstrates how enormously intertwined are the technology supply chains between the United States and China in the communications market and how varied the considerations are when assessing the relevant issues and impacts. An ever-growing multitude of components (hundreds of thousands, or perhaps millions) now constitute an integrated U.S. supply chain supporting communications and information exchanges on a global basis.

Analysis of China's technology integration is not so different from the analysis of the trade dynamics of any international resource: tracing trade routes, purchases, and ports of call reveals a great deal of information, some of which may be useful evidence in forming conclusions about source-derived risks. In technology, networks constitute global information "trade routes," with switches, routers, hubs, handsets, and computers becoming the ports of call. Numerous foreign manufacturers contribute to the supply chain in the U.S. communications sector. If foreign suppliers do not already provide the majority of products in these trade routes (either directly under their own brand names or indirectly under U.S. brand names), it is only a matter of time for this to become true if present trends continue.<sup>305</sup>

Diligent analysis of communications supply chains, such as switches, routers, modems, handsets, LANS, WANS, etc., reveals very few areas where supply chains did not have at least some integration with Chinese manufacturers as well as manufacturers from many other global points of origin. This is due in great part to sourcing strategies adopted by U.S. manufacturers and service providers. Outsourcing is one of the key ways in which U.S. product manufacturers have been able to achieve greater efficiencies in their business models, satisfying shareholder demands for ever-increasing profits and consumer demands for ever-improving value-to-price ratios.

However, as the extent of manufacturing outsourcing increases, the abilities of a nation to mitigate risks in its high-technology supply chain are further eroded. High-technology risks have accelerated in parallel with the dramatic development of telecommunications and information technologies. Vulnerabilities in the communications supply chain have the potential to be enormous given the complex number of manufacturers, mergers, acquisitions, and general globalization of the technology supply chain. A network architecture, whether in space or on the ground, might have thousands of suppliers and hundreds of thousands of subcomponents.

In many cases, U.S. government tracing of products or components to points of origin often consists of looking at product lines and "country of origin" based on 50 percent cost and point of "manufacture" rules (such as in the Buy America Act, or substantial transformation rules such as those found in the Trade Agreements Act).<sup>306</sup> Although components and subcomponents may be made in other countries, they may still be eligible to be sold as completed domestic products in the United States. Hypothetically, a U.S. buyer may not realize that a product designated as domestic under Buy America and Trade Agreements Act rules, and purchased from a domestic

<sup>305</sup> Reperi internal research on trends in the global communications supply chain.

<sup>306</sup> Reed Smith LLP, "New Amendment Rationalizes Country-of-Origin Preferences for Defense and Civilian Acquisitions," Client Bulletin 03-03, January 2003. <http://www.reedsmith.com/db/documents/bull0303.pdf>.

U.S. company, may still be partly or largely sourced from an overseas supplier. A meaningful attempt to trace product or component origins in the telecommunications and technology supply chains would be a monumental undertaking, requiring extraordinary levels of interaction and cooperation with both foreign and domestic businesses.

Using the U.S. Department of Defense as an example, tracing product origins adds layers of new complexity to an already complex supply chain environment. In a 2004 estimate, the Department of Defense maintained an inventory of supplies and equipment worth more than \$80 billion across multiple services and organizations, many of which use different automated supply systems.<sup>307</sup> Simply unifying and streamlining inventory management systems and methods is a difficult task that may take years to succeed, even without adding checks and balances based on considerations of electronic and information security risks based on product or component country of origin. In many cases, government procurement officials simply rely on established standard practices and do not examine products to a fine enough level to be meaningful for determining countries of origin at component levels.

According to the Defense Science Board Task Force, "The Defense Department does not directly acquire components at the integrated circuit level. Individual circuits are most often specified by designers of subsystems; even system primes have little knowledge of the sources of the components used in their system level products."<sup>308</sup> This is a particularly important point when considering government options: How will a government buyer know what it is procuring within the context of foreign supplier security risks at the integrated circuit level, if the prime manufacturer from whom they are purchasing does not know what it is selling?

## RESPONSES TO SUPPLY CHAIN CHALLENGES

Shaping the rate of change of supply chains and technologies will be a major challenge of the 21<sup>st</sup> century. We may have to cope both with technological change happening too fast (the tempo of technological developments producing new risks faster than the rate of effective response) or too slow (the tempo of innovation no longer being competitive). Are there ways constructively to change either the pace of technological change or the willingness of the U.S. market to be meaningfully selective in deciding which new technologies should be developed and adopted? Where supply chains are transforming too quickly or too slowly, how may their rate of change be influenced beneficially?

Government buyers and commercial providers must develop both a keener sense of component-level make-ups and capabilities/risks of telecom and technology products being sold to the U.S. government, and work together to mitigate or limit risks. U.S. government organizations must also become adept at tracking the dynamics of the global telecom and technology markets, to include maintaining a watchful eye on mergers, acquisitions, technology trends, and other business context changes that may have profound strategic meaning for government business.

<sup>307</sup> Daniel W. Engels et al., "Improving Visibility in the DOD Supply Chain," [http://www.almc.army.mil/aloc/issues/mayJun04/aloc\\_supple%20chain.htm](http://www.almc.army.mil/aloc/issues/mayJun04/aloc_supple%20chain.htm).

<sup>308</sup> Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on High-Performance Microchip Supply* (Arlington, VA: Department of Defense, February 2005), p. 5. <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.



In trying to determine the acceptability of risks resulting from further Chinese involvement in vital U.S. supply chains, issues such as Collingridge's "control dilemma" complicate the decision-making process.<sup>309</sup> That is to say, by locking in a technologically exclusionary policy too soon, the United States may irrevocably harm its own global competitiveness; However, delaying decision-making long enough to better understand the potential risks involved may result in limited options and lost opportunities, or in the worst cases, irrevocable harm if catastrophic consequences occur.

Globally, innovation in the communications industry is not uniform, unilateral, or symmetric, but it is rapid. The changing nature of innovation and sourcing is another conundrum that decision makers must wrestle with: how can policy frameworks account for the continuous nature of technological evolution and the vast and ever-evolving array of options for obtaining or providing new communications technologies? New thinking and a pluralistic institutional approach is called for that will provide appropriate mechanisms to:

- monitor new Chinese technologies and supply-chain risks to provide meaningful early warnings of unacceptable risks;
- spur American technological and supply-chain innovations that will enable means for responding to early warnings or mitigating the impacts of such risks when early warning surveillance fails; and
- provide effective implementation for appropriate technological or supply-chain responses, when such actions are warranted.

The rapid pace of change in the communications market, the profound impacts of these continual changes, and the way in which individual market segments play into the overall communications supply chain all warrant continual surveillance. How the U.S. government (and commercial vendors used by the government) may suffer from increased national security risk exposure, the erosion of the national industrial base, and other potential future liabilities and outcomes must be reassessed on an ongoing basis.

## **THE CHESS GAME OF STANDARDS – The New Method for Owning Supply Chains**

Large parts of the supply chain have gone to China – a transfer brought about by business evolution rather than revolution, with China filling a void created by a manufacturing base in America that, for many products, has been globally less competitive on a per-unit cost production basis. In many ways, China's presence in the U.S. supply chain has fulfilled vital needs of American companies and has been a "good marriage" for many. By all indications, Chinese companies have gone to considerable lengths to earn a seat among global technology giants such as IBM, Alcatel-Lucent, and other respected companies. On current growth paths, companies like Huawei should overtake the largest technology companies in the world. This is not surprising when we acknowledge that companies like Huawei have gone to great lengths to identify, understand, and emulate the most successful global business models they encounter.

---

<sup>309</sup>David Collingridge, "The Social Control of Technology," (Birmingham, England: University of Aston, Technology Policy Unit, 1980). The fundamental dilemma of technological governance is that, during early manifestations of technological evolution, there are many paths for advancement that may seem appropriate, but not enough is known to allow choosing the best paths forward. By the time enough is known about the impacts of a technological evolution for best paths to become apparent, society is already locked in, has vested its interests, and is left with limited options.



U.S. businesses looking to reduce labor costs have increasingly moved parts of their production chain to China. Initially, this involved preprocessing of raw materials and basic manufacturing to reduce costs and make companies more competitive. Over the years, this process has expanded to include much of the product development, design, and production cycles and is an expanding phenomenon fueled by circumstances within both the United States and China. Creating a technology product, such as a cell phone, or wireless broadband equipment like WiMAX (a standard much like the WiFi routers in our homes and offices – only designed to cover miles of distance) requires numerous manufacturers of all of the parts to agree on how those pieces are going to interoperate or work together. Numerous working groups exist to create standards so that wireless networks can operate on frequencies that are different in each country.

Eventually, standards are adopted and thousands of product parts are made to support that standard; for example, 3Com must design routers for wireless Internet protocols. For devices to talk to each other in the United States or globally, international bodies must agree on the standard that 3Com will use to guide its design process. Because the United States has been the technology leader of the world, most standards have been influenced by North American companies such as IBM, Intel, Cisco, 3Com, Qualcomm, Microsoft, Nortel, and Motorola. However, this is changing: In 2007, Intel received approval to perform chip manufacturing in China and is investing in research and development and production with Chinese manufacturers. This move was necessary to compete with Advanced Micro Devices and other manufacturers. As more products are manufactured overseas, supply chains have followed. In the wireless market, routers, cell phones, power supplies, peripherals, software, control devices, and semiconductors are produced in China. With China's ready supply of design engineers, innovative Chinese companies have spawned new, unique products.

Throwing a population of more than 1.5 billion potential consumers at the wireless market, then adding manufacturing for North America, South America, and Europe to the equation, gives China the ability to dominate standards--in other words, determine product specifications for next-generation products. In the communications world, that means the protocols for how networks will communicate will likely be heavily influenced by China, and manufacturers outside of the China market may begin to lose global market share in dramatic fashion.

## **INNOVATION IN AMERICA, AND THE SHORTAGE OF MATHEMATICIANS, SCIENTISTS, AND ENGINEERS**

The Thomson Reuters' *2008 Global Innovation Study* showed that on the basis of the total number of unique inventions issued in granted patents and published patent applications, 70 percent of the top ten innovators in the United States were non-U.S. companies. Meanwhile, U.S. companies are conspicuously absent from Asian and European top ten lists.<sup>310</sup> When we further examine the surge of patent filings in China (the number of patent filings is one of the classic indicators of the levels of innovation in a country), as of 2007 China was well ahead of the United States in the number of filings annually and may soon overtake the United States in the number of patents issued annually. Based on 2006 statistics, patent filings in China were

---

<sup>310</sup> Thomson Reuters, *2008 Global Innovation Study*, March 24, 2009.  
[http://science.thomsonreuters.com/press/2009/innovation\\_study/](http://science.thomsonreuters.com/press/2009/innovation_study/).

increasing at a rate of 20 percent per year, with Huawei Technologies standing as the single largest filer of 20-year patents.<sup>311</sup>

This comparative view offers an indication that innovation in China may be outpacing innovation in the United States and that the patent-seeking environment for multinational and U.S. entities is now dramatically more complicated. Earlier patent filings in China may represent prior arts<sup>312</sup> to a later patent filing in the United States. With China also offering ten-year intermediate patents (“utility model”) that do not require the same robust level of effort and proofs that are necessary to obtain a full-fledged 20-year invention patent (comparable intermediate patents are not available in the United States), American innovators may find themselves at a profound disadvantage in seeking intellectual property protections.

While the manufacturing supply chain has shifted to Chinese and overseas markets for a range of communications products, so have design and engineering. For America to remain competitive and generate future innovations, as well as to maintain control over technology standards, it is essential to provide incentives for continued development of the U.S. scientific and engineering workforce. Such an effort cannot be modest. It must be a commitment on a grand scale in order to reverse course and regain headway. Such measures would be akin to developing public-private partnerships that shift program dollars into funding tuition for math, science, and engineering.

Outsourcing the control of manufacturing and manufacturing processes also has the unintended consequence of making domestic revival of those processes more difficult. If a U.S. enterprise attempts to bring back some outsourced activities – even in an effort to reduce potential vulnerabilities – it may find that the necessary capabilities are difficult to reconstitute, due not just to a loss of physical plant facilities but also to an erosion in relevant skills among the workforce.<sup>313</sup> Outsourcing can also affect future prospects for technological innovation: As the outsourcing trend continues, it has already been shown that the number of students enrolling in engineering and computer science disciplines in the United States has been declining for several years. This trend will continue as long as the potential job market and pay structures offer fewer job opportunities. Talent will shift to where the leading-edge research and development is taking place.

The figure below illustrates how the loss of science and engineering graduates in America continues to contribute to this problem.

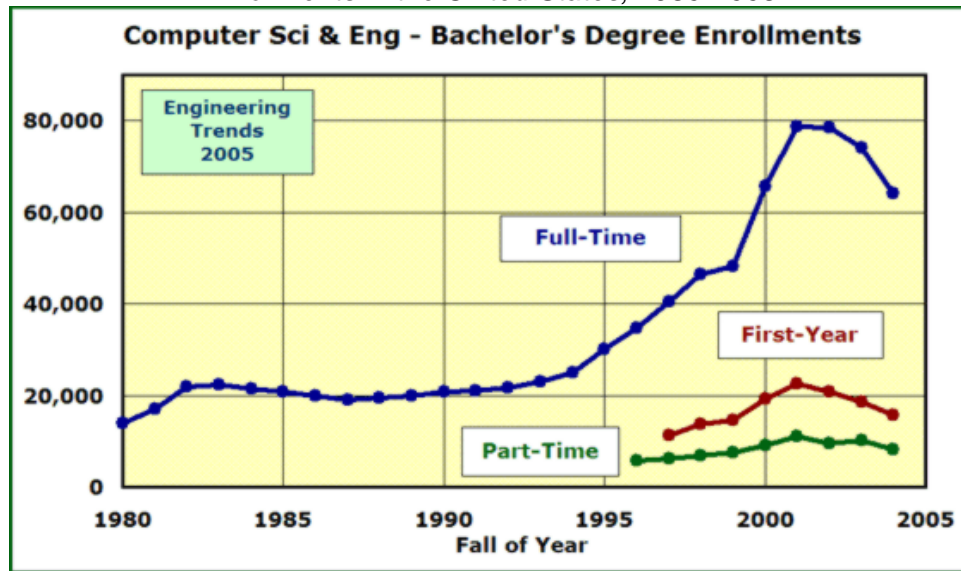
---

<sup>311</sup> Michael Orey, “Patent Filings Surge in China,” *Bloomberg Businessweek*, June 3, 2008. [http://www.businessweek.com/bwdaily/dnflash/content/jun2008/db2008063\\_332712.htm?chan=top+news\\_top+news+index\\_technology](http://www.businessweek.com/bwdaily/dnflash/content/jun2008/db2008063_332712.htm?chan=top+news_top+news+index_technology).

<sup>312</sup> In patent law, “prior art” is “all information that has been made available to the public in any form before a given date that might be relevant to a patent’s claims of originality... If an invention has been described in prior art, a patent on that invention is not valid.” See Wikipedia, “Prior Art.” [http://en.wikipedia.org/wiki/Prior\\_art](http://en.wikipedia.org/wiki/Prior_art).

<sup>313</sup> Reperi – General knowledge based on experience. Also, <http://www.engtrends.com/IEE/1005E.php>. Computer science and engineering saw declining student interest in the early 2000s. Relative undergraduate enrollments (“computer” fraction of engineering) began to decline in the late 1990s, and total undergraduate enrollments began to decline in the early 2000s. Data now show that graduate enrollments are being affected.

Table 3: Computer Science and Engineering Bachelor's Degree Enrollments in the United States, 1980-2005



Source: Engineering Trends website, "What Is Happening to Computer Science and Engineering?" Report 1005E, October 2005. <http://www.engtrends.com/IEE/1005E.php>.

Without necessary talent and processes in place, the United States could find itself at a disadvantage in dealing with foreign suppliers who may or may not be willing to supply the resources needed during a national emergency. Incentives are needed to stimulate development of next-generation technology solutions as well as alternatives that reduce dependency on foreign manufacturers. Developing such alternatives will require investment and the funding of continued technological innovation.

## PRODUCT CONTROL ISSUES IN GOVERNMENT COMMUNICATIONS SYSTEMS

The government should develop vulnerabilities models for assessing present and future supply chain vulnerabilities and their impacts on national security and network security, in tandem with supply chain testing of individual components. When risks are well quantified, reasonable actions should be taken to address any unacceptable impacts in the telecommunications and communications sector. This must be done particularly with an eye toward protecting critical elements of the defense industrial base and secure critical communications infrastructure. Such steps might include the following:

- Developing incentives for returning critical vulnerable supply chain elements back to the United States for manufacturing by U.S. companies.
- Asking vendors, in acquiring commercial network services from commercial providers, to inventory and certify vital networks to the component and individual component level, identifying which subelements were manufactured by foreign manufacturers either inside or outside of the United States, regardless of brand identity.
- Eliminating or reducing the number of non-U.S. vendors who receive government funds for contracting and/or subcontracting work on sensitive systems. (This has been difficult to accomplish, primarily due to the global nature of manufacturing and resource

acquisitions, as well as to government pressures to reduce costs. Turning the situation around and moving against the stream will cost ever more as time progresses and be ever more difficult to implement.)

In gaining a broad and deep view of the infusion of outsourced technologies and products, we see signs of momentum that are potentially irresistible. The American economy must learn how to thrive in the avalanche zone of the global telecom and technology marketplaces. America must learn to emphasize and export those areas of business where America offers a better value, and efficiently and safely import in those areas where America does not offer better value.

It will be important to observe China's strategic investments in technology throughout the communications supply chain. An appropriate, multifaceted approach would include a review of each layer of the supply chain based upon historical facts covering mergers and acquisitions, technology architectures, technology evolutions, and supply chain consolidations. Without being unduly alarmist, decision makers in both government and industry should nevertheless take an objective look at the potential security vulnerabilities posed by dependence upon Chinese corporations for electronics components and/or telecommunications services and work toward solutions that appropriately balance U.S. economic and national security interests.

## APPENDIX A

### WHAT IS A CYBER ATTACK?

Most personal computers are now networked and have access to other systems throughout the Internet and/or private networks managed or leased by government agencies and business enterprises. The ready linkages between personal computers have facilitated the spread of malicious code often referred to as viruses or malware. (The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including computer viruses, worms, Trojan horses, most rootkits, backdoors, botnets, and other malicious and unwanted software, including true viruses.<sup>314</sup>)

Network services such as the Internet; e-mail; instant messaging; and file-sharing systems, such as social networking sites, can all be used to propagate malware. It is easy to load malware to a system from a compact disk, USB (universal serial bus) storage device, or many similar means. Furthermore, new devices and external links are constantly introduced to wire-line and wireless networking environments. We live in a networked world, and almost every device accessing those networks can pose a potential cyber security risk.

Antivirus software is used to prevent, detect, and remove malware, including computer viruses, worms, and Trojan horses. A variety of strategies are typically employed to thwart malware. Signature-based detection involves searching for known malicious patterns in executable code. However, it is possible for a user to be infected with new malware for which no remedy yet exists. To counter such "zero-day" threats, heuristics (a *heuristic* is a mental shortcut that allows people to solve problems and make judgments quickly and efficiently) can be used. One type of heuristic approach, generic signatures, can identify new viruses or variants of existing viruses by looking for known malicious code (or slight variations of such code) in files. Some antivirus software can also predict what a file will do if opened/run by emulating it in a sandbox (a "firewalled" application space that allows an operating system to safely run a program as a test, to see if it might be hostile before allowing it to run in the system's main memory space) and analyzing what it does to see if it performs any malicious actions. If it does, this could mean that the file is malicious.<sup>315</sup>

Unlike other exploits, distributed denial of service (DDOS) attacks are not used to gain unauthorized access or control of a system; instead, they are designed to render the system unusable. One common method of attack involves saturating the target (victim) machine with external communications requests such that it cannot respond to legitimate traffic or responds

---

<sup>314</sup> A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the owner. A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other computers on the network, and it may do so without any user intervention. A Trojan horse is a program that disguises itself as another program. Similar to viruses, these programs are hidden and usually cause an unwanted effect, such as installing a backdoor into the system that can be used by hackers. Rootkits allow the concealment of a malicious program that is installed on a system by modifying the host operating system so that the malware is hidden from the user. Rootkits can prevent a malicious process from being visible in the system's list of processes or keep its files from being read. A backdoor is a method of bypassing normal authentication procedures. Once a system has been compromised (by one of the above methods or in some other way), one or more backdoors may be installed. Backdoors may also be installed prior to malicious software, to allow attackers entry. In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as botnets. In a botnet, the malware allows the attacker to give instructions to all the infected systems simultaneously. Botnets can also be used to push upgraded malware to the infected systems, keeping them resistant to antivirus software or other security measures.

<sup>315</sup> Peter Szor, *The Art of Computer Virus Research and Defense*, (Addison-Wesley, 2005), pp. 474–481.

so slowly as to be rendered effectively unavailable. In general terms, DDOS attacks are implemented by either forcing the targeted computer(s) to reset, consuming its resources so that it can no longer provide its intended service, or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.<sup>316</sup>

On two occasions to date, attackers have performed domain name server (DNS) backbone distributed denial of service attacks on the overall Internet DNS root servers. Since this class of DNS provides baseline DNS service to the entire Internet, these two DDOS attacks might be classified as attempts to take down the entire Internet; however, it is unclear what the attackers' true motivations were. The first occurred in October 2002 and disrupted service at nine of the 13 root servers. The second occurred in February 2007 and caused disruptions at two of the root servers.<sup>317</sup>

In the weeks leading up to the five-day 2008 South Ossetia war, a DDOS attack directed at Georgian government sites containing the message "win+love+in+Rusia" effectively overloaded and shut down multiple Georgian servers. Websites targeted included the website of the Georgian president, Mikhail Saakashvili, (which was rendered inoperable for 24 hours), and the National Bank of Georgia. The Russian government was widely suspected of orchestrating the attack through a proxy, the St. Petersburg-based criminal gang known as the Russian Business Network, or R.B.N. However, the Russian government denied the allegations, stating that it was possible that individuals in Russia or elsewhere had taken it upon themselves to start the attacks.<sup>318</sup>

During the 2009 Iranian election protests, foreign activists seeking to help the opposition engaged in DDOS attacks against Iran's government. The official website of the Iranian government (ahmedinejad.ir) was rendered inaccessible on several occasions.<sup>319</sup>

Analysis by researchers indicates that the United States is highly vulnerable to cyber attack<sup>320</sup> and that China has been working hard to develop cyber warfare capabilities for approximately 20 years. In the event of a major conflict with the United States with a cyber dimension, an attacker might concentrate some of its most devastating attacks on American

<sup>316</sup> CERT Coordination Center, Software Engineering Institute, *Denial of Service Attacks* (Pittsburgh, PA: Carnegie Mellon University, [http://www.cert.org/tech\\_tips/denial\\_of\\_service.html](http://www.cert.org/tech_tips/denial_of_service.html)).

<sup>317</sup> Wikipedia, "Distributed Denial of Service Attacks on Root Nameservers."

[http://en.wikipedia.org/wiki/Distributed\\_denial\\_of\\_service\\_attacks\\_on\\_root\\_nameservers](http://en.wikipedia.org/wiki/Distributed_denial_of_service_attacks_on_root_nameservers). The reference does not identify who runs the root servers that were attacked. Further research shows that in the February 2007 attack, at least six root servers were attacked but only two of them were noticeably affected: the "g-root," which is run by the U.S. Department of Defense and is physically based in Ohio, and the "l-root," run by the Internet Corporation for Assigned Names and Numbers (ICANN), which is physically based in California. Reference:

<http://www.icann.org/en/announcements/factsheet-dns-attack-08mar07.pdf>.

October 2002 - The 13 domain name service root servers are designated "A" through "M." The most affected servers, according to Matrix NetSystems, were the "A" and "J" servers owned by VeriSign Global Registry Services in Herndon, Va.; the "G" server owned by the U.S. Department of Defense Network Information Center in Vienna, Va.; the "H" server at the U.S. Army Research Lab in Aberdeen, Md.; the "I" server, located in Stockholm; the "K" server, located in London; and the "M" server, located in Tokyo. This reference identifies seven of the nine servers:

[http://news.cnet.com/Assault-on-Net-servers-fails/2100-1002\\_3-963005.html?tag=mncol](http://news.cnet.com/Assault-on-Net-servers-fails/2100-1002_3-963005.html?tag=mncol).

<sup>318</sup> John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008.

<http://www.nytimes.com/2008/08/13/technology/13cyber.html?ref=world>.

<sup>319</sup> Noah Shachtman, "Activists Launch Hack Attacks on Tehran Regime," *Wired*, June 15, 2009.

<sup>320</sup> Alex Spillius, "Cyber Attack 'Could Fell US Within 15 Minutes'," *Telegraph* (UK), May 7, 2010.

<http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7691500/Cyber-attack-could-fell-US-within-15-minutes.html>.



energy interests within the United States and abroad.<sup>321</sup> However, proving that a nation, such as China, is the source of such an attack would be very difficult, if even possible, due to the extremely fluid and dynamic nature of cyberspace.

A key fear among analysts is that the potential impact of cyber attacks remains poorly understood and potentially underestimated.<sup>322</sup> There are issues with how cyber attacks are classified and dealt with by decision makers: For example, cyber espionage is a form of attack but does not require the same type of response as a cyber intrusion that is perpetrated in order to create a cascading failure of a nation's power infrastructure or a malware attack intended to destroy data.

Comprehensive analysis has been done on China's cyber warfare capabilities, with conclusions indicating a mature capability with comprehensive doctrine and global reach:

*In a conflict with the US, China will likely use its CNO [computer network operation] capabilities to attack select nodes on the military's Non-classified Internet Protocol Router Network (NIPRNET) and unclassified DoD and civilian contractor logistics networks in the continental US (CONUS) and allied countries in the Asia-Pacific region. The stated goal in targeting these systems is to delay US deployments and impact combat effectiveness of troops already in theater. No authoritative PLA open source document identifies the specific criteria for employing [a] computer network attack against an adversary or what types of CNO actions PRC leaders believe constitutes an act of war. Ultimately, the only distinction between computer network exploitation and attack is the intent of the operator at the keyboard: The skill sets needed to penetrate a network for intelligence gathering purposes in peacetime are the same skills necessary to penetrate that network for offensive action during wartime. The difference is what the operator at that keyboard does with (or to) the information once inside the targeted network. If Chinese operators are, indeed, responsible for even some of the current exploitation efforts targeting US Government and commercial networks, then they may have already demonstrated that they possess a mature and operationally proficient CNO capability.*<sup>323</sup>

-- Northrop Grumman Corporation

<sup>321</sup> Daniel Ventre, "China's Strategy for Information Warfare: A Focus on Energy," *Journal of Energy Security* (May 18, 2010). [http://www.ensec.org/index.php?option=com\\_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361](http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361).

<sup>322</sup> Stephen M. Walt, "Is the cyber threat overblown?" *Foreign Policy* (March 30, 2010).

[http://walt.foreignpolicy.com/posts/2010/03/30/is\\_the\\_cyber\\_threat\\_overblown?obref=obnetwork](http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown?obref=obnetwork).

<sup>323</sup> Northrop Grumman Corporation, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (study performed on behalf of the U.S.-China Economic and Security Review Commission), October 16, 2009.

[http://www.uscc.gov/researchpapers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper\\_FINAL\\_Approved%20Report\\_16\\_Oct2009.pdf](http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16_Oct2009.pdf).

## APPENDIX B GLOSSARY

<b>GLOSSARY</b>	
<b>1G</b>	Analog cellular wireless -- in essence, the first generation of cellular wireless standards introduced in 1981.
<b>2G</b>	Digital cellular wireless, the second generation of cellular wireless standards introduced in 1992.
<b>3G</b>	The third generation of cellular wireless standards, introduced in 2002, based on International Mobile Telecommunications-2000, or "IMT-2000," also known as 3G or 3rd generation. In essence, 3G provides multimedia support, spread spectrum transmission, and at least 200 kbit/s broadband bandwidth. 3G is based on a family of standards for mobile telecommunications meeting specifications established by the International Telecommunication Union (ITU). 3G includes UMTS, CDMA2000, DECT (Digital Enhanced Cordless Telecommunications – a digital communication standard principally used for creating cordless phone systems), and WiMAX (Worldwide Interoperability for Microwave Access).
<b>4G</b>	The fourth generation of cellular wireless standards and a successor to the 1G, 2G, and 3G families of standards. In essence, 4G refers to all-IP-packet-switched networks, mobile ultrabroadband access (gigabit speed), and multicarrier transmission. Pre-4G technologies such as mobile WiMAX (available since 2006 – the proposed 802.16m standard) and 3G Long-Term Evolution (available since 2009 – LTE is considered a "3.9G" standard).
<b>ANDROID</b>	Google's operating system for mobile devices.
<b>ASIC</b>	Application-Specific Integrated Circuit.
<b>BACKBONE</b>	Primary transit networks or series of networks designed to carry data between different WANS or LANS. Backbones usually have greater data carrying capacity, or "bandwidth," than the networks they are interconnecting. The Internet Backbone is the interconnection of high-speed networks, primarily government, commercial telecommunications, and academic, that route data for Internet users.
<b>BACKDOOR</b>	A method of gaining remote control of a victim's computer through the use of a surreptitious means of entry built into a legitimate software or system. In essence, backdoors are created by configuring installed legitimate software to allow backdoor access, or through the installation of a specialized program designed to allow access under attacker-defined conditions. Trojan horse programs and rootkits often contain backdoor components.
<b>BASIS-OF-TRADE</b>	Relative trade or import/export strengths and weaknesses a nation or other entity has in relation to others and the marketplace in general.
<b>BBP</b>	A phone's Baseband Processor – the processor chipset that is designed to process signals for the telephone handset or system.
<b>BLUETOOTH</b>	Bluetooth is an open wireless technology standard for creating personal area networks (PANs) with high levels of security, and exchanging data over short distances using short-length radio waves from fixed and mobile devices. Bluetooth uses frequency-hopping spread spectrum, which breaks apart data being sent and transmits portions of it on up to 79 bands of 1 MHz width in the range 2402-2480 MHz, which is in the globally unlicensed Industrial, Scientific, and Medical (ISM) 2.4 GHz short-range radio frequency band.
<b>BRIC</b>	BRIC nations (Brazil, Russia, India, and China) in market analysis. An acronym used by Jim O'Neill during his time as head of global economic research at Goldman Sachs in 2001. According to a Goldman Sachs paper in 2005, Mexico and South Korea are comparable to the BRICs but were

	excluded initially because their economies were considered to be more developed already. Goldman Sachs argued that due to rapid development in the BRIC, by 2050 their combined economies might eclipse the combined economies of the current richest nations. Combined, the BRIC accounts for more than 25 percent of the world's land area and more than 40 percent of global population.
<b>BROADBAND</b>	An Internet connection with a much larger capacity than dial-up or ISDN (typically greater than 200 kilobits/per second).
<b>CDMA2000</b>	A family of 3G mobile technology standards that use CDMA channel access to send voice, data, and signaling data between mobile phones and cell sites.
<b>CFIUS</b>	Committee on Foreign Investment in the United States – an interagency committee of the U.S. government that reviews national security implications of foreign investments in U.S. companies or markets. <a href="http://www.treas.gov/offices/international-affairs/cfius">http://www.treas.gov/offices/international-affairs/cfius</a>
<b>CHIPSETS</b>	A set of specialized chips in a system's main, peripheral, or expansion circuitry.
<b>CIC</b>	China Investment Corporation, headquartered in Beijing. <a href="http://www.china-inv.cn/cicen">http://www.china-inv.cn/cicen</a> .
<b>CNA</b>	Computer Network Attack – The use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.
<b>CNCI</b>	Comprehensive National Cybersecurity Initiative. <a href="http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative">http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative</a> .
<b>CND</b>	Computer Network Defense – The use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and computer networks.
<b>CNE</b>	Computer Network Exploitation – Enabling operations and intelligence collection through computer networks to gather data from target systems or networks.
<b>CNO</b>	Computer Network Operations – encompasses Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE).
<b>CONUS</b>	Continental United States. Typically refers to being geographically located within the boundaries of the 48 contiguous states of the United States. CONUS does not typically include Hawaii and Alaska or the outlying territories (Guam, Puerto Rico, etc.).
<b>CPU</b>	Central Processing Unit – the central processor portion of a computer system that carries out the main instructions of a computer program and is the primary element carrying out the computer's functions.
<b>CYBER SECURITY</b>	Security against electronic attacks, such as cyber warfare and other forms of hostile CNO.
<b>DATA COM</b>	Data Communications.
<b>DDOS</b>	Distributed Denial of Service (DDOS) attacks – attacks that consume computing or communications resources by engaging many intermediate (or proxy) computers simultaneously to attack one or a few victims with a flood of traffic and system requests. The purpose is to flood target systems with so much traffic and/or so many computational requests that no other traffic can get through or no other useful functions can occur. Intermediate or proxy systems used in DDOS attacks have often been previously compromised and are under the control of hostile actors.
<b>DNS</b>	Domain Name Server.
<b>DRAM</b>	Dynamic random access memory – a type of random access memory that stores each bit of data in a separate capacitor within an integrated circuit.
<b>DSL</b>	A family of technologies that provides digital data transmission over the wires

	of a local telephone network. This is typically a terrestrially based technology for providing broadband services over legacy copper-wire infrastructures of PSTNs (Public Switched Telecommunications Network).
<b>DSP</b>	Digital signal processing--a specialized microprocessor with an architecture optimized for digital signal processing.
<b>EDGE</b>	Enhanced Data rates for GSM Evolution (EDGE) – also known as Enhanced GPRS (EGPRS), IMT Single Carrier (IMT-SC), or “Enhanced Data rates for Global Evolution.” A backward-compatible digital mobile phone technology allowing improved data transmission rates on top of standard GSM.
<b>ELECTRO-OPTICAL</b>	Pertaining to effects of an electric field on the optical properties of a material.
<b>ESSENTIAL PATENTS</b>	Patents that disclose and claim one or more inventions that are required to practice a given industry standard. Standardization bodies often require that members disclose and grant licenses to patents and pending patent applications that they own and that cover a standard that the body is developing. If standards bodies fail to get licenses to all patents that are essential to practicing a standard, then the owners of those unlicensed patents can often demand royalties from those who ultimately adopt the standards.
<b>ETHERNET</b>	A set of network cabling and network access (CSMA/CD) protocol standards for bus topology computer networks invented by Xerox Corporation and now managed by the 802.3 subcommittee of the IEEE (Institute of Electrical and Electronics Engineers).
<b>EV-DO</b>	“Evolution-Data Optimized” or “Evolution-Data Only,” abbreviated as EV-DO or EVDO and often EV, is a 3G telecommunications standard for the wireless transmission of data through radio signals for broadband Internet access.
<b>FAR</b>	The U.S. government’s Federal Acquisition Regulation – the principal set of rules in the Federal Acquisition Regulation System.
<b>FIB</b>	Focused-Ion-Beam.
<b>FIREWALL</b>	Part of a system or network designed to block unauthorized access while permitting authorized communications.
<b>FREQUENCY DIVISION</b>	Frequency-Division Duplexing (FDD) means that the transmitter and receiver operate at different carrier frequencies.
<b>FREQUENCY-HOPPING SPREAD-SPECTRUM</b>	A method of transmitting radio signals by rapidly switching a carrier among many frequency channels using pseudo-random sequences known to transmitter and receiver pairs or groups.
<b>FTP</b>	File Transfer Protocol - A standard Internet protocol implemented in FTP server and client software and most web browsers to “transfer data reliably and efficiently.”
<b>GPS</b>	The U.S. Global Positioning System.
<b>GSE</b>	Government-sponsored enterprises--a group of financial services corporations created by the United States Congress. GSEs' function is to enhance the flow of credit to targeted sectors of the economy and to make those segments of the capital market more efficient and transparent. Residential mortgage borrowing is the largest of the borrowing segments in which the GSEs operate, in which they hold approximately \$5 trillion worth of mortgages.
<b>GSM</b>	Global System for Mobile Communications – a wireless mobile telephone standard in use broadly on a worldwide basis.
<b>HACKER</b>	An individual using computer technology in hostile or nefarious ways generally not originally intended by the publisher or manufacturer. In essence, people who attack others using computers or networks.
<b>HOTSPOT</b>	A physical site that offers Internet access over a wireless local area network.

	Hotspots are typically based on WiFi technology.
<b>HSDPA</b>	High-Speed Downlink Packet Access.
<b>HTTP</b>	Hypertext Transfer Protocol – The message format and exchange standard used by web browsers and web servers.
<b>HUB</b>	An unintelligent device for connecting multiple twisted pair or fiber-optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. Hubs are a form of multiport repeater.
<b>IC</b>	Integrated Circuit.
<b>IDS</b>	Intrusion Detection System – A computer or network monitoring system capable of matching observed phenomenon to patterns of known or suspected unauthorized activity and using this as a basis for intercepting penetrations by hostile users or applications.
<b>IEEE</b>	Institute of Electrical and Electronics Engineers.
<b>INFOCON</b>	Information Operations Condition – INFOCON classifications mirror those used in the Defense Conditions (DEFCON) Alert System and are a uniform system of five progressive readiness conditions (INFOCON 5 thru INFOCON 1). INFOCON 5 indicates nominal conditions at normal levels of readiness. INFOCON-1 indicates a maximum level of high alert due to impending severe threat or attack. As INFOCON levels increase, elements of network functionality or services deemed lower priority or at high risk of attack may be temporarily suspended. Offensive CNA tools used by hostile attackers that might be effective during an INFOCON-5 normal state of readiness may be rendered ineffective if the services or applications they exploit are turned off.
<b>INTERNET</b>	Global networks of computers that communicate using Internet Protocol (IP) and Border Gateway Protocol (BGP) to identify the best paths to route communications between end-points.
<b>IP ADDRESS</b>	Internet Protocol Address – a number assigned to each computer's or other device's network interface(s) that are active on a network supporting the Internet Protocol.
<b>IP TELEPHONY</b>	Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies that deliver voice communications over IP networks (the Internet or other packet-switched networks). Other terms frequently encountered and synonymous with VoIP are "IP Telephony," "Internet Telephony," Voice Over Broadband (VoBB), "Broadband Telephony," and "Broadband Phone." Communications services (voice, facsimile, and/or voice-messaging applications) that are transported via the Internet rather than the public switched telephone network (PSTN).
<b>IPS</b>	Intrusion Prevention System – an inline system or software that applies IDS-style logic and approves or rejects network traffic, program and data access, hardware use, etc. Where an IDS is designed to detect intrusions that are in progress and intercept/manage them before they progress too far, an IPS is designed to prevent intrusions from gaining any penetration whatsoever.
<b>IPV4</b>	Internet Protocol version 4 is the fourth revision in the development of the Internet Protocol and the first version of the protocol to be widely deployed. A connectionless protocol for use on packet-switched Link Layer networks such as Ethernet. IPv4 operates on a "best effort" delivery model that does not guarantee delivery, proper sequencing, or duplicate delivery. Delivery and data integrity are addressed by TCP (Transmission Control Protocol), an upper-layer transmission control protocol – hence the common acronym "TCP/IP". IPv4 uses 32-bit (four-byte) addresses, limiting address space to 4,294,967,296 possible unique addresses. Some are reserved for special purposes, such as private networks (~18 million addresses) or multicast addresses (~270 million addresses), reducing the number of addresses that potentially can be allocated for routing on the public Internet. IPv4 address



	shortages have been developing and will eventually result in exhaustion of IPv4 address space, which has led to development of the IPv6 protocol as a long-term solution.
<b>IPV6</b>	Internet Protocol version 6 is an Internet Protocol version that is designed to succeed IPv4. IPv6 was defined in December 1998 by the IETF (Internet Engineering Task Force) with publication of RFC 2460. IPv6 has a larger address space than IPv4 due to the use of a 128-bit address versus IPv4's 32-bit address. IPv6's new address space supports $2^{128}$ (about $3.4 \times 10^{38}$ ) addresses. This dramatic expansion provides flexibility in allocating addresses and routing traffic and eliminates the widespread need for network address translation (NAT). IPv6 is a vastly improved protocol standard that incorporates many new enhancements over IPv4 in addition to a vastly increased address space. New routing techniques, expanded protocol capabilities, enhanced security, and other improvements are available in IPv6.
<b>ISP</b>	Internet Service Provider.
<b>IW</b>	Information Warfare – Efforts to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own resources.
<b>IXP</b>	Internet Exchange Point (IX or IXP) – a physical infrastructure through which Internet service providers exchange Internet traffic between their networks.
<b>JAILBREAKING</b>	A process that allows iPad, iPhone, and iPod Touch users to run any software code on their devices, as opposed to only code authorized by Apple. Once jailbroken, device users are able to download many extensions and themes previously unavailable through Apple's App Store, via pirated or unofficial means.
<b>LAN</b>	Local Area Network – an interconnection of computers that are in relatively close proximity to one another, such as within a building.
<b>LAST-MILE</b>	The "last mile" or "last kilometer" is the final leg of delivering connectivity from a communications provider to a customer.
<b>LEGACY</b>	Systems or applications that continue to be used beyond intended service life because users do not want to replace or redesign them.
<b>LMR</b>	Land Mobile Radio – a wireless communications system intended for use by terrestrial users in vehicles (mobile) or on foot (portable). LMR is typically used by emergency first responder, public works, or companies with large numbers of vehicle or field staff. LMR systems may be independent but often are connected to other fixed systems such as the public switched telephone network (PSTN) or cellular networks.
<b>LTE</b>	Long-Term Evolution), also known as "3.9G," is the trademarked project name of a high-performance air interface for cellular mobile telephony. It is a project of the 3rd Generation Partnership Project (3GPP), operating under a name trademarked by the European Telecommunications Standards Institute. The current generation of mobile telecommunication networks are collectively known as 3G (for "third generation"). Although LTE is often marketed as 4G, LTE is actually a 3.9G technology (pre-4G). LTE does not fully comply with IMT Advanced 4G requirements. As a pre-4G standard, LTE is evolving into "LTE Advanced," a 4th generation standard (4G) radio technology.
<b>MACRO LEVEL</b>	Characterizes societies or systems as a whole, rather than parts (meso- or microlevels).
<b>MICROCHIP</b>	An integrated circuit (also known as IC, microcircuit, microchip, silicon chip, or chip). Miniaturized electronic circuits that consist mainly of semiconductor devices and other passive components and that are manufactured in the surface of thin substrates of semiconductor materials.
<b>MIIT</b>	The Ministry of Industry and Information Technology of the People's Republic of China. <a href="http://www.miit.gov.cn">http://www.miit.gov.cn</a> .
<b>MOTHERBOARD</b>	The main or central circuit board in modern computers that holds many crucial system components and provides connectors for other accessory system



	components and peripherals.
<b>MPU</b>	Microprocessor Unit – a term occasionally used to describe a CPU (Central Processor Unit).
<b>NBA</b>	Network Behavioral Analysis – intrusion detection systems that detect and model network traffic to discern and analyze violations of known benign activities.
<b>NIPRNET</b>	Nonclassified Internet Protocol Router Network. A network of the U.S. Department of Defense providing unclassified Internet access and interconnectivity to DOD users and facilities.
<b>NODE</b>	Typically, the individual devices or computers on a network.
<b>OBEX</b>	OBEX (Object EXchange), and IrOBEX (Infrared OBEX), is a communications protocol facilitating exchange of binary data between devices. The OBEX standard is managed by the Infrared Data Association and has also been adopted by the Bluetooth Special Interest Group and the SyncML wing of the Open Mobile Alliance (OMA).
<b>OCONUS</b>	Outside of the geographic boundary of the contiguous 48 states of the United States. In essence, the opposite of CONUS.
<b>OUTSOURCING</b>	Transfer of a potentially internal business function to an external service provider.
<b>PBX</b>	Private Branch Exchange – a telecommunications switching system, usually physically located at a customer's place of business, providing internal communication between users and access to outside (trunk) telephone lines.
<b>PHOTODETECTOR</b>	Any device used to detect electromagnetic radiation.
<b>PROGRAMMABLE LOGIC ARRAY</b>	Programmable devices used to implement combinational logic circuits.
<b>RENMINBI (RMB)</b>	The renminbi is the official physical currency of the People's Republic of China, whose principal unit of account is the yuan ("¥" or "CNY"). The currency is legal tender in mainland China but not in Hong Kong and Macau. Renminbi translates as people's currency. The renminbi is issued by the People's Bank of China, the monetary authority of the PRC. In practice, use of "renminbi" is analogous to the use of "sterling" within the United Kingdom, where sterling is the actual physical currency but the Pound is the official unit of account by which sterling are denominated.
<b>REPEATER</b>	An electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances.
<b>RFC</b>	Request for Comments, an IETF (Internet Engineering Task Force) memorandum on Internet systems and standards.
<b>ROOTKIT</b>	Software used by a second or third party after gaining access to a computer system in order to conceal alteration of files, file systems, or processes without the user's knowledge.
<b>ROUTER</b>	Telecommunications devices that direct packets of information using OSI layer 3 (network layer) information. Also describes Internet devices that connect local area networks to form larger Internets.
<b>SAFE</b>	The State Administration of Foreign Exchange (SAFE), a Chinese government body that manages China's foreign exchange reserves. <a href="http://www.safe.gov.cn">http://www.safe.gov.cn</a> .
<b>SERVICE FOOTPRINT</b>	An area of services coverage. Typically, the geographic area within which a service may be provided.
<b>SMART PHONES</b>	Mobile phones that offer more advanced computing abilities and connectivity than basic "feature phones." Some feature phones are able to run simple applications based on generic platforms such as Java; smart phones allow much more advanced applications. Smart phones run complete operating systems and provide platforms for application developers. They may be considered handheld computers with mobile telephone capabilities.

<b>SMS</b>	Short Message Service is the text communication service component of mobile communication systems. Standard communications protocols allow the exchange of SMS messages between mobile phone devices.
<b>SPYWARE</b>	Malware intended to be installed on a user's system to surreptitiously collect incremental information about users.
<b>SRAM</b>	Static Random Access Memory – semiconductor memory where, unlike dynamic RAM (DRAM), it does not need to be periodically refreshed. SRAM uses bistable latching circuitry to store each bit.
<b>STRUCTURED ASIC</b>	Structured ASIC design (also “Platform ASIC”) has a variety of contextual meanings. The basic premise infers that both manufacturing cycle time and design cycle time are reduced compared to cell-based ASIC. Predefined metal layers reduce manufacturing time, and precharacterization of what is on the silicon reduces design cycle time.
<b>SUPPLY CHAIN</b>	Systems of organizations, people, technology, activities, information, and resources involved in moving products or services from suppliers to customers/users.
<b>SWITCHES</b>	Network switches are computer networking devices that connect network segments. The term commonly refers to network bridges that process and route data at data link layers (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches. The term network switch does not generally encompass unintelligent or passive network devices such as hubs and repeaters.
<b>TIME DIVISION</b>	Digital or analog multiplexing in which two or more signals or bit-streams are transferred simultaneously as subchannels in one communication channel while physically taking turns on the channel.
<b>TROJAN</b>	Non-self-replicating malware that appears to perform desirable functions for users but instead facilitates unauthorized access to user computer systems.
<b>USB</b>	Universal Serial Bus – a “serial bus” standard for connecting devices.
<b>UV</b>	Ultraviolet.
<b>WAN</b>	Wide Area Network – computer networks covering large geographic areas and that can refer to several buildings in a city or several cities. A WAN can also refer to a group of LANs connected by dedicated long-distance links.
<b>WCDMA</b>	Wideband Code Division Multiple Access, UMTS-FDD, UTRA-FDD, or IMT-2000 CDMA Direct Spread – a wireless interface standard in 3G mobile telecommunications networks.
<b>WiFi</b>	A wireless local area network model based on the IEEE 802.11 standards and the most widely used WLAN technology today.
<b>WiMAX</b>	Worldwide Interoperability for Microwave Access – a telecommunications technology providing wireless data, voice, and video over long distances. Currently provides fixed and fully mobile Internet access up to 40 Mbit/s based on the IEEE 802.16 standard and is expected to offer up to 1 Gbit/s fixed speeds with the IEEE 802.16m update.
<b>WIRELESS CHARGING</b>	Inductive Charging – a technology using the electromagnetic fields to transfer energy between objects.
<b>WORM</b>	Self-replicating malware computer programs that use computer networks to (potentially) automatically, autonomously, and/or surreptitiously send copies of themselves to other nodes/systems.
<b>YUÁN</b>	A cause of some confusion, a “yuan” (“元” or “CNY”) is the base unit of a number of modern Chinese currencies. Distinction between the yuan and a renminbi (a name also used for the Chinese currency) can be viewed as analogous to that between the pound and sterling in Great Britain. The yuan is the unit of account, and a renminbi is the actual physical scrip or change of currency. The symbol for the yuan “元” may also be used in some circumstances to refer to the currency units of Japan and Korea and also to

	translate the currency unit of a dollar relative to yuan. The U.S. dollar is called Měiyuán or American yuan, in Chinese. When used in English in the context of the modern foreign exchange market, the Chinese yuan most commonly refers to the renminbi but may be indicated by the simple symbol of a yuan (CNY).
<b>ZERO-DAY</b>	Zero-day (or zero-hour or day-zero) attacks or threats are attempts to exploit system or application vulnerabilities that are currently (at the time of attack) unknown or undisclosed to software developers and users.

## APPENDIX C

### PARTIAL BIBLIOGRAPHY

- "Asia Private Equity Review," April 2006. Reprinted in China C SR.com, May 27, 2008.
- Adee, Sally. "The Hunt for the Kill Switch." *IEEE Spectrum*, May 2008. <http://www.spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>.
- Agence France-Presse, "China cements role as top creditor to US: Treasury," March 17, 2009. <http://www.google.com/hostednews/afp/article/ALeqM5hqDfBfaypzFV7bvJ1j3vkN0qW8A9>.
- Alcatel Alenia Press Release. "Alcatel Alenia Space Wins New Communication and Broadcast Satellite Contract Chinastat 6B From ChinaSatcom, Bolstering Cooperation With China." Available at Red Orbit.com. December 5, 2005,. [http://www.redorbit.com/news/space/1838943/esa\\_and\\_thales\\_alenia\\_space\\_enter\\_negotiations\\_for\\_mtg/index.html](http://www.redorbit.com/news/space/1838943/esa_and_thales_alenia_space_enter_negotiations_for_mtg/index.html).
- AllBusiness.Com. "Qualcomm, China TechFaith Create Wireless Company." March 27, 2009.
- *Asia Times*, "China's trillion-dollar kitty is ready," October 2, 2007. [http://www.atimes.com/atimes/China\\_Business/IJ02Cb01.html](http://www.atimes.com/atimes/China_Business/IJ02Cb01.html).
- *Asia Times*, "3G is Key to a Foreign Telecom Role in China," December 6, 2006. [http://www.atimes.com/atimes/China\\_Business/HL06Cb02.html](http://www.atimes.com/atimes/China_Business/HL06Cb02.html).
- Bhagat, Sanjai. *Reforming Executive Compensation: Focusing and Committing to the Long-term*. New Haven, CT: Yale Law School, February 2009. [http://www.law.yale.edu/documents/pdf/cbl/Bhagat\\_Romano\\_Reforming\\_Executive.pdf](http://www.law.yale.edu/documents/pdf/cbl/Bhagat_Romano_Reforming_Executive.pdf).
- Blakely, Rhys, et al. "MI5 Alert on China's Cyberspace Spy Threat." *Times* (London), December 1, 2007. [http://business.timesonline.co.uk/tol/business/industry\\_sectors/technology/article2980250.ece](http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece).
- Bliss, Jeff. "China's Spying Overwhelms U.S. Counterintelligence." Bloomberg.com. April 2, 2007. <http://www.bloomberg.com/apps/news?pid=20601087&sid=ab2PiDI1qW9Q&refer=home>.
- *Bloomberg Businessweek*. Huawei Confirms Plans for Handset Division Sale. June 10, 2008. [http://www.businessweek.com/globalbiz/content/jun2008/gb20080619\\_118434.htm?campaign\\_id=rss\\_as](http://www.businessweek.com/globalbiz/content/jun2008/gb20080619_118434.htm?campaign_id=rss_as).
- Bounds, Jeff. "Huawei to Add Hundreds of Tech Jobs." *Texas Business Journal* (May 1, 2009). <http://dallas.bizjournals.com/dallas/stories/2009/05/04/story15.html>.
- Brown, Paul B. "Trojan Horse on a Chip." *New York Times*, April 5, 2008. <http://www.nytimes.com/2008/04/05/business/05offline.html>.
- C114.net. "Alcatel Lucent chases profits, three years on." January 6, 2010. <http://www.cn-c114.net/583/a473644.html>.
- *Caijing China*, "The 3Com Deal, Behind the Security Flap," October 23, 2007. <http://www.cn-c114.net/582/a314041.html>.
- Carew, Rick. "China Seeks External Help for Wealth Fund." *Wall Street Journal*, December 14, 2007. <http://online.wsj.com/article/SB119759666432928557.html>.
- Carew, Rick. "Great Wall Street of China." *Wall Street Journal*, December 20, 2007. <http://online.wsj.com/article/SB119805649734239175.html>.

- Carnegie Endowment for International Peace. "China Mainland." Commentary and Analysis. 2010.  
<http://www.carnegieendowment.org/regions/?fa=viewRegions&region=1000185>.
- Carnegie Endowment for International Peace. "Chinese Economy." Commentary and Analysis. 2010.  
<http://www.carnegieendowment.org/topic/?fa=viewTopic&topic=3000164>.
- Carnegie Mellon University. "Denial of Service Attacks." Pittsburgh, PA: CERT Coordination Center, Software Engineering Institute, June 4, 2001 (updated).  
[http://www.cert.org/tech\\_tips/denial\\_of\\_service.html](http://www.cert.org/tech_tips/denial_of_service.html).
- Cellular-News. "Huawei Taps Former Nortel Exec to European Job," July 13, 2009.  
<http://www.cellular-news.com/story/38491.php>.
- Chang, Maria Hsia. "China Policy of Engagement Needs an Overhaul." *San Francisco Chronicle*, June 7, 1999, p. A23. [http://articles.sfgate.com/1999-06-07/opinion/17692104\\_1\\_senkaku-china-last-summer-diaoyu](http://articles.sfgate.com/1999-06-07/opinion/17692104_1_senkaku-china-last-summer-diaoyu).
- Cheng, Dean. "PLA Views on Space: The Prerequisite for Information Dominance." Alexandria, VA: Center for Naval Analysis, October 2007.  
<http://www.cna.org/documents/5.pdf>.
- *China Daily*, "China's telecoms sector gets 3G licenses," January 7, 2009.  
[http://www.chinadaily.com.cn/bizchina/2009-01/07/content\\_7375721.htm](http://www.chinadaily.com.cn/bizchina/2009-01/07/content_7375721.htm).
- *China Daily*, "China Finally Awards Telecom Operators 3G Wireless," January 7, 2009.  
[http://www.chinadaily.com.cn/bizchina/2009-01/07/content\\_7374321.htm](http://www.chinadaily.com.cn/bizchina/2009-01/07/content_7374321.htm).
- *China Daily*, "Huawei Puts Terminal Unit Sale on Hold," October 10, 2008.  
[http://www.chinadaily.com.cn/business/2008-10/10/content\\_7094113.htm](http://www.chinadaily.com.cn/business/2008-10/10/content_7094113.htm).
- ChinaTechNews.com. "Indian Government Bans Import of Chinese Telecom Equipment." April 30, 2010. <http://www.chinatechnews.com/2010/04/30/11981-indian-government-bans-import-of-chinese-telecom-equipment>.
- ChinaTechNews.com. "Pakistan Welcomes More Chinese Telecom Investment." February 18, 2009. <http://www.chinatechnews.com/2009/02/18/8855-pakistan-welcomes-more-chinese-telecom-investment>.
- Christensen, Thomas J. "Windows and War: Trend Analysis and Beijing's Use of Force." In *New Directions in the Study of China's Foreign Policy*. Edited by Alastair Iain Johnston and Robert Ross. Palo Alto, CA: Stanford University Press, 2006.  
<http://www.sup.org/book.cgi?id=9777>.
- Coleman, Kevin. "Private Sector-Military Collaboration Vital To Confront Cyber Threats." *Defense Tech*. April 19, 2010. <http://defensetech.org/2010/04/19/private-sector-military-collaboration-vital-to-confront-cyber-threats/#ixzz0oBCGbUKY>.
- Collingridge, David. *The Social Control of Technology*. New York, NY: St. Martin's Press, 1980.
- Cowen Latitude. *Technology and Telecom Sector M&A Report 1<sup>st</sup> Quarter 2009*.  
[http://www.cowenlatitude.com/document/09q1\\_china\\_tech\\_ma.pdf](http://www.cowenlatitude.com/document/09q1_china_tech_ma.pdf).
- CSC Staff. "Krugman in China: Stimulating, Controversial, and Expensive." *ChinaStakes* (Shanghai), May 16, 2009. ChinaStakes.com  
<http://www.chinastakes.com/2009/5/krugman-in-china-stimulating-controversial-and-expensive.html>.
- Dalrymple, Jim. "Apple Fixes iPhone SMS Flaw." *CNet.com*. July 31, 2009,  
[http://news.cnet.com/8301-1009\\_3-10301001-83.html](http://news.cnet.com/8301-1009_3-10301001-83.html).
- Dambala, Inc. "The Command Structure of the Aurora Botnet, History, Patterns and Findings." March 3, 2010.  
[http://www.damballa.com/downloads/r\\_pubs/Aurora\\_Botnet\\_Command\\_Structure.pdf](http://www.damballa.com/downloads/r_pubs/Aurora_Botnet_Command_Structure.pdf).



- Del Oro Group Press Release. "Chinese Vendors Huawei and ZTE Gain Ground on Leaders Ericsson and Nokia Siemens." April 26, 2010.  
<http://www.delloro.com/news/2010/WPC042610.htm>.
- Derene, Glenn, and Joan Pappalardo. "Counterfeit Chips Raise Big Hacking, Terror Threats, Experts Say." *Popular Mechanics*, October 1, 2009.  
<http://www.popularmechanics.com/technology/gadgets/news/4253628>.
- DeWeese, Steve, et al. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. Northrop Grumman Corporation for the U.S.-China Economic and Security Review Commission, October 16, 2009.  
[http://www.uscc.gov/researchpapers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper\\_FINAL\\_Approved%20Report\\_16Oct2009.pdf](http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf).
- Dezan Shira & Associates. *Made in USA: China and India Invest Abroad*. May 13, 2010.  
<http://www.2point6billion.com/news/2010/05/13/made-in-usa-china-and-india-invest-abroad-5645.html>.
- Edgerton, David. *The Shock of the Old: Technology and Global History Since 1900*. New York: Oxford University Press, 2006.  
<http://www.oup.com/us/catalog/general/subject/HistoryOther/HistoryofTechnology/?view=usa&ci=9780195322835>.
- Einhorn, Bruce. Huawei's 3Com Deal Flops. *Business Week*, February 21, 2008.  
[http://www.businessweek.com/globalbiz/blog/eyeonasia/archives/2008/02/huaweis\\_3com\\_deal\\_flops.html](http://www.businessweek.com/globalbiz/blog/eyeonasia/archives/2008/02/huaweis_3com_deal_flops.html).
- Elgan, Mike. "Is China Cyber-Stealing Your Secrets?" *Datamation*, September 17, 2009.  
<http://itmanagement.earthweb.com/secu/article.php/3839541/Is-China-Cyber-Stealing-Your-Secrets.htm>.
- Enck, William, et al. *Exploiting Open Functionality in SMS-Capable Cellular Networks*. University Park, PA: Pennsylvania State University, September 2, 2005.  
<http://www.smsanalysis.org/smsanalysis.pdf>.
- Engels, Daniel W., et al. "Improving Visibility in the DOD Supply Chain." June 2004.  
[http://www.almc.army.mil/alog/issues/mayJun04/alog\\_supple%20chain.htm](http://www.almc.army.mil/alog/issues/mayJun04/alog_supple%20chain.htm).
- Engineering Trends.com. "What is Happening To Computer Science and Engineering?" Report 1005E, October 2005. <http://www.engtrends.com/IEE/1005E.php>.
- Fallows, James. The \$1.4 Trillion Question, The Chinese are subsidizing the American way of life. Are we playing them for suckers—or are they playing us? *Atlantic* (January/February 2008). <http://www.theatlantic.com/doc/200801/fallows-chinese-dollars/4>.
- Fallows, James. The \$1.4 Trillion Dollar Question. *Atlantic Monthly*, January/February 2008. <http://www.theatlantic.com/doc/200801/fallows-chinese-dollars>.
- *Federal Communications Law Journal*. June 6, 2005.
- Fierce Wireless; Huawei Website. "Huawei to deploy CDMA 2000 infrastructure for Cricket Communications." July 11, 2007.  
<http://www.huawei.com/news/view.do?id=4445&cid=42>.
- Fisher, Richard Jr. *People's Liberation Army Leverage of Foreign Military Technology*. Alexandria, VA: International Assessment and Strategy Center, March 22, 2006.  
[http://www.strategycenter.net/research/pubID.97/pub\\_detail.asp](http://www.strategycenter.net/research/pubID.97/pub_detail.asp).
- *Forbes*. Huawei Buys Back Into 3Com. October 1, 2007.  
<http://www.forbes.com/2009/03/27/huawei-security-clearwire-technology-enterprise-tech-huawei.html>.
- Fox News. "Experts: Zombie Cell-Phone Hack Attacks May Be Next." October 16, 2008.  
<http://www.foxnews.com/story/0,2933,438481,00.html>.
- Gasper, Peter D. "Cyber Threat to Critical Infrastructure - 2010-2015." Paper presented at the Idaho National Laboratory, "Information & Cyberspace Symposium, Fort



Leavenworth, KS., September 22-24, 2008.

[http://usacac.army.mil/cac2/cew/repository/papers/Cyber Threat to CI.PDF](http://usacac.army.mil/cac2/cew/repository/papers/Cyber%20Threat%20to%20CI.PDF).

- Global Crossing Press Release. "Global Crossing to Acquire Global Marine Subsidiary of Cable and Wireless." April 26, 1999; and Funding Universe. Global Crossing backgrounder. 10Ks and Annual Report Data.
  - Goetz, John, and Marcel Rosenbach. "Cyber Spies: 'GhostNet' and the New World of Espionage." *Der Spiegel* online, April 10, 2009.  
<http://www.spiegel.de/international/world/0,1518,618478,00.html>.
  - Goodall, Randy. "External Programs: Briefing to the Defense Science Board Task Force on High-performance Microchip Supply." June 23, 2004.  
<http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.
  - Goodchild, Joan. "3 Simple Steps to Hack a Cell Phone." CSOnline.com. April 29, 2009.  
[http://www.csoonline.com/article/491200/ Simple Steps to Hack a Smartphone Includes Video](http://www.csoonline.com/article/491200/Simple%20Steps%20to%20Hack%20a%20Smartphone%20Includes%20Video).
  - Goodchild, Joan. "CISCO: SMS Smartphone Attacks on the Rise." CSOnline.com. July 14, 2009.  
[http://www.csoonline.com/article/497120/Cisco SMS Smartphone Attacks on the Rise](http://www.csoonline.com/article/497120/Cisco%20SMS%20Smartphone%20Attacks%20on%20the%20Rise).
  - Gorman, S.P. *Networks, security and complexity: the role of public policy in critical infrastructure protection*. Cheltenham, England: Edward Elgar Publishing, 2005.
  - Greenberg, Andy. "The Deal that Could Have Saved Nortel." *Forbes*, January 14, 2009.  
[http://www.forbes.com/2009/01/14/nortel-huawei-china-tech-wire-cx\\_ag\\_0114nortel.html](http://www.forbes.com/2009/01/14/nortel-huawei-china-tech-wire-cx_ag_0114nortel.html).
  - Greenberg, Andy. Nortel's China Syndrome. *Forbes*, January 12, 2009.  
[http://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx\\_ag\\_0112nortel.html](http://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx_ag_0112nortel.html).
  - Greenberg, Andy. "Nortel's China Syndrome, Concerns over Chinese cyber-spying may have stalled a deal with Huawei that Nortel needs." *Forbes*.com. January 12, 2009.  
[http://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx\\_ag\\_0112nortel.html](http://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx_ag_0112nortel.html).
  - Greenberg, Andy. Huawei's U.S. coming out Party. *Forbes*, March 27, 2009.  
<http://www.forbes.com/2009/03/27/huawei-security-clearwire-technology-enterprise-tech-huawei.html>.
  - Grow, Brian, et al. The New E-spying Threat. *BusinessWeek*, April 10, 2008.  
[http://www.businessweek.com/magazine/content/08\\_16/b4080032218430.htm](http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm).
  - Harris, Shane. "China's Cyber-Militia." *National Journal*, May 31, 2008.  
[http://www.nationaljournal.com/njmagazine/cs\\_20080531\\_6948.php](http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php).
  - Hewlett Packard Press Release. "H.P. to Acquire 3Com for \$2.7 billion." November 11, 2009. <http://www.hp.com/hpinfo/newsroom/press/2009/091111xa.html>.
  - Hobsbawm, Eric. *The Age of Revolution: Europe 1789–1848*. London: Weidenfeld & Nicolson Ltd., 1996 (paperback).
  - House Armed Services Committee. Subcommittee on Terrorism, Unconventional Threats, and Capabilities. *Information Technology*. Statement by Michael E. Krieger. 111th Cong., 2nd sess., May 5, 2009.
  - House Committee on Homeland Security. Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. "Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action." Testimony of O. Sami Saydjari. 110th Cong., 1st sess., April 25, 2007.  
<http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf>.
- <http://nobelprize.org/educational/economics/trade/ohlin.html>.

- Hutchison Whampoa Limited Press Release. "Hutchison Whampoa and Global Crossing complete telecom joint Venture in Hong Kong." January 12, 2000. [http://www.hutchison-whampoa.com/eng/media/press\\_releases/press\\_releases.htm?category=Corporate&fye\\_ar=&show=all](http://www.hutchison-whampoa.com/eng/media/press_releases/press_releases.htm?category=Corporate&fye_ar=&show=all).
- InformationWeek. FCC Approves Sprint Clearwire Merger, National WiMAX Coming. November 5, 2008. <http://www.informationweek.com/news/telecom/business/showArticle.jhtml?articleID=212000757>.
- InfoTech News. Research and Markets: Gigabit Ethernet Fiber and Copper Cabling Systems.TMCNET.com. April 15, 2010. <http://it.tmcnet.com/news/2010/04/15/4731374.htm>.
- Jackson, David. "China Mobile - Millicom Deal Threatens Ericsson, Nokia, Lucent, Motorola, Qualcomm." Seekingalpha.com. May 25, 2006. <http://seekingalpha.com/article/11224-china-mobile-millicom-deal-threatens-ericsson-nokia-lucent-motorola-qualcom>.
- Jenkins, Holman W. Jr. "China, Google and the Cloud Wars, Your personal data still aren't safe." *Wall Street Journal*, January 22, 2010. <http://online.wsj.com/article/SB10001424052748703699204575016801501346056.html>.
- Jie, Liu. "Curbing overcapacity, stimulating consumption key for China's economic revival." Xinhua, January 7, 2010. Chinaview.cn, [http://news.xinhuanet.com/english/2010-01/07/content\\_12771682.htm](http://news.xinhuanet.com/english/2010-01/07/content_12771682.htm).
- Kanwal, Gurmeet. "China's Emerging Cyber War Doctrine." *Journal of Defence Studies* Vol. 3, No 3 (July 2009). [http://www.idsa.in/system/files/jds\\_3\\_3\\_gkanwal\\_0.pdf](http://www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf).
- Kou, Kaiser. "China's 4G Master Plan." February 26, 2008. <http://digitalwatch.ogilvy.com.cn/en/?p=205>.
- Kravets, David. "iPhone Jailbreaking Could Crash Cellphone Towers, Apple Claims." *Wired*, July 28, 2009. <http://www.wired.com/threatlevel/2009/07/jailbreak/>.
- Kwok, Vivian Wai-yin. "China Investment Corp. Flashes its Yuan." *Forbes.com*, May 5, 2007. [http://www.forbes.com/2007/10/05/china-investment-fund-markets-equity-cx\\_vk\\_1005markets03.html](http://www.forbes.com/2007/10/05/china-investment-fund-markets-equity-cx_vk_1005markets03.html).
- Lewis, James A., et al. *Securing Cyberspace for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, CSIS Commission on Cybersecurity for the 44th Presidency, December 8, 2008. <http://csis.org/publication/securing-cyberspace-44th-presidency>.
- Light Reading Mobile. "Clearwire Confirms Huawei Deal." August 11, 2009. [http://www.lightreading.com/document.asp?doc\\_id=180326](http://www.lightreading.com/document.asp?doc_id=180326).
- Light Reading; Cable Digital News. "Cox, Huawei Make Wireless Connection." March 30, 2009. [http://www.lightreading.com/document.asp?doc\\_id=174434&site=lr\\_cable](http://www.lightreading.com/document.asp?doc_id=174434&site=lr_cable).
- LightReading. "Huawei Supplies Leap Wireless." August 15, 2006. [http://www.lightreading.com/document.asp?doc\\_id=101446](http://www.lightreading.com/document.asp?doc_id=101446).
- Manji, Firoze, and Stephen Marks. "African Perspectives on China in Africa." Fahamu-- Networks for Social Justice. 2007.
- Manye, Kevin. "The New Face of IBM" - "China's biggest IT brand wants to go global. So it bought the PC division - and the world-class management - of an American icon. Who says being "oceans apart" is a bad thing?" *Wired.com*, July 2005. <http://www.wired.com/wired/archive/13.07/lenovo.html>.
- MarketWatch Inc. "Taiwan stocks on fire on China Mobile-Far EasTone." April 29, 2009. <http://www.marketwatch.com/story/china-mobiles-taiwan-plan-could-change-everything>.
- Markoff, John, and David Barboza. "Academic Paper in China Sets Off Alarms in U.S." *New York Times*, March 20, 2010. <http://www.nytimes.com/2010/03/21/world/asia/21grid.html>.

- Markoff, John. "Before the Gunfire, Cyberattacks." *New York Times*, August 12, 2008. <http://www.nytimes.com/2008/08/13/technology/13cyber.html?ref=world>.
- Marquand, Robert, and Ben Arnoldy. "China Emerges as Leader in Cyberwarfare." *Christian Science Monitor*, September 14, 2007. <http://www.csmonitor.com/2007/0914/p01s01-woap.html>.
- Marsan, Carolyn Duffy. Invisible IPv6 Traffic Poses Serious Network Threat. *Network World*, July 13, 2009. <http://www.networkworld.com/news/2009/071309-roque-ipv6.html>.
- Martin, Michael F. China's Sovereign Wealth Fund. *Sovereign Wealth Fund News*, January 22, 2008. <http://www.sovereignwealthfundnews.com/safe.php>. Also, Congressional Reporting Service. <http://www.fas.org/sqp/crs/row/RL34337.pdf>.
- *Mass High Tech: The Journal of New England Technology*. "Bain Bids on Huawei Mobile Handsets." September 30, 2008. <http://www.masshightech.com/stories/2008/09/29/daily17-Bain-bids-on-Huawei-mobile-handsets.html>.
- McKee, Michael, and Alex Nicholson. "Paulson Says Russia Urged China to Dump Fannie, Freddie Bonds." *Bloomberg.com*, January 29, 2009. <http://www.bloomberg.com/apps/news?pid=newsarchive&sid=afbSjYv3v814#>.
- McMillan, Robert. "Some SMS Networks Vulnerable to Attack." July 28, 2009. [http://tech.yahoo.com/news/pcworld/20090729/tc\\_pcworld/somesmsnetworksvulnerabletoattack](http://tech.yahoo.com/news/pcworld/20090729/tc_pcworld/somesmsnetworksvulnerabletoattack).
- Meredith, Robyn. Panda-ring To China? - The unwelcome sea change in U.S.-China business relations. *Forbes*, March 2, 2010. <http://www.forbes.com/2010/02/02/china-fedex-panda-diplomacy-opinions-columnists-robyn-meredith.html>.
- Meyer, David. "TeliaSonera touts first LTE '4G' launch." *CNET News.com*. December 14, 2009. ([http://news.cnet.com/8301-1035\\_3-10414665-94.html](http://news.cnet.com/8301-1035_3-10414665-94.html))
- Miller, Sandra Kay. "Hacking at the Speed of Light." *Securitysolutions.com*. April 1, 2006.
- Mills, Elinor. "Researchers take control of iPhone via SMS." *ZDNet.com*. July 30, 2009. ([http://news.zdnet.com/2100-9595\\_22-326501.html](http://news.zdnet.com/2100-9595_22-326501.html))
- Mills, Elinor. "SMS Messages Could Be Used to Hijack a Phone." *CNet.com*. April 19, 2009. [http://news.cnet.com/8301-1009\\_3-10222921-83.html](http://news.cnet.com/8301-1009_3-10222921-83.html).
- Mobile Monday.Net. "UT Starcom Buys 3Com's Operator Assets." March 5, 2003. [http://www.lightreading.com/document.asp?doc\\_id=29233](http://www.lightreading.com/document.asp?doc_id=29233).
- Moore, Malcolm. "China's Global Cyber-Espionage Network GhostNet Penetrates 103 Countries." *Telegraph.co.uk*. March 29, 2009. <http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-globalcyber-espionage-network-GhostNet-penetrates-103-countries.html>.
- Morrison, Wayne, and Marc Labonte. "China's Holdings of U.S. Securities: Implications for the U.S. Economy." Congressional Reporting Service, CRS-7, January 9, 2008. <http://opencrs.com/document/RL34314/>.
- Mulvenon, James. "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability." In *Beyond the Strait: PLA Missions Other Than Taiwan*. Edited by Roy Kamphausen, David Lai, and Andrew Scobell, Carlisle, PA: Strategic Studies Institute, April 2009. <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB910.pdf>.
- *New York Times*, "Silverlake Eyes Asia Tech Investments," November 28, 2008. <http://dealbook.blogs.nytimes.com/2008/11/25/silver-lake-eyes-asia-tech-investments/>.
- *New York Times*, "U.S. Opens Inquiry in Plan to Sell Global Crossing to Asians," April 4, 2003. <http://www.nytimes.com/2003/04/30/business/us-opens-inquiry-in-plan-to-sell-global-crossing-to-asians.html>.

- *New Zealand Herald*, "China's technological challenger," March 15, 2007. [http://www.nzherald.co.nz/telecommunications/news/article.cfm?c\\_id=93&objectid=10428813](http://www.nzherald.co.nz/telecommunications/news/article.cfm?c_id=93&objectid=10428813).
- Newman, Bill. "Up to Bat Again – Will it be Strike Two for Huawei in the U.S.?" Inbound Acquisitions and Investments Blog, quoting *Financial Times*, April 16, 2010. <http://www.usainbounddeals.com/2010/04/articles/deals-developments/up-to-bat-again-will-it-be-strike-two-for-huawei-in-the-united-states/>.
- Ngo, Dong. "Jailbreaking iPhone could pose threat to national security, Apple claims." CNet.com. July 29, 2009. [http://reviews.cnet.com/8301-19512\\_7-10298646-233.html](http://reviews.cnet.com/8301-19512_7-10298646-233.html).
- Nortel.com. "Nortel Obtains Court Orders for Creditor Protection." January 14, 2009. [http://www2.nortel.com/go/news\\_detail.jsp?cat\\_id=-8055&oid=100251347&locale=en-US](http://www2.nortel.com/go/news_detail.jsp?cat_id=-8055&oid=100251347&locale=en-US).
- Nobelprize.org. "Why Trade?" Nobelprize.org. February 28, 2006.
- Nortel.com. "Nortel, Huawei to Establish Joint Venture to Address Broadband Access Market." "Plan to Jointly Develop Ultra Broadband Products for Delivery of Converged Services." February 1, 2006. [http://www2.nortel.com/go/news\\_detail.jsp?cat\\_id=-8055&oid=100194923](http://www2.nortel.com/go/news_detail.jsp?cat_id=-8055&oid=100194923).
- NPR.org. "Chinese Telecom Companies Look to Global Markets." August 16, 2005. <http://www.npr.org/templates/story/story.php?storyId=4801437>.
- Nystedt, Dan. China Mobile Wins Approval for Taiwan Subsidiary. *PCWorld*, May 11, 2010. [http://www.pcworld.com/article/196019/china\\_mobile\\_wins\\_approval\\_for\\_taiwan\\_subsidary.html](http://www.pcworld.com/article/196019/china_mobile_wins_approval_for_taiwan_subsidary.html).
- Orey, Michael. Patent Filings Surge in China. *Bloomberg Businessweek*, June 3, 2008. [http://www.businessweek.com/bwdaily/dnflash/content/jun2008/db2008063\\_332712.htm?chan=top+news\\_top+news+index\\_technology](http://www.businessweek.com/bwdaily/dnflash/content/jun2008/db2008063_332712.htm?chan=top+news_top+news+index_technology).
- Pei, Minxin. The Dark Side of China's Rise. *Foreign Policy* (March/April 2006). Reprinted in Carnegie Endowment for International Peace publication. <http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=18110&prog=zch>.
- Pei, Minxin. The Real Lessons from the Google-China Spat. In *The Diplomat*. Washington, DC: Carnegie Endowment for International Peace, February 3, 2010. <http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=24801>.
- Peilin, Li, and Zhangyi. "Consumption Stratification In China: An Important Tool In Stirring Up Economy." Chinese Academy of Social Science (2008). <http://www.sociology.cass.cn/english/papers/P020080715377553596141.pdf>.
- Prasso, Sheridan. American made...Chinese owned: Full version. CNNMoney.com. *Fortune*, May 7, 2010. [http://money.cnn.com/2010/05/06/news/international/china\\_america\\_full.fortune](http://money.cnn.com/2010/05/06/news/international/china_america_full.fortune).
- Price, Ray. "Briefing to the Defense Science Board Task Force on High-Performance Microchip Supply." May 20, 2004. <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.
- Rautu, Ovidiu. "Nokia Siemens Partners with Huawei - The agreement covers worldwide use of all standards essential patents of all parties." SoftPedia/Telecoms. September 29, 2008. <http://news.softpedia.com/news/Nokia-Siemens-Partners-With-Huawei-94374.shtm>.
- RCR Wireless. "Huawei's Aggressive Push Pays Off." September 24, 2008. <http://www.rcrwireless.com/ARTICLE/20080924/WIRELESS/809239966/huawei-146-s-aggressive-push-pays-off>.
- Reed Smith LLP. "New Amendment Rationalizes Country-of-Origin Preferences for Defense and Civilian Acquisitions." Client Bulletin 03-03, January 2003. <http://www.reedsmith.com/db/documents/bull0303.pdf>.



- Reuters, "Opposition Leads Bain to Call Off 3Com Deal," March 21, 2008.  
<http://www.nytimes.com/2008/03/21/technology/21com.html>.
- Reuters, "Russia's MTS picks Huawei for 3G Armenia Network," January 16, 2009.  
<http://www.reuters.com/article/idUSLG46594520090116>.
- Rogin, Josh. The top 10 Chinese cyber attacks (that we know of). *Foreign Policy* online. January 22, 2010.  
[http://thecable.foreignpolicy.com/posts/2010/01/22/the\\_top\\_10\\_chinese\\_cyber\\_attacks\\_that\\_we\\_know\\_of](http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of).
- Schwankert, Steven. "US Congressmen Accuse China of Hacking Their Computers." Infoworld.com. IDG Network. June 12, 2008.  
<http://www.infoworld.com/archive/200806?page=46>.
- ScienceDaily LLC. "Stealth Attack Drains Cell Phone Batteries." August 30, 2006.  
<http://www.sciencedaily.com/releases/2006/08/060829090243.htm>.
- Scissors, Derek. *Chinese Foreign Investment: How Much and Where?* Business Forum China and The Heritage Foundation, August 11, 2009.  
<http://www.heritage.org/Research/Commentary/2009/08/Chinese-Foreign-Investment-How-Much-and-Where>.
- Scissors, Derek. "U.S.–China Strategic and Economic Dialogue: America Must Lead by Example." Washington, DC: The Heritage Foundation, May 24, 2010.  
<http://www.heritage.org/Research/Reports/2010/05/US-China-Strategic-and-Economic-Dialogue-America-Must-Lead-by-Example>.
- Sevastopulo, Demetri. "Hackers Breach White House System." *Financial Times*, November 6, 2008.  
[http://us.ft.com/ftgateway/superpage.ft?news\\_id=fto110620081938360726&page=2](http://us.ft.com/ftgateway/superpage.ft?news_id=fto110620081938360726&page=2).
- Shachtman, Noah. "Activists Launch Hack Attacks on Tehran Regime." *Wired*, June 15, 2009. <http://www.wired.com/dangerroom/2009/06/activists-launch-hack-attacks-on-tehran-regime/>.
- Shankar, Vivek, and Amy Thomson. "3Com Agrees to \$2.2 Billion Takeover Offer From Bain (Update4)." Bloomberg.com, September 28, 2007.  
<http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aC5FJiGpl5lq&refer=us>.
- Singer, Jason, and Jason Dean. "China Mobile Nears \$5.3 Billion Deal For Millicom Beijing's Biggest Purchase Overseas Would Intensify Push Into Emerging Markets." *China Daily*, May 25, 2006. [http://www.chinadaily.com.cn/world/2006-05/25/content\\_600127.htm](http://www.chinadaily.com.cn/world/2006-05/25/content_600127.htm).
- Singer, Jason, and Jason Dean. "China Mobile Nears \$5.3 Billion Deal For Millicom Beijing's Biggest Purchase Overseas Would Intensify Push Into Emerging Markets." *China Daily*, May 25, 2006. [http://www.chinadaily.com.cn/world/2006-05/25/content\\_600127.htm](http://www.chinadaily.com.cn/world/2006-05/25/content_600127.htm).
- Smith, Michael. "Spy chiefs fear Chinese cyber attack." *Sunday Times (London)*, March 29, 2009. <http://www.timesonline.co.uk/tol/news/uk/article5993156.ece>.
- Softpedia.com. "Nokia Siemens Partners with Huawei." September 29, 2008.  
<http://news.softpedia.com/news/Nokia-Siemens-Partners-With-Huawei-94374.shtml>.
- Spillius, Alex. "Cyber attack 'could fell US within 15 minutes'." *Telegraph (UK)*, May 7, 2010. <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7691500/Cyber-attack-could-fell-US-within-15-minutes.html>.
- Stokes, Mark A. *China's Strategic Modernization: Implications for the United States*. Carlisle, PA: Strategic Studies Institute, September 1, 1999.  
<http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=74>.
- Strasburg, Jenny, and Rick Carew. "China Ready to Place Bets on Hedge Funds." *Wall Street Journal*, June 19, 2009.  
<http://online.wsj.com/article/SB124535652071428705.html>.

- Strazheim, Donald. China Buys Wall Street. Forbes.com, December 27, 2007. [http://www.forbes.com/2008/12/26/straszheim-china-cic-oped-cx\\_dhs\\_1227straszheim.html](http://www.forbes.com/2008/12/26/straszheim-china-cic-oped-cx_dhs_1227straszheim.html).
- Sung, Chinmei, and Janet Ong. "Taiwan Opens 100 Industries to Chinese Investment (Update2)." Bloomberg.com. June 30, 2009. <http://www.bloomberg.com/apps/news?pid=20601080&sid=aFeN1SK55G7U>.
- Symantec Press Release. Huawei and Symantec Commence Joint Venture. February 5, 2008. [http://www.symantec.com/about/news/release/article.jsp?prid=20080205\\_01](http://www.symantec.com/about/news/release/article.jsp?prid=20080205_01).
- Szor, Peter. *The Art of Computer Virus Research and Defense*. Boston, MA: Addison-Wesley, 2005, pp. 474–481.
- TechTarget. "SMiShing." SearchMobileComputing.com. Definitions. January 30, 2007. [http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40\\_gci1241308,00.html](http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1241308,00.html).
- TelecomsEurope.net. "Cisco, Juniper Lose Routing Market Share in 2009." "Cisco and Juniper's combined market share fell from 69% in 2008 to 59% in 2009. Huawei and Alcatel-Lucent gained much of the share these companies lost." February 22, 2010. <http://www.telecomseurope.net/content/cisco-juniper-lose-routing-market-share-2009>.
- TeleGeography's ComsUpdate. "Guine Telecom to receive USD50m in Chinese investment." October 21, 2008. [http://www.telegeography.com/cu/article.php?article\\_id=25675](http://www.telegeography.com/cu/article.php?article_id=25675).
- Texas Instruments Press Release. "TI Completes Sale of Sensor Control Business to Bain Capital." April 26, 2006. <http://focus.ti.com/pr/docs/preldetail.tsp?sectionId=594&preId=c06022>.
- Thomas, Timothy L. "Taiwan Examines Chinese Information Warfare." *High Frontiers* Vol. 5, No. 3 (May 2009). <http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf>.
- Thomson Financial News, "China Unicom acquires Netcom," June 2, 2008.
- Thomson Reuters, "2008 Global Innovation Study," March 24, 2009. [http://science.thomsonreuters.com/press/2009/innovation\\_study/](http://science.thomsonreuters.com/press/2009/innovation_study/).
- Thornburgh, Nathan. The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them). *Time*, August 29, 2005. <http://www.time.com/time/magazine/article/0,9171,1098961,00.html>.
- Timmons, Heather. "India Tells Mobile Firms to Delay Deals for Chinese Telecom Equipment," *New York Times*, April 30, 2010. <http://www.nytimes.com/2010/05/01/business/global/01delhi.html>.
- Timmons, Heather. "India Tells Mobile Firms to Delay Deals for Chinese Telecom Equipment." *New York Times*, April 30, 2010. <http://www.nytimes.com/2010/05/01/business/global/01delhi.html>.
- U.S. Department of Defense. *Defense Science Board Task Force on High-Performance Microchip Supply*. Arlington, VA: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2005. <http://www.acq.osd.mil/dsb/reports/ADA435563.pdf>.
- U.S.-China Economic and Security Review Commission. Various Annual Reports to Congress. <http://www.uscc.gov>.
- Ventre, Daniel. "China's Strategy for Information Warfare: A Focus on Energy." *Journal of Energy Security* (May 18, 2010). [http://www.ensec.org/index.php?option=com\\_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361](http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361).
- Ventre, Daniel. China's Strategy for Information Warfare: A Focus on Energy." *Journal of Energy Security* (May 18, 2010). [http://www.ensec.org/index.php?option=com\\_content&view=article&id=241:critical-](http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-)



*energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361.*

- Voice&Data Online. "ZTE Right Pricing." September 3, 2008.  
[http://voicendata.ciol.com/content/service\\_provider/108090303.asp](http://voicendata.ciol.com/content/service_provider/108090303.asp).
- *Wall Street Journal*, "China's Huawei May Sell a Stake Abroad," May 8, 2008.
- *Wall Street Journal*, "China's Telecom Gear Makers, Once Laggards at Home, Pass Foreign Rivals," April 10, 2010.  
[http://www.en.zte.com.cn/en/press\\_center/press\\_clipping/200904/t20090410\\_171143.html](http://www.en.zte.com.cn/en/press_center/press_clipping/200904/t20090410_171143.html).
- *Wall Street Journal*, "Chinese Barriers to Foreign Firms – Good for Innovation," April 15, 2010. <http://blogs.wsj.com/digits/2010/04/15/chinese-barriers-to-foreign-firms-good-for-innovation/>.
- Walt, Stephen, M. "Is the cyber threat overblown?" *Foreign Policy* online. March 30, 2010.  
[http://walt.foreignpolicy.com/posts/2010/03/30/is\\_the\\_cyber\\_threat\\_overblown?obref=obnetwork](http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown?obref=obnetwork).
- War impact maps of the Serbian networks during their 1999 conflict. Available at <http://www.cheswick.com/ches/map/ys/index.html>.
- Washington State. Office of the Attorney General. "Cell Phones Under Attack: How to block text spam and viruses." December 19, 2007.  
(<http://www.sciencedaily.com/releases/2006/08/060829090243.htm>).
- Weisman, Steven R. "Sale of 3Com to Huawei is derailed by U.S. security concerns." *New York Times*, February 21, 2008.  
<http://www.nytimes.com/2008/02/21/business/worldbusiness/21iht-3com.1.10258216.html>.
- Whelan, Carolyn. China's New Frontier. *Fortune*, June 25, 2009. CNNMoney.com.  
[http://money.cnn.com/2009/06/23/technology/china\\_telecom\\_latin\\_america.fortune/index.htm](http://money.cnn.com/2009/06/23/technology/china_telecom_latin_america.fortune/index.htm).
- Wilson, Richard. "China Goes for 4G LTE in a Big Way." *Electronicsweekly.com*. July 29, 2009. <http://www.electronicsweekly.com/Articles/2009/07/29/46620/china-goes-for-4g-lte-in-a-big-way.htm>.
- WiMAX (Worldwide Interoperability for Microwave Access). "What is WiMAX." WiMAX.com. <http://www.wimax.com/education>.
- XChange. Huawei: 'It' Vendor 2010. January 8, 2010.  
<http://www.von.com/articles/2010/01/huawei-it-vendor-of-2010.aspx>.
- Xiaobei, Cheng. "How to Stimulate Domestic Consumption?" *China Today*, February 25, 2009. [http://www.chinatoday.com.cn/ctenglish/se/txt/2009-02/25/content\\_180244.htm](http://www.chinatoday.com.cn/ctenglish/se/txt/2009-02/25/content_180244.htm).
- Xiaohong, Ouyang. "China's Sovereign Wealth Fund Favors Real Economy." *Economic Observer*, March 2, 2009.  
[http://www.eeo.com.cn/ens/finance\\_investment/2009/03/06/131432.shtml](http://www.eeo.com.cn/ens/finance_investment/2009/03/06/131432.shtml).
- Yeo, Vivian. "Chinese Firms Behind 'Sexy Space' Trojan." *CNet.com*. July 22, 2009.  
[http://news.cnet.com/8301-1009\\_3-10292917-83.html](http://news.cnet.com/8301-1009_3-10292917-83.html).
- Zachary, G. Pascal. *See No Evil - How American businesses collaborate with China's repressive government*. ThirdWorldTraveler.com. November 2005.  
[http://www.thirdworldtraveler.com/Transnational\\_corps/See\\_No\\_Evil\\_China.html](http://www.thirdworldtraveler.com/Transnational_corps/See_No_Evil_China.html).

Additional information derived from selected studies, papers, transcripts, lectures, conversations, and collaborations with sources, public and private:

The University of Oxford, Stanford University, Harvard University, Reperi Analysis Center, Trends Digest, RAND Corporation, Carnegie Endowment for International Peace, U.S. Department of Commerce's National Telecommunications and Information Administration, U.S. Federal Communications Commission, National Telecommunications Cooperative Association, U.S. National Institute of Standards and Technology, U.S. National Defense University, U.S. Department of Energy Idaho National Laboratory, U.S. Federal Bureau of Investigation, U.S. Department of Homeland Security, U.S. Department of State, U.S. Air Force Space Command, U.S. National Science Foundation, U.S. Department of Commerce National Technical Information Service, U.S. Department of the Army Foreign Military Studies Office, U.S. Library of Congress, Asia Programme at the Royal United Services Institute for Defence Studies in Whitehall London, Technische Universität Berlin, The Heritage Foundation, Council on Foreign Relations, Foreign Policy Research Institute, APICS Association for Operations Management, European Organization for Nuclear Research, MITRE Corporation, Jawaharlal Nehru University, Institute for Defence Studies and Analyses in New Delhi, Regional Center for Strategic Studies in Sri Lanka, and various other private corporations, universities, individuals, and government institutions.

Other useful publicly available information sources:

The Republic of China Government Information Office (Taiwan), Fudan University, Zhejiang University, Shanghai Academy of Social Sciences, Lanzhou University, Shanghai Center for International Studies, Ministry of Foreign Affairs of the People's Republic of China, China Investment Corporation, China Academy of Military Science, and various other Republic of China (Taiwan) and People's Republic of China sources of publications available as English translations through the U.S. Department of Commerce's National Technical Information Service or other open source translations.

Special thanks to those individuals, including business executives and outside subject-matter experts, who volunteered time, thoughtfulness, and energies to contribute to this report.

# EXHIBIT 4

**2011**  
**REPORT TO CONGRESS**  
*of the*  
**U.S.-CHINA ECONOMIC AND  
SECURITY REVIEW COMMISSION**

ONE HUNDRED TWELFTH CONGRESS  
FIRST SESSION

---

NOVEMBER 2011

---

Printed for the use of the  
U.S.-China Economic and Security Review Commission  
Available via the World Wide Web: <http://www.uscc.gov>



---

U.S. GOVERNMENT PRINTING OFFICE  
WASHINGTON : 2011



**U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION**

Hon. WILLIAM A. REINSCH, *Chairman*  
DANIEL M. SLANE, *Vice Chairman*

**COMMISSIONERS**

CAROLYN BARTHOLOMEW  
DANIEL A. BLUMENTHAL  
PETER T.R. BROOKES  
ROBIN CLEVELAND  
Hon. C. RICHARD D'AMATO

JEFFREY L. FIEDLER  
Hon. PATRICK A. MULLOY  
Hon. DENNIS C. SHEA  
MICHAEL R. WESSEL  
LARRY M. WORTZEL

MICHAEL R. DANIS, *Executive Director*  
KATHLEEN J. MICHELS, *Associate Director*

DANIEL HARTNETT, *Sr. Analyst for Military-Security Issues*  
PAUL MAGNUSSON, *Sr. Analyst for Economics-Trade Issues*

The Commission was created on October 30, 2000, by the Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Pub. L. No. 106-398, 114 STAT. 1654A-334 (2000) (codified at 22 U.S.C. § 7002 (2001), as amended by the Treasury and General Government Appropriations Act for 2002 § 645 (regarding employment status of staff) & § 648 (regarding changing annual report due date from March to June), Pub. L. No. 107-67, 115 STAT. 514 (Nov. 12, 2001); as amended by Division P of the "Consolidated Appropriations Resolution, 2003," Pub. L. No. 108-7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of Commission); as amended by Pub. L. No. 109-108 (H.R. 2862) (Nov. 22, 2005) (regarding responsibilities of Commission and applicability of FACA); as amended by Pub. L. No. 110-161 (Dec. 26, 2007) (regarding changes in annual report due date; submission of financial reports; printing and binding of Congressional reports; employee compensation and performance reviews; and applicability of House rules for travel by members and staff).

The Commission's full charter <http://www.uscc.gov/about/charter.php> and Statutory Mandate <http://www.uscc.gov/about/overview.php> are available via the World Wide Web.

## U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

NOVEMBER 9, 2011

The Honorable Daniel Inouye,  
*President Pro Tempore of the U.S. Senate, Washington, DC 20510*  
 The Honorable John Boehner,  
*The Honorable Nancy Pelosi,*  
*Speaker of the U.S. House of Representatives, Washington, DC 20510*

DEAR SENATOR INOUE AND SPEAKER BOEHNER:

On behalf of the U.S.-China Economic and Security Review Commission, we are pleased to transmit the Commission's 2011 Annual Report to the Congress—the ninth major Report presented to Congress by the Commission—pursuant to Public Law 106–398 (October 30, 2000), as amended by Public Law No. 109–108 (November 22, 2005). This report responds to the mandate for the Commission “to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People’s Republic of China.” In this Report, the Commission reached a broad and bipartisan consensus; it approved the Report unanimously, with all 12 members voting to approve and submit it.

In accordance with our mandate, this Report, which is current as of November 9, includes detailed treatment of our investigations of the areas identified by Congress for our examination and recommendation. These areas are:

- **PROLIFERATION PRACTICES**—The role of the People’s Republic of China in the proliferation of weapons of mass destruction and other weapons (including dual-use technologies), including actions the United States might take to encourage the People’s Republic of China to cease such practices;
- **ECONOMIC TRANSFERS**—The qualitative and quantitative nature of the transfer of United States production activities to the People’s Republic of China, including the relocation of high technology, manufacturing, and research and development facilities, the impact of such transfers on United States national security, the adequacy of United States export control laws, and the effect of such transfers on United States economic security and employment;
- **ENERGY**—The effect of the large and growing economy of the People’s Republic of China on world energy supplies and the role the United States can play (including joint research and development efforts and technological assistance), in influencing the energy policy of the People’s Republic of China;
- **UNITED STATES CAPITAL MARKETS**—The extent of access to and use of United States capital markets by the People’s Republic of China, including whether or not existing disclosure and transparency rules are adequate to identify People’s Republic of China companies engaged in harmful activities;
- **REGIONAL ECONOMIC AND SECURITY IMPACTS**—The triangular economic and security relationship among the United States, [Taiwan] and the People’s Republic of China (including the military modernization and force deployments of the People’s



Republic of China aimed at [Taiwan]), the national budget of the People's Republic of China, and the fiscal strength of the People's Republic of China in relation to internal instability in the People's Republic of China and the likelihood of the externalization of problems arising from such internal instability;

- UNITED STATES–CHINA BILATERAL PROGRAMS—Science and technology programs, the degree of noncompliance by the People's Republic of China with agreements between the United States and the People's Republic of China on prison labor imports and intellectual property rights, and United States enforcement policies with respect to such agreements;
- WORLD TRADE ORGANIZATION COMPLIANCE—The compliance of the People's Republic of China with its accession agreement to the World Trade Organization (WTO); and
- FREEDOM OF EXPRESSION—The implications of restrictions on speech and access to information in the People's Republic of China for its relations with the United States in the areas of economic and security policy.

**The Commission conducted its work through a comprehensive set of eight public hearings, taking testimony from over 65 witnesses from the Congress, the executive branch, industry, academia, policy groups, and other experts. For each of its hearings, the Commission produced a transcript (posted on its Web site—[www.uscc.gov](http://www.uscc.gov)). The Commission also received a number of briefings by officials of executive branch agencies, intelligence community agencies, and the armed services, including classified briefings on China's cyber operations and military and commercial aerospace modernization. (The Commission is preparing a classified report to Congress on those topics.)**

Commissioners also made an official delegation visit to China, Hong Kong, and Taiwan to hear and discuss perspectives on China and its global and regional activities. In these visits, the Commission delegations met with U.S. diplomats, host government officials, representatives of the U.S. and foreign business communities, and local experts.

The Commission also relied substantially on the work of its excellent professional staff, and supported outside research in accordance with our mandate.

The Report includes 43 recommendations for Congressional action. Our 10 most important recommendations appear on page 14 at the conclusion of the Executive Summary.

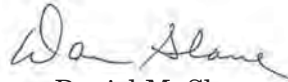
We offer this Report to the Congress in the hope that it will be useful as an updated baseline for assessing progress and challenges in U.S.-China relations.

Thank you for the opportunity to serve. We look forward to continuing to work with you in the upcoming year to address issues of concern in the U.S.-China relationship.

Yours truly,



William A. Reinsch  
*Chairman*



Daniel M. Slane  
*Vice Chairman*

Commissioners Approving the 2011 Report



William A. Reinsch, Chairman



Daniel M. Slane, Vice Chairman



Carolyn Bartholomew, Commissioner



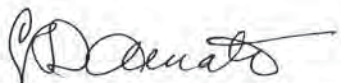
Daniel A. Blumenthal, Commissioner



Peter T. R. Brookes, Commissioner



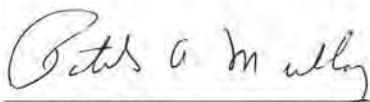
Robin Cleveland, Commissioner




C. Richard D'Amato, Commissioner



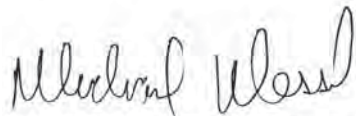
Jeffrey L. Fiedler, Commissioner



Patrick A. Mulloy, Commissioner



Dennis C. Shea, Commissioner



Michael R. Wessel, Commissioner



Larry M. Wortzel, Ph.D., Commissioner



## CONTENTS

---

TRANSMITTAL LETTER TO THE CONGRESS .....	Page iii
COMMISSIONERS APPROVING THE REPORT .....	v
EXECUTIVE SUMMARY .....	1
KEY RECOMMENDATIONS .....	14
INTRODUCTION .....	17

### 2011 REPORT TO CONGRESS OF THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

<b>Chapter 1: The U.S.-China Trade and Economic Relationship .....</b>	<b>21</b>
Section 1: The U.S.-China Trade and Economic Relationship's Current Status and Significant Changes During 2011 .....	21
Section 2: Chinese State-Owned Enterprises and U.S.-China Bilateral Investment .....	40
Section 3: Indigenous Innovation and Intellectual Property Rights .....	70
Section 4: China's Five-Year Plan and Technology Development and Transfers to China .....	88
Section 5: China's Internal Dilemmas .....	107
Recommendations .....	129
Endnotes .....	132
<b>Chapter 2: China's Activities Directly Affecting U.S. Security Interests .....</b>	<b>155</b>
Section 1: Military and Security Year in Review .....	155
Section 2: China's "Area Control Military Strategy" .....	182
Section 3: The Implications of China's Civil and Military Space Activities ....	198
Recommendations .....	221
Endnotes .....	223
<b>Chapter 3: China's Foreign Policy .....</b>	<b>241</b>
Section 1: An Overview of China's Relations with North Korea and Iran .....	241
Section 2: Actors in China's Foreign Policy .....	261
Section 3: Taiwan .....	275
Section 4: Hong Kong .....	290
Recommendations .....	299
Endnotes .....	301
<b>Chapter 4: China's Public Diplomacy Initiatives Regarding Foreign and National Security Policy .....</b>	<b>321</b>
Recommendations .....	342
Endnotes .....	343
<b>Comprehensive List of the Commission's Recommendations .....</b>	<b>355</b>
<b>Additional Views of Commissioners .....</b>	<b>361</b>

VIII

	Page
<b>Appendices:</b>	
Appendix I: U.S.-China Economic and Security Review Commission Charter .....	367
Appendix II: Background of Commissioners .....	377
Appendix III: Public Hearings of the Commission During 2011 .....	387
Appendix IIIA: List of Witnesses Who Testified at Commission Public Hearings During 2011 .....	391
Appendix IV: List of Interlocutors During Commission Fact-Finding Trips to Asia During 2010 and 2011 .....	395
Appendix V: List of Research Material .....	399
Appendix VI: Acronyms and Abbreviations .....	403
<b>2011 Commission Staff and Acknowledgements</b> .....	405

## **EXECUTIVE SUMMARY**

### **The U.S.-China Trade and Economic Relationship**

China is now the second-largest economy in the world and the world's largest manufacturer. Its market exceeds that of the United States in industries such as automobiles, mobile handsets, and personal computers. Although Chinese leaders acknowledge the need to balance their economy by increasing domestic consumption, China continues to maintain an export-driven economy with policies that subsidize Chinese companies and undervalue the renminbi (RMB). While the RMB rose by roughly 6 percent in nominal terms over the last year, it is still widely believed to be substantially undervalued. For the first eight months of 2011, the U.S. trade deficit with China increased 9 percent over the same period in 2010. The U.S. trade deficit with China is now more than half of the total U.S. trade deficit with the world. In the year to date ending August 2011, the United States exported about \$13.4 billion in advanced technology products to China, but imported over \$81.1 billion in advanced technology products from China, for a deficit of about \$67.7 billion. This is a 17 percent increase in the advanced technology products deficit for the same period over the previous year, ending in August 2010.

The Chinese government's special treatment of state-owned enterprises (SOEs) is of particular concern to U.S. businesses, as it can overcome comparative advantages of competitors, thereby harming American economic interests. China's SOEs are also an issue of contention in government procurement, as China seeks to wall off a large portion of its economy from foreign competition.

In 2010, the amount of foreign direct investment (FDI) flowing into China jumped to \$105.7 billion, up from \$90 billion in 2009. Foreign-invested enterprises were responsible for 55 percent of China's exports and 68 percent of its trade surplus in 2010. While some Chinese sectors are now open to foreign sales, huge swathes of the economy are reserved for Chinese firms. Despite Chinese claims that U.S. inward investment policies are protectionist, for the past two years there has been a more than 100 percent year-on-year growth of Chinese investment in the United States. Chinese investments have focused on manufacturing and technology, with an emphasis on brand acquisition. Some critics of China's foreign direct investment in the United States contend that Beijing's efforts are focused on acquiring and transferring technology to Chinese firms.

In March 2011, China ratified its 12th Five-Year Plan (2011–2015), a government-directed industrial policy that focuses on the development and expansion of seven “strategic emerging industries.” The central and local governments will likely continue to combine targeted investment with preferential tax and procure-



ment policies to ensure that Chinese firms emerge as global leaders, or “national champions,” in these industries within the next five years.

China’s indigenous innovation plans that limit government procurement to Chinese companies and China’s continuing lack of enforcement of intellectual property rights are both problematic. In addition, China maintains policies of forced technology transfer in violation of international trade agreements and requires the creation of joint venture companies as a condition of obtaining access to the Chinese market. While the publication of national indigenous innovation product catalogues that favor procurement of Chinese goods over foreign competitors appears to have slowed, local-level catalogues are still in circulation. China continues to be one of the largest sources of counterfeit and pirated goods in the world. The Chinese government itself estimates that counterfeits constitute between 15 and 20 percent of all products made in China and are equivalent to about 8 percent of China’s gross domestic product (GDP). Chinese goods accounted for 53 percent of seizures of counterfeits at U.S. ports of entry in 2010, and the U.S. International Trade Commission estimates that employment in the United States would increase by up to 2.1 million jobs if China were to adopt an intellectual property system equivalent to that of the United States.

The Chinese Communist Party (CCP) relies on economic growth and strict authoritarian rule to maintain control over a factious and geographically vast nation. Socioeconomic issues have been a large driver of protests in China. The party is particularly concerned about inflation, including a 10 percent increase in food prices over the past year, as well as such catalysts of protests as corruption, pollution, and income inequality. In order to maintain control more effectively, the party has created an extensive police and surveillance network to monitor its citizens and react to any potential threat to stability. In 2010, China invested \$83.5 billion in domestic security, which surpassed China’s published military budget of \$81.2 billion for the same year. In early 2011, the central government responded forcefully to the possibility that the unrest in the Middle East might lead to unrest in China. The Chinese government expanded restrictions on online information and access to communication services, reported government propaganda in domestic news outlets, restricted the freedom of foreign journalists, and arrested dissidents with little or no cause.

### **Conclusions**

#### *The U.S.-China Trade and Economic Relationship’s Current Status and Significant Changes During 2011*

- The U.S.-China trade deficit in 2010 set a record high of \$273 billion. The U.S.-China trade deficit now accounts for more than 50 percent of the total U.S. trade deficit with the world.
- Over the last 12 months, the RMB has appreciated by 6 percent. Economists estimate, however, that it remains substantially undervalued. There is increasing grassroots pressure in China to widen the trading band of the RMB and increase the pace of appreciation.

- The Chinese economy, generally, and Chinese exports, in particular, are moving up the value chain. On a monthly basis, the United States now imports roughly 560 percent more advanced technology products from China than it exports to China. Exports of low-cost, labor-intensive manufactured goods as a share of China's total exports decreased from 37 percent in 2000 to 14 percent in 2010.
- China's foreign currency reserves are skyrocketing. A major contributor to this phenomenon is China's continued policy of maintaining closed capital accounts. China's foreign currency reserves currently exceed \$3 trillion, three times higher than the next largest holder of foreign currency reserves, Japan.
- Commensurate with growth in foreign currency reserves, China's domestic money supply is ballooning out of control. Between 2000 and 2010, China's money supply grew by 434 percent. China's money supply is now ten times greater than the U.S. money supply, despite the fact that China's GDP is only one-third as large.
- Such rapid growth in China's domestic money has created strong inflationary pressure. This has helped create a real estate bubble, which resulted in price increases of more than 100 percent in some cities within a handful of years. In September, China's consumer price index topped 6.1 percent across the board and higher in rural areas.
- China has grown more assertive and creative in using WTO procedures to alleviate, eliminate, and avoid certain restrictions in the Accession Protocol. At the same time, the WTO has ruled that China's existing system of state monopoly over imports of cultural products is inconsistent with WTO obligations. China has not yet complied fully with the WTO ruling, and the United States has the right to initiate further proceedings to compel China to do so.

*Chinese State-owned Enterprises and U.S.-China Bilateral Investment*

- China's privatization reforms during the past two decades appear in some cases to have been reversed, with a renewed use of industrial policies aimed at creating SOEs that dominate important portions of the economy, especially in the industrial sectors, reserved for the state's control.
- The Chinese government promotes the state-owned sector with a variety of industrial policy tools, including a wide range of direct and indirect subsidies, preferential access to capital, forced technology transfer from foreign firms, and domestic procurement requirements, all intended to favor SOEs over foreign competitors.
- The value and scope of U.S.-China bilateral investment flows have expanded significantly in the past ten years. However, U.S. direct investment in China is more than 12 times greater than Chinese direct investment in the United States. Official U.S. statistics show that U.S. cumulative FDI in China was

\$60.5 billion in 2010. The Chinese Ministry of Commerce estimated that in 2010, cumulative Chinese FDI in the United States was \$4.9 billion.

- The Chinese government guides FDI into those sectors it wishes to see grow and develop with the help of foreign technology and capital. Foreign investors are frequently forced into joint ventures or other technology-sharing arrangements, such as setting up research and development facilities, in exchange for access to China's market. Meanwhile, large swathes of the Chinese economy are closed to foreign investors. China's investment policies are part of the government's plan to promote the development of key industries in China through access to foreign technology and capital.
- Chinese FDI in the United States is a relatively recent phenomenon and remains very small compared to the U.S. investment in China, but there is great potential for growth. China has stated a desire to diversify its holdings of foreign exchange, estimated at \$3.2 trillion in mid-2011, the majority of which is invested in dollar-denominated debt securities. As with other statistics, there are discrepancies between official U.S. and Chinese statistics on bilateral investment.
- Due to the considerable government ownership of the Chinese economy, provision by Chinese companies of critical infrastructure to U.S. government or acquisition by Chinese companies of U.S. firms with sensitive technology or intellectual property could be harmful to U.S. national interests. The Committee on Foreign Investment in the United States investigates the national security implications of mergers and acquisitions by foreign investors of U.S. assets.
- In areas where there are no national security considerations, Chinese FDI has the potential to create jobs and economic growth.
- China has recently introduced a national security investment review mechanism similar to the Committee on Foreign Investment in the United States, although there are concerns among foreign companies that the Chinese government may use the mechanism to derail investment by foreigners in those companies and sectors it wants to remain under government control.

#### *Indigenous Innovation and Intellectual Property Rights*

- China's indigenous innovation policy is an outgrowth of the government's broad industrial policy and has been openly developed and documented through public plans and pronouncements, particularly the *National Medium- and Long-Term Plan for the Development of Science and Technology (2006–2020)*. The indigenous innovation policy seeks to nurture certain high-wage, high value-added industries designated by the government. Chinese firms are to be favored over foreign firms or China-based foreign affiliates in government procurement contracts. State-owned enterprises and municipal and provincial governments are also to show favoritism to Chinese domestic industries and businesses.

- Chinese officials, including President Hu, have pledged to modify China's indigenous innovation policy in response to protests from U.S. business leaders and top officials. Those promises have not been implemented at the local and provincial levels, however. China has a history of making promises and delivering little, particularly when doing as little as possible benefits the Chinese economy, as has been the case with China's promises to bring its intellectual property protections up to international standards and to cease requiring technology transfers from foreign firms.
- Foreign-invested enterprises seeking to be considered for government procurement contracts or public works projects are expected to file for patents and copyrights within China in order to qualify for preferential treatment in government contracting. Foreign affiliates risk the unintended transfer of their technology to Chinese firms if they do so, because of the nature of the Chinese intellectual property system and the lax enforcement of intellectual property laws and regulations in China.
- Although China agreed in 2001 to stop explicitly requiring foreign companies to surrender their technology to China in return for market access and investment opportunities, the government in Beijing still employs several tactics to coerce foreign firms to share trade secrets with Chinese competitors. China's industrial policy in general and its indigenous innovation policy in particular seek to circumvent accepted intellectual property protections and to extort technology from U.S. companies.
- In addition, the long effort by the central government to foster indigenous innovation is a message that will likely outlive any product catalogues. Restricting market access to domestic firms and requiring technology transfer as a cost for foreigners attempting to do business in China demonstrated the government's view that Chinese companies and governments are better off substituting domestic goods for imports.

*China's 12th Five-Year Plan and Technology Development and Transfers to China*

- One of the main objectives of the 12th Five-Year Plan is to redirect China's economy to one more focused on domestic consumption and less on exports and investment. The plan assumes that China's growth would therefore be more balanced and sustainable. The plan also emphasizes higher value-added production and increased government support for domestic high-tech industries.
- There is cause for skepticism about China's prospects for carrying out the rebalancing goals of the 12th Five-Year Plan. The Chinese government had similar goals in previous plans, but their implementation was sidelined in favor of pursuing higher export and investment growth.

- Increasing household consumption, a major goal of the 12th Five-Year Plan, and the subsequent emergence of a more assertive consumer class, may be in direct contradiction to the Chinese government's policy of keeping economic power firmly in the hands of the state and may compromise lending to many vested interests, including SOEs and the export sector.
- The 12th Five-Year Plan also advocates a move up the manufacturing value chain with the explicit mention of seven strategic emerging industries: New-generation information technology, high-end equipment manufacturing, advanced materials, alternative-fuel cars, energy conservation and environmental protection, alternative energy, and biotechnology. These industries, which will receive targeted government support, have the potential to be a source of economic growth and advanced innovation.
- Analysts and foreign business leaders fear that the emphasis on industrial upgrading will lead to the introduction of new government subsidies, which in turn will disadvantage foreign competitors.
- As part of its indigenous innovation policy, China incentivizes foreign companies to transfer technology in exchange for market access.
- Chinese government requirements that foreign corporations transfer technology to Chinese joint venture partners in exchange for market access violate written WTO prohibitions on forced technology transfers. The new requirements for technology transfer from foreign partners are often made in implicit rather than explicit terms, which may make challenging them in the WTO dispute procedure more difficult.

#### *China's Internal Dilemmas*

- The primary objective of the CCP is to remain in power. All other goals are intended to serve that end. As a consequence, the party has dedicated enormous resources to repress dissent before it becomes a destabilizing element and threatens the party's control.
- Despite the efforts of the party and the government to minimize dissent, citizen protest has been on the rise. Protests are sometimes brutally suppressed. The government will arrest and detain as a precautionary measure those it considers a threat to its control. The party and the government employ the news media to propagandize and mislead the public.
- The party is well aware of the dangers to its continuing authority posed by public rejection of a government that is unresponsive to the people. The party therefore reacts to citizen ire by attempting appeasement. This may take the form of authorizing the news media to highlight official abuses, particularly those committed by local officials. Still, corruption in all levels of government remains a problem for Beijing.

- Inflation has historically caused problems for the government in China. The rural poor and migrant workers are particularly disadvantaged by higher prices because they are so often reflected disproportionately in food and energy, which consume a larger portion of family expenses in rural areas. The government has responded to rising inflation with price controls and some curbs on bank lending. These tools are inadequate in the long run. China's policy of keeping the RMB undervalued in order to gain an export advantage removes a powerful anti-inflation tool from the central bank.
- Income and wealth inequality is a growing problem in China. One cause is the *hukou* system of residential registration, which was intended to limit the migration of the rural poor to the cities. This has created a large migrant population in China, moving from city to city to seek work in factories but unable to access healthcare and education services without the proper *hukou* designation for that area. This situation perpetuates poverty among the disadvantaged. Local officials favor it, because it limits their responsibility toward the migrant workers. A smaller group, known as the "ant tribe," consists of college graduates from second-tier schools in rural areas who also lack the *hukou* to live in urban areas but who nevertheless seek but are unable to find the jobs that they have trained for. This restive and disappointed population is a potential source of unrest.
- China's middle class has been considered by some to be a potential force for political reform. But the opposite is likely. As long as the party can deliver strong economic growth, particularly in urban areas, the middle class is likely to remain a force for stability.
- China's central government has reacted strongly to perceived challenges to its authority. It detains and imprisons dissidents. It censors the news and punishes journalists for infractions of its unwritten and arbitrary rules. China also attempts to control and censor the Internet and has had more success than most other authoritarian regimes in suppressing the flow of information among the public.

### **China's Activities Directly Affecting U.S. Security Interests**

China continues to demonstrate progress in its military modernization efforts. Of note, the People's Liberation Army (PLA) is acquiring specific means to counter U.S. military capabilities and exploit U.S. weaknesses. Since January 2011, China has conducted a flight test of its next-generation fighter aircraft, continued development of its antiship ballistic missile, and conducted a sea trial of its first aircraft carrier. These developments, when operational, will allow China to better project force throughout the region, including the far reaches of the South China Sea.

The PLA's military strategy is designed to provide the army with the means to defeat a technologically superior opponent, such as the U.S. military. As such, it focuses on controlling China's periphery, especially the western Pacific Ocean, degrading an opponent's technological advantages, and striking first in order to gain sur-



prise over an enemy in the event of a conflict. The Commission prefers to use the term “area control” for China’s regional strategy, because the terms “antiaccess” or “area denial” foster a U.S.-centric view that downplays the PLA’s ability to easily conduct operations against regional states. While U.S. bases in East Asia are vulnerable to PLA air and missile attacks, Japanese, Philippine, and Vietnamese bases are just as vulnerable, if not more so.

Tensions continued in 2011 between China and other claimants in the South China Sea territorial disputes as well as with Japan over territory in the East China Sea. Despite intermittent statements of cooperation, Chinese assertiveness in the South China Sea indicates that China is unlikely to concede its sovereignty claims. An implication of China’s growing assertiveness, especially its harassment and intimidation of foreign vessels, is the growing risk of escalation due to miscommunication and miscalculation. As chances of confrontation grow, so could the consequences for the United States, especially with regard to the Philippines, with which the United States holds a mutual defense treaty.

In 2011, as in previous years, the U.S. government, foreign governments, defense contractors, commercial entities, and various nongovernmental organizations experienced a substantial volume of actual and attempted network intrusions that appear to originate in China. Of concern to U.S. military operations, China has identified the U.S. military’s reliance on information systems as a significant vulnerability and seeks to use Chinese cyber capabilities to achieve strategic objectives and significantly degrade U.S. forces’ ability to operate.

The Commission’s *2011 Annual Report to Congress* investigates China’s advancing space program. China is now among the top few space powers in the world. China’s leadership views all space activities through the prism of comprehensive national power, using civil space activities to promote its legitimacy in the eyes of its people, to produce spin-off benefits for other industries, and for military-related activities. For example, China appears to be making great strides toward fielding regional reconnaissance-strike capabilities. China has also continued to develop its antisatellite capabilities, following up on its January 2007 demonstration that used a ballistic missile to destroy an obsolete Chinese weather satellite, creating thousands of pieces of space debris. As a result, in April 2011, astronauts evacuated the International Space Station out of concern of a possible collision with this debris. In addition, authoritative Chinese military writings advocate attacks on space-to-ground communications links and ground-based satellite control facilities in the event of a conflict. Such facilities may be vulnerable: in recent years, two U.S. government satellites have experienced interference apparently consistent with the cyber exploitation of their control facility.

## **Conclusions**

### *Military and Security Year in Review*

- Over the past year, China has demonstrated progress in modernizing the PLA. Recent developments confirm that the PLA seeks to improve its capacity to project force throughout the region.

- Continued improvements in China's civil aviation capabilities, as first noted in the Commission's 2010 Annual Report, enhance Chinese military aviation capabilities because of the close integration of China's commercial and military aviation sectors.
- In an effort to calm regional fears, China attempts to broadcast a benign image of its growing military capabilities. Official statements from Beijing over the past year describe China as a status quo power and downplay its military modernization efforts.
- In 2011, China continued a pattern of provocation in disputed areas of the South China Sea. China's policy in the region appears driven by a desire to intimidate rather than cooperate. Many of China's activities in the region may constitute violations of the *United Nations Convention on the Law of the Sea* and the *Declaration on the Conduct of Parties in the South China Sea*. While China sometimes demonstrates a willingness to cooperate with other claimants to disputed waters in the South China Sea, it is unlikely that China will concede any of its claims.
- China's government or military appeared to sponsor numerous computer network intrusions throughout 2011. Additional evidence also surfaced over the past year that the Chinese military engages in computer network attacks. These developments are consistent with the PLA's known missions and organizational features, as noted by the Commission's *2009 Annual Report to Congress* and contracted research study *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*.
- China's military strategy envisions the use of computer network exploitation and attack against adversaries, including the United States. These efforts are likely to focus on operational systems, such as command, control, communications, computers, intelligence, surveillance, and reconnaissance assets. This could critically disrupt the U.S. military's ability to deploy and operate during a military contingency. Chinese cyber attacks against strategic targets, such as critical infrastructure, are also possible.

*China's "Area Control Military Strategy"*

- The PLA's military strategy is best described as an Area Control Strategy. At its core, this strategy seeks to provide guidance to the PLA on how to defeat a technologically superior opponent.
- In order to defeat a superior opponent, the Area Control Strategy emphasizes degrading an opponent's technological advantages; striking first in a conflict; and establishing military control over China's periphery, especially the maritime region off of China's eastern coast.

- Many of the PLA's force modernization efforts reflect China's Area Control Strategy. As a result, the PLA is acquiring capabilities that allow it to conduct surprise attacks aimed at degrading a superior military's advantages and preventing an opponent from effectively operating along China's periphery.
- Many of the PLA's evolving capabilities appear aimed at directly countering U.S. military capabilities or to exploit potential weaknesses in U.S. military operations. In addition, as the PLA expands its force projection capabilities, China's Area Control Strategy and supporting means will increasingly impact regional states. Finally, the heavy focus on offensive operations inherent in the PLA's Area Control Strategy could serve to undermine stability in the region.

*The Implications of China's Civil and Military Space Activities*

- China is one of the top space powers in the world today. The nation's capabilities, which are state of the art in some areas, follow from decades of substantial investment and high prioritization by China's top leaders. The prestige of space exploration and the national security benefits of space systems serve as primary motivators for Chinese decisionmakers.
- China views all space activities in the context of "comprehensive national power." This concept includes many dimensions, but military aspects are fundamental. The PLA's primacy in all of China's space programs, including nominally civil activities, illustrates this emphasis.
- China's civil space programs have made impressive achievements over the past several decades. If Chinese projections hold, these programs are poised for continued accomplishments over the next ten to 15 years, such as the development of a space laboratory and eventually a space station. As part of an active lunar exploration program, China may attempt to land a man on the moon by the mid-2020s.
- China seeks new opportunities to sell satellites as well as satellite and launch services in international commercial space markets. Chinese firms' prospects for greater success in this field remain uncertain over the near term. However, China's international space-related diplomatic initiatives and their firms' ability to offer flexible terms on sales to developing countries may provide additional opportunities.
- In the military sphere, China appears to seek "space supremacy." The PLA aims to implement this policy through two tracks. First, they increasingly utilize space for the purposes of force enhancement. The best example is China's integration of space-based sensors and guided weapons. Second, they seek the capabilities to deny an adversary the use of space in the event of a conflict. To this end, China has numerous, active, counterspace weapons programs with demonstrated capabilities. China's military space and counterspace activities are part of a larger strategy for area control.

### **China's Foreign Policy**

Despite Beijing's attempts to emphasize its peaceful rise, China continues to support countries that undermine international security. In particular, China's support for North Korea and Iran undermines international efforts to compel these countries to discontinue agendas and programs that destabilize their regions and undercut U.S. interests. As China's global interests expand in a complex international environment, Beijing has experienced a growing number of domestic actors, such as SOEs, interested in determining China's foreign policies. The plethora of new and emerging voices in China's foreign policy-making process makes it more challenging for foreign countries to interact effectively with China. In addition, the pluralization of China's foreign policy actors increases the chance of miscalculations when determining its foreign policies.

In a positive development, economic and diplomatic ties across the Taiwan Strait continue to improve; however, military relations between China and Taiwan lack progress. China maintains some 1,200 short-range ballistic missiles opposite Taiwan. U.S.-Taiwan relations were dominated this year by the question of whether the United States would approve Taiwan's separate requests for additional arms sales. Taiwan has requested three different sales: new F-16C/D fighter jets; upgrades for its current fleet of F-16A/B fighter jets; and diesel-electric submarines. In August 2011 the United States notified Congress of the sale of F-16A/B upgrades but not new F-16C/D fighter jets nor diesel-electric submarines. Reacting against the sale of any new military equipment, China has indicated that it may suspend some military-to-military engagements with the United States.

Some developments in Hong Kong over the past year suggest that Beijing's influence in the region's affairs is growing. During 2011, Beijing increased its focus on Hong Kong's economy, especially its role as a vehicle for the internationalization of China's currency. Mainland involvement in Hong Kong's political affairs was an issue of contention among Hong Kong policymakers and citizens throughout 2011. While Hong Kong citizens and press largely continue to enjoy freedom of expression and assembly, at times these rights were challenged by Hong Kong authorities, who were often perceived to be acting out of deference to Beijing.

### **Conclusions**

#### *An Overview of China's Relations with North Korea and Iran*

- China has continued over the past year to support North Korea despite North Korea's destabilizing actions. Diplomatically, China shields North Korea from pressure in international fora. China also continues to trade with and invest in North Korea, providing it with an economic lifeline in the face of growing international ostracism. Beijing's continued support for Pyongyang is primarily driven by its fear of a collapse of the North Korean regime and the consequences this would have for China's economic, social, and security interests, as well as the fear of the loss of a buffer state on its border.

- Despite U.S. efforts to sanction Iran for its support of international terrorism and pursuit of weapons of mass destruction, China remains a large investor in Iran's petroleum industry and a major provider of refined oil products. China may also be supplying Iran with advanced conventional weapons, such as cruise missiles. China's investments in Iran's petroleum industry, and its continued provision of gasoline and advanced conventional weapons, may be at odds with U.S. laws.
- Continued Chinese support for North Korea and Iran demonstrates China's willingness to place its national interests ahead of regional stability by providing economic and diplomatic support to countries that undermine international security.

#### *Actors in China's Foreign Policy*

- As China expands and diversifies its overseas activities, it encounters an increasingly complex environment requiring the input and advice from knowledgeable subject matter experts. As a result, China's foreign policy-making process is changing to accommodate input from actors who previously had little or no say.
- Actors with increasing influence on China's foreign policies include the PLA, large state-owned enterprises, and academics and think tanks. In addition, while still minor compared to other actors, public opinion, expressed primarily online, appears to have a modicum of influence on some Chinese foreign policies.
- The CCP remains firmly in control of China's foreign policies, especially for issues deemed critical, such as China's policies toward the United States, North Korea, and Taiwan. This is despite the increased difficulty Beijing may have in coordinating a coherent policy among a growing number of actors.
- The growing complexity of China's foreign policy-making process has mixed implications for the United States. On the one hand, Washington may find it more difficult to interact with priority counterparts in Beijing as the number of actors in the policy process expands. On the other hand, the plethora of Chinese actors may provide U.S. foreign policymakers with opportunities to understand or influence Beijing.

#### *Taiwan*

- In 2011, Taiwan and China have continued to strengthen their economic and diplomatic relations by focusing on implementing previous agreements rather than signing new agreements.
- A major factor leading to the slower pace of reduced tensions across the Taiwan Strait is Taiwan's upcoming presidential and legislative elections. Seeking to prevent improving cross-Strait ties from being used against the incumbent Kuomintang Party, both Taiwan and China have moved away from pressing for rapid negotiations and developments as in previous years.

- The cross-Strait military balance continues increasingly to favor China, making it less likely that a peaceful resolution to the Taiwan issue will occur. Despite attempts to improve its capacity to defend the island against a potential attack from the mainland, Taiwan continues publicly to call for additional U.S. arms sales to augment its defense needs.

#### *Hong Kong*

- Hong Kong plays a central role in China's policy goal of internationalizing its currency. In 2011, China introduced substantial new measures supporting Hong Kong's status as China's primary platform for RMB offshoring.
- Mainland involvement in Hong Kong's political affairs was evident in 2011, prompting citizen discontent and conflict within Hong Kong's democratic groups.
- Hong Kong continued to have a vibrant protest culture in 2011, with record amounts of participants in some annual protests. However, there were reports that police sometimes challenged Hong Kong citizens' rights during protests, especially when protests targeted mainland China.
- Hong Kong's mass media reported increased interference in their activities by Hong Kong authorities in 2011. Public perception of self-censorship in Hong Kong's press peaked in 2011, and public opinion of press credibility fell to its lowest level in eight years.

#### **China's Public Diplomacy Initiatives Regarding Foreign and National Security Policy**

The CCP treats the control of propaganda/public diplomacy messages to foreign audiences as a fundamental tool of statecraft. China is highly critical of what it calls the "western media's ideological assault on the rest of the world" and sees itself as engaged in a "global war for public opinion." In pursuit of a larger voice in international affairs, Chinese media officials have significantly increased resources for state-controlled foreign language news outlets. In addition, Chinese propaganda organs are actively engaged in influencing foreign officials and media. This is particularly concerning given the possibility that the People's Republic of China's official messages may not always reflect actual Chinese foreign policy goals.

#### ***Conclusions***

- The Chinese government places a high priority on the management of information as a tool of policy, to include the messages that it promotes to international audiences regarding its goals in foreign and national security policy. The central leadership of the Chinese Communist Party selects official foreign policy messages intended to support state policy goals. These messages are then disseminated through diplomatic channels, state-controlled media, advertising, and "track two" exchanges.



- The Chinese government's official narratives stress China's desire for mutually beneficial "peaceful development" and for a "harmonious" international environment that will allow China to focus attention and resources on its economic and social development. China's statements on its defense policies emphasize that they are entirely defensive in nature and that China will never pose a threat to any of its neighbors.
- There are notable differences between the optimistic character of China's official messages on national security policy, which stress prospects for international cooperation, and the nature of its domestic discourse, which portrays the United States as a dangerous and predatory "hegemon" of the international system.
- The Chinese government frequently discusses important policy issues in terms of China's "core interests," accompanied by an insistence that other countries accept the PRC's non-negotiable positions on these issues. However, conflicting statements from different parts of the Chinese government leave it unclear as to exactly which issues fall into the category of a "core interest." In order to prevent misunderstandings with the United States and other countries that could have serious diplomatic consequences, Beijing should clarify which issues it sees as truly representing a "core interest."
- The emergence of a more outspoken field of PRC foreign policy actors has produced messages that are sometimes at variance with official government narratives. This is particularly true of nationalist voices within the Chinese military.
- The Chinese government makes extensive use of front organizations. Congress and the American public often are not aware that nominally private civic organizations in China that purport to have educational, cultural, or professional purposes are frequently controlled by military, intelligence, or Communist Party organs. These front organizations are used to advance PRC state interests while disguising the guiding role of the government.

### **THE COMMISSION'S KEY RECOMMENDATIONS**

The Commission believes that ten of its 43 recommendations to Congress are of particular significance. These are presented below in the order in which they appear in the Report. The complete list of 43 recommendations appears at the Report's conclusion on page 355.

The Commission recommends that:

- Congress, through legislation, require the president to assign the National Security Council to conduct an agency-wide comprehensive review of the U.S. economic and security policies toward China to determine the need for changes to address the increasingly complicated and serious challenges posed by

China to U.S. international and domestic interests. Such a review should be examined and debated as appropriate by Congressional committees.

- Congress urge the administration to employ all necessary remedies authorized by WTO rules to counter the anticompetitive and trade-distorting effects of the Chinese government's extensive subsidies for Chinese companies operating in China and abroad.
- Congress direct the U.S. Department of Commerce to report annually on Chinese investment in the United States including, among other things, data on investment in the United States by Chinese SOEs and other state-affiliated entities.
- Congress direct the U.S. Securities and Exchange Commission to revise its protocols for reviewing filings by foreign entities listed on or seeking to be listed on the U.S. stock exchanges. The Securities and Exchange Commission should develop country-specific data to address unique country risks to assure that U.S. investors have sufficient information to make investment decisions. The commission should focus, in particular, on state-owned and -affiliated companies, and subsidies and pricing mechanisms that may have material bearing on the investment.
- Congress assess the reauthorization of Super 301 to assist in the identification of the policies and practices that China pursues that create the greatest impediment to U.S. exports entering the Chinese market and the most important policies or practices that unfairly or unjustifiably harm U.S. producers and workers in the U.S. market. Priority should be given to addressing such practices by the United States Trade Representative under such legislation.
- Congress direct the U.S. Government Accountability Office to undertake an evaluation of investments and operations of U.S. firms in the Chinese market and identify what federally supported R&D is being utilized in such facilities and the extent to which, and on what terms, such R&D has been shared with Chinese actors in the last ten years.
- Congress assess the adequacy of U.S. Department of Defense capabilities to conduct major operations in a degraded command, control, communications, computer, intelligence, surveillance, and reconnaissance environment for an extended period of time.
- Congress assess the adequacy and regularity of U.S. military exercises and training activities that simulate the destruction, denial, degradation, or manipulation of U.S. space assets. In addition, Congress should periodically evaluate whether the U.S. Department of Defense is taking sufficient measures to diversify its traditionally space-oriented capabilities, such as in navigation, communications, intelligence, surveillance, and reconnaissance.

- Congress investigate whether U.S. sanctions have been imposed on all Chinese firms that have violated the sanction laws by investing in Iran's petroleum industry or providing Iran with refined petroleum products or advanced conventional weapons.
- Congress urge the administration to sell Taiwan the additional fighter aircraft it needs to recapitalize its aging and retiring fleet.

## INTRODUCTION

This is the Commission's tenth year examining U.S.-China relations. During this time the United States has welcomed China's peaceful rise with the belief that by engaging China it would be encouraged to open up to the United States and the world, both economically and diplomatically, that it would expand freedom and human rights, and that it would become a responsible global stakeholder. For the last ten years the Commission has documented Chinese export subsidies; weapons proliferation; cyber attacks; non-compliance with World Trade Organization (WTO) obligations; forced technology transfers; military modernization; resource acquisition strategies; expansion of Chinese foreign policy interests; the Chinese military threat to Taiwan; espionage; and information control, among other issues. While China has taken some steps to engage the international community, by and large the Communist Party of China (CCP) has continued to steer policy in its own narrow self-interest at home and abroad, often without regard for international rules and norms. As a result, worldwide concern about China is growing as more people see the implications of the rise of a powerful authoritarian state.

In 2011, China assumed a more assertive role on the global stage. China's new posture was reflected in an aggressive trade agenda, a push for a larger role in international institutions, and provocative moves in the South and East China Seas. These actions were both a reflection and a consequence of China's growing economic prominence and resource needs, as well as China's view that the United States is in decline while China is ascendant. Chinese policies have had an impact on the United States, ranging from a negative effect on the U.S. economy to increased pressure from some parts of the international community for the United States to ensure the security of the global commons.

Last year, the Commission highlighted China's backsliding from market reforms in favor of an increased role of the state in the economy. In contrast to the general trend of economic liberalization over the last three decades, last year's pattern of increased state dominance continued in 2011. China subsidizes its state-owned enterprises to the detriment of both private Chinese firms and international competitors. Nevertheless, Chinese leaders acknowledge the economy must be moved away from its investment-led, export-driven growth model toward one more dependent on domestic consumption.

Even when China makes a commitment to economic reform, the government reverts to its historical pattern of inadequate implementation. President Hu Jintao and other Chinese officials responded to western pressure in January 2011, promising to ease a policy of discriminating against foreign companies in government

procurement decisions; however, real change remains elusive, particularly among the provincial and local governments.

In March 2011, China approved its 12th Five-Year Plan (2011–2015), which calls for the transformation of the Chinese economy into a high-technology and innovation-oriented juggernaut. The plan identifies seven strategic emerging industries in which the Chinese hope to become world leaders. While the desire to move up the manufacturing value chain is a common goal among nations, the web of Chinese industrial policies used to achieve this objective has often had a detrimental impact on U.S. interests and is often inconsistent with China's obligations under the WTO. Practices such as forced technology transfer and the creation of joint venture companies as a condition to obtaining access to the Chinese market; the adoption of unique, Chinese-specific standards for high-tech equipment; and extensive intellectual property rights violations are among the faulty policies designed to help China achieve its goal of becoming a high-tech leader.

China's military modernization, combined with the unclear nature of Beijing's views of what constitutes an attack and the People's Liberation Army's military doctrine that emphasizes striking first in a conflict, increases the possibility for inadvertent conflict in the region. China's massive military modernization includes the sea test of its first aircraft carrier, the introduction of a fifth-generation stealth fighter, and the further development of already sophisticated cyber warfare and counterspace capabilities. Designed to defeat a technologically superior opponent, China's military strategy emphasizes striking first and controlling the nation's periphery in the event of a conflict. While the exact pace and scale of China's military modernization effort and the intentions behind it remain opaque to the outside world, it is clear that China is acquiring specific means intended to counter U.S. military capabilities and exploit U.S. weaknesses.

While China has taken an externally assertive posture, it faces many internal challenges. The CCP relies on economic growth, combined with strict authoritarian rule, to maintain control over a factious and geographically vast nation. Sharp increases in consumer prices, a pivotal factor in the early days of the student protests in Tiananmen Square in 1989, are once again a problem for the Chinese economy. While the party is particularly concerned about inflation, it also struggles to respond to other causes of protest such as corruption, pollution, and income inequality. The CCP faces the dilemma that the very authoritarian measures it uses to assert control of the Chinese people result in abuse, corruption, and policies that increase popular dissatisfaction. In turn, China's domestic instability may be fueling its external assertiveness if Chinese leaders bend to or encourage nationalist sentiment.

Secretary of State Hillary Rodham Clinton observed that China represents one of the most challenging and consequential bilateral relationships the United States has had to manage. While promoting messages of reassurance to the international community, China focuses on pursuing its own narrow interests. Despite the threatening and unpredictable conduct of North Korea, the CCP appears to have calculated that its interests are better served by the support of the regime than by its removal. Likewise, China's

relationship with Iran undermines international efforts to curtail Iran's pursuit of weapons of mass destruction and support of international terrorism.

Despite the improvement in economic and diplomatic relations across the Taiwan Strait, China deploys some 1,200 short-range ballistic missiles against the island. In response to the U.S. sale to Taiwan of a new \$5.8 billion package of upgrades to its aging fleet of F-16 fighter jets, China indicated that it may suspend a series of military-to-military engagements. To the consternation of its neighbors, China asserts its expansive territorial claims in the South and East China Seas. China is increasingly capable of pursuing its own interests at the expense of regional, perhaps even global, stability.

China's opaque intentions complicate our understanding and response to its rise as a world power. China's stated desire to maintain stable and peaceful international relationships conflicts with such actions as harassing vessels operating in international waters off the Chinese coast, aggressively pressing unrecognized territorial claims in the East and South China Seas, and supporting North Korea in the aftermath of unprovoked acts of aggression against South Korea. In fact, the People's Republic of China's official messages may be a cover for China's actual foreign policy goals. In addition, internal power struggles among Chinese foreign policy-makers make it difficult to understand the decision-making process in China, increasing the chance of miscalculating China's foreign policy.

The next few years will illustrate how China wishes to embrace the international order and the manner in which it will use its increasing power. China is faced with a choice. It can either join the community of nations in the existing international order based on the rule of law, or it can aggressively assert its own interests without regard for the concerns of other states and face growing opposition from the global community. The latter is not in anyone's interest. By welcoming China into the WTO and other international bodies, the U.S. government has demonstrated that it wants the Chinese government to be a responsible international stakeholder; however, until China more fully complies with international norms, the United States must be more forceful in asserting its own national interests. Insisting on reciprocity in our economic relationship and respect for international laws and norms in our geostrategic relationship is a start. This would not only benefit U.S. citizens but also demonstrate to the world that the United States is still the standard-bearer for stability and rule of law. We are in a global competition with China, and U.S. policies should flow from this premise. The United States should insist on reciprocity and mutual benefit as guiding principles of the U.S.-China relationship. It is clear that China will pursue its own narrow goals unless international pressure is brought to bear to modify any objectionable behavior.

While effectively responding to China is not an easy task, the Commission's 2011 Report is an outline that we believe will be helpful to Congress in addressing China's rise. The Commission recommends that Congress, through legislation, require the president to assign the National Security Council to conduct an agency-



wide comprehensive review of U.S. economic and security policies toward China to determine the need for changes to address the increasingly complicated and serious challenges posed by China to U.S. international and domestic interests. Such a review should be examined and debated as appropriate by Congressional committees.

# CHAPTER 1

## THE U.S.–CHINA TRADE AND ECONOMIC RELATIONSHIP

### SECTION 1: THE U.S.–CHINA TRADE AND ECONOMIC RELATIONSHIP’S CURRENT STATUS AND SIGNIFICANT CHANGES DURING 2011

#### Introduction

In the ten years since China joined the World Trade Organization (WTO), China has maintained a steep growth trajectory, outpacing both Germany and Japan to become the second largest economy in the world. China’s gross domestic product (GDP) has grown from \$1.32 trillion in 2001 to a projected \$5.87 trillion in 2011. This represents an increase of more than 400 percent. In certain industries, such as automobiles, mobile handsets, and personal computers, China’s market already exceeds that of America’s. Concurrently, China has lifted 400 million of its citizens out of poverty and has experienced the largest rural-to-urban migration in history.<sup>1</sup>

At the same time, the concerns that originally surrounded China’s accession to the WTO—that China’s blend of capitalism and state-directed economic control conflict with the organization’s free market principles—have proven to be prophetic. Although China did not meet all of the traditional requirements for accession, the WTO took a calculated gamble that China could effectuate the reforms necessary to conform to those requirements within a reasonable period of time. The U.S.-China Economic and Security Review Commission was established by the United States Congress in part to monitor the outcome of that gamble. Ten years later, China’s state-directed financial system and industrial policy continue to contribute to trade imbalances, asset bubbles, misallocation of capital, and dangerous inflationary pressures. Meanwhile, China’s legal reforms are in jeopardy from a bureaucratic backlash.<sup>2</sup> China’s adherence to WTO commitments remains spotty despite the decade that the country’s rulers were given to adjust. These circumstances create an uneven playing field for China’s trading partners and threaten to deprive other WTO signatories of the benefit of their bargain.

Each of these issues will be analyzed in detail in this section, beginning with an examination of U.S.-China trading relations, followed by U.S.-China financial relations and, finally, an evaluation of China’s role in the WTO. The fact that a decade has now passed since China’s controversial admission to the WTO means that

China is now relieved of its burden of facing an annual review by the WTO of China's compliance. This section will examine the implications of this change.

### U.S.-China Trading Relations

For the first eight months of 2011, China's goods exports to the United States were \$255.4 billion, while U.S. goods exports to China were \$66.1 billion, yielding a U.S. deficit of \$189.3 billion. This represents an increase of 9 percent over the same period in 2010 (\$119.4 billion). During this period China exported four dollars' worth of goods to the United States for each dollar in imports China accepted from the United States. In 2010, the United States shipped just 7 percent of its total exports of goods to China; China shipped 23 percent of its total goods exports to the United States. In the ten years since China joined the WTO, the U.S. trade deficit with China has grown by 330 percent (see table 1, below).

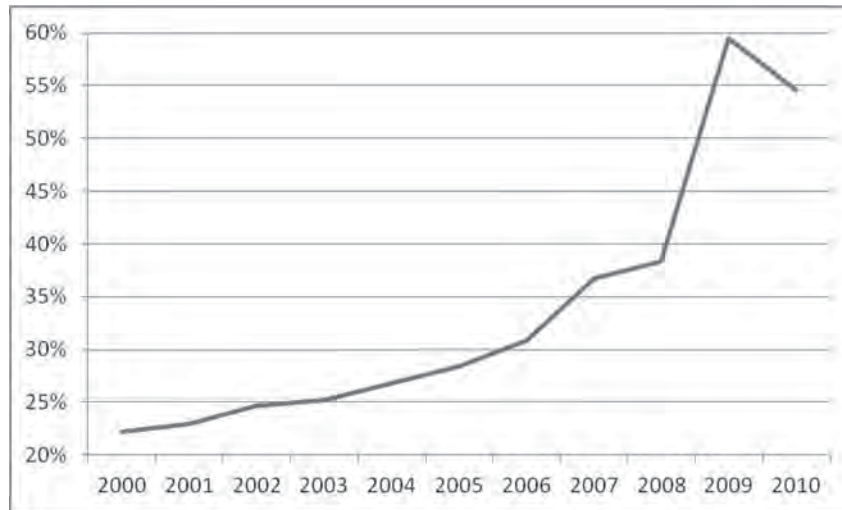
**Table 1: U.S.-China Trade in Goods (\$ billions), 2000-2011 YTD**

	00	01	02	03	04	05	06	07	08	09	10	11 (YTD)
U.S. Exports	16	19	22	28	34	41	55	65	69	69	91 <sup>3</sup>	66
U.S. Imports	100	102	125	152	196	243	287	321	337	296	364	255
Balance	-83	-83	-103	-124	-162	-201	-232	-256	-268	-226	-273	-189

Source: U.S. Census Bureau, *U.S. Trade in Goods and Services* (Washington, DC: U.S. Department of Commerce, August 15, 2011).

At first glance, this trade deficit may appear to be explained by a broader trend of American dependence on imports, but this is not the case. In the first eight months of 2011, Chinese goods accounted for 20 percent of U.S. imports, while U.S. goods accounted for only 5 percent of Chinese imports.<sup>4</sup> China's portion of America's trade deficit has increased considerably. While the overall U.S. trade deficit with the world has grown from \$376.7 billion in 2000 to \$500 billion in 2010, China's share of this deficit has nearly tripled during the period, from 22 percent in 2000 to 60 percent in 2009 and 55 percent in 2010 (see figure 1, below).

**Figure 1: China's Share of the U.S. Global Trade Deficit (by percentage), 2000–2010**



Source: U.S. Bureau of the Census, *U.S. Trade in Goods and Services* (Washington, DC: U.S. Department of Commerce, August 15, 2011).

These data suggest that the growth in the U.S. global trade deficit reflects growth in the U.S. trade deficit with China and that other emerging economies are being replaced by China as a final supplier of finished exports to the United States. Indeed, numerous international trade scholars have asserted a causal link between increases in China's trade surplus with the United States and decreases in the bilateral balance of trade of other nations of South and South East Asia with the United States.<sup>5</sup>

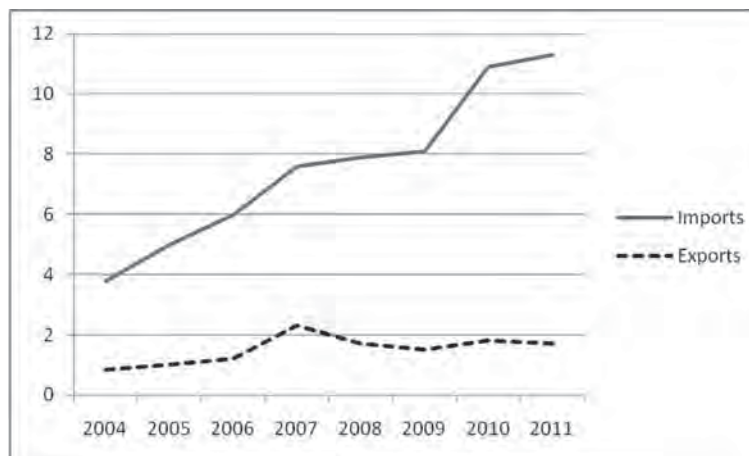
The more significant trend, however, is not the magnitude of the U.S. trade deficit with China but the composition of goods. Over the last ten years, Chinese manufacturing has undergone a dramatic restructuring away from labor-intensive goods toward investment-intensive goods. Production is driven increasingly less by low-cost labor and increasingly more by low-cost capital, which is used to build next-generation manufacturing facilities and to produce advanced technology products for export. This can be seen most clearly by examining Chinese exports of labor-intensive products, such as clothing and footwear, as a percentage of total exports. In 2000, exports of labor-intensive products constituted 37 percent of all Chinese exports. By 2010, this percentage fell by more than half had fallen to just 14 percent (see table 2, below).

**Table 2: Chinese Labor-intensive Exports (as a percentage of total exports), 2000–2010**

	2000	2005	2010
Apparel and clothing	24	10	9
Footwear	7	3	2
Furniture	3	2	2
Travel goods	3	1	1
<b>Total</b>	<b>37</b>	<b>16</b>	<b>14</b>

Source: Manufacturers Alliance, “U.S. and Chinese Trade Imbalances in Manufactures Surge” (Maple Grove, MN: Manufacturers Alliance Economic Report, ER-728, August 2011).

This shift has serious implications for the U.S. economy. As China joined the WTO, the United States had already lost production of low-value-added, low-wage-producing commodities such as umbrellas and coffee cups. But America’s export strength lay in such complex capital goods as aircraft, electrical machinery, generators, and medical and scientific equipment. China’s exports to the United States are increasingly from its capital-intensive industries, particularly advanced technology products. From 2004 to 2011, U.S. imports of Chinese advanced technology products grew by 16.5 percent on an annualized basis, while U.S. exports of those products to China grew by only 11 percent.<sup>6</sup> In August 2011, U.S. exports of advanced technology products to China stood at \$1.9 billion, while Chinese exports of advanced technology products to the United States reached \$10.9 billion, setting a record one-month deficit of more than \$9 billion. On a monthly basis, the United States now imports more than 560 percent more advanced technology products from China than it exports to that country (see figure 2, below).<sup>7</sup>

**Figure 2: U.S. Exports to and Imports from China of Advanced Technology Products in the Month of June (\$ billion), 2004–2011**

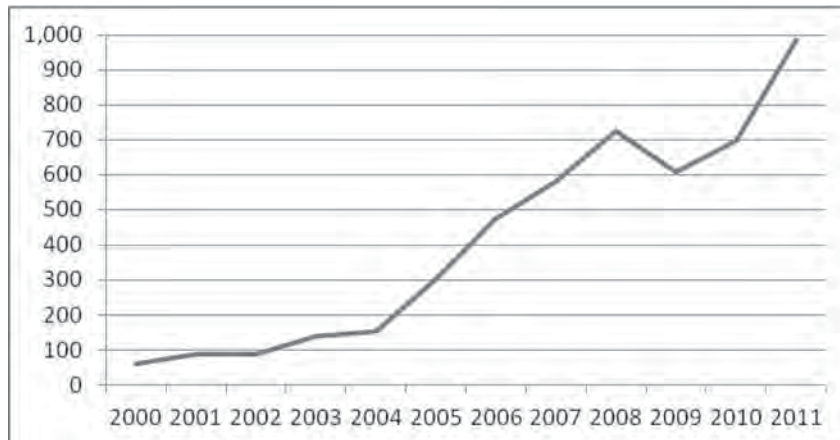
Source: U.S. Bureau of the Census, *U.S. Trade in Goods and Services* (Washington, DC: U.S. Department of Commerce, August 15, 2011).

The weakness in U.S. exports of advanced technology products to China is explained in part by barriers to market access experienced by U.S. companies attempting to sell into the Chinese market.<sup>8</sup> According to a recent survey conducted by the American Chamber of Commerce in China, 71 percent of American businesses operating in China believe that foreign businesses are subject to more onerous licensing procedures than Chinese businesses.<sup>9</sup> Additionally, twice as many respondents report that Chinese licensing strictures have grown more onerous over the last year than those who believe that licensing requirements have eased. Finally, four times as many respondents report that they have been harmed by national treatment as those who report that they were aided. Encountering market access barriers, however, is not unique to American business. A similar 2011 study by the European Chamber of Commerce in China found that inconsistencies in the procurement process employed by the Chinese central government resulted in a lost opportunity for European businesses that is equal in size to the entire economy of South Korea, or one trillion dollars.<sup>10</sup>

Import barriers are part of China's policy of switching from imports to domestically produced goods. In particular, part of China's "indigenous innovation" policy protects domestically produced goods by discriminating against imports in the government procurement process, particularly at the provincial and local levels of government.<sup>11</sup> (For a more complete discussion of the indigenous innovation policy, please see chap. 1, sec. 3, of this Report.)

By contrast, the monthly U.S. trade surplus in scrap and waste reached a record high of \$1.1 billion in August 2011. The annual U.S. trade surplus in scrap and waste grew from \$715 million in 2000 to \$8.4 billion in 2010, representing an increase of 1,187 percent, or 28 percent per year on an annualized basis (see figure 3, below). Unfortunately, however, the gains to the U.S. economy from this trend are limited, as the value-added component of scrap and waste is almost nothing.

**Figure 3: U.S. Trade Surplus in Scrap and Waste with China in the Month of June (\$ million), 2000–2011**

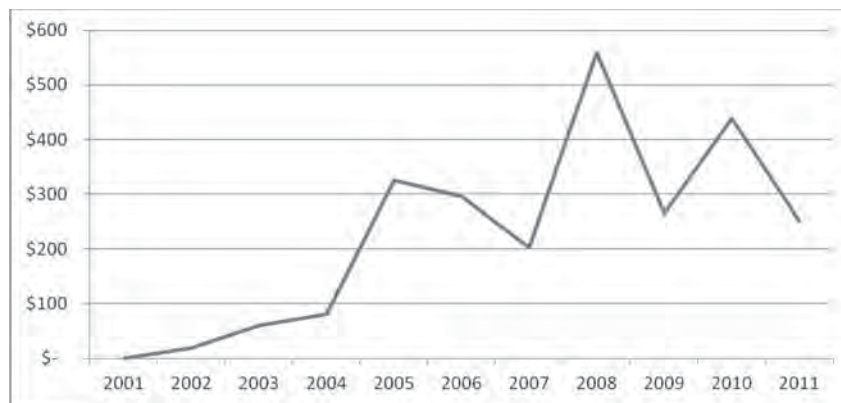


Source: U.S. Bureau of the Census, *U.S. Trade in Goods and Services* (Washington, DC: U.S. Department of Commerce, August 15, 2011).



Similarly, the U.S. trade surplus in agricultural products with China has experienced dramatic growth (see figure 4, below). This trend has been fueled by higher grain prices in the Chinese market, greater demand for animal feed from Chinese farmers, and a series of water shortages that have left China more or less dependent on foreign sources of food. The inflationary antecedents to these trends are discussed in greater depth below.

**Figure 4: July U.S. Surplus of Trade in Agricultural Products with China (\$ million), 2001–2011**



Source: U.S. Bureau of the Census, *U.S. Trade in Goods and Services* (Washington, DC: U.S. Department of Commerce, August 15, 2011).

### U.S.-China Financial Relations

U.S.-China financial relations are largely determined by two bed-rock monetary policies of the Chinese government: a closed capital account and a closely managed exchange rate. Since 1994, the Chinese government has used a variety of methods to insulate the value of its currency from market forces that would otherwise have caused the renminbi (RMB) to appreciate against the dollar. In various policy statements and in its 12th Five-Year Plan (2011–2015), the Chinese Communist Party has once again identified gradual liberalization of the capital account as one of its priorities.<sup>12</sup>

Consequently, movement toward a more market-based currency has been slow and halting.<sup>13</sup> Chinese merchants who export to foreign parties are still left with little choice other than to relinquish their foreign currency earnings to the state-owned banks in exchange for renminbi. Thus, when China runs a trade surplus, the supply of RMB in circulation grows.<sup>14</sup> To counteract the inflation that would naturally spring from a rapidly expanding money supply, the Chinese government issues special bonds in an attempt to attract investors and thereby soak up the extra money.<sup>15</sup> Thus, the government is left holding both foreign currency and RMB, and the Chinese public is left holding sterilization bonds denominated in RMB. The Chinese government must then reinvest the foreign currency if it is to avoid losing value to inflation. The Chinese government could pursue any investment strategy, but in order to satisfy

the second of its two primary monetary policies, namely, a managed exchange rate, it chooses to invest its foreign currency in bonds, primarily U.S. Treasury bonds.

This activity helps maintain the price of dollars relative to the RMB.<sup>16</sup> To avoid a black market in foreign currency, the government requires that most Chinese businesses and citizens exchange their dollars at a bank, the large majority of which are state owned. Each day the central bank declares the price at which the state-owned banks will exchange dollars for RMB. Finally, in order to keep this maneuver affordable, the government must maintain an abnormally low domestic rate of interest. For if the prevailing interest rate at Chinese banks were to increase, then the government would be forced to increase the interest rate on sterilization bonds in order to maintain their attractiveness in the market, which would significantly increase the cost associated with the exchange rate policy. These conditions create a perfect setting for inflation, as the following data will illustrate.

In June 2011, China's foreign exchange reserves surged on strong trade surpluses to \$3.2 trillion, up nearly one trillion from \$2.4 trillion in June 2010, or roughly 30 percent year-on-year growth.<sup>17</sup> China's foreign exchange reserves are now roughly three times greater than that of Japan, which has the second-highest foreign exchange reserves in the world. Roughly two-thirds of China's foreign exchange reserves are generally thought to be denominated in U.S. dollars, although the exact makeup of the reserves is unknown, because the Chinese government considers it to be a state secret.

Somewhat better known is the volume of China's foreign exchange reserves that are made up of U.S. Treasury securities. As of July 2011, the official estimate by the U.S. Treasury Department stood at \$1.2 trillion, up slightly from the same period one year before.<sup>18</sup> The real amount is considerably higher, since the \$1.2 trillion does not take into account any purchases made on the secondary market nor does it factor in purchases made by intermediaries or made through tax havens, such as the Cayman Islands. (For a more thorough examination of this issue, see the Commission's *2010 Annual Report to Congress*, chap. 1, sec. 2, "The Implications and Repercussions of China's Holdings of U.S. Debt.")

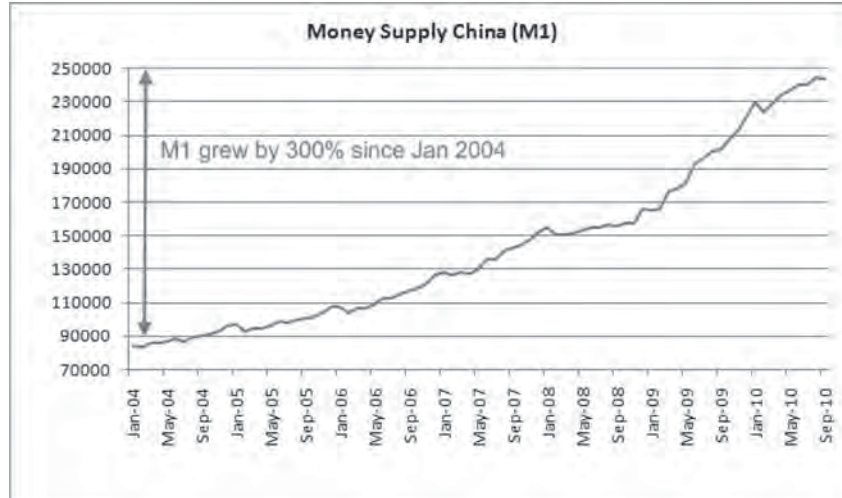
China's decision to purchase U.S. government securities is not born out of any diplomatic beneficence but, rather, the economic self-interest of China, seeking to fix the exchange rate of the RMB to the dollar. In 2011, China's resolve was tested when a major rating agency reduced the credit rating of U.S. Treasury bonds. As the party with the largest holdings of U.S. government debt, China stands to lose the most from any drop in value of U.S. Treasury securities.

Beijing remained silent during the summer debt ceiling impasse in Washington.<sup>19</sup> However, following Standard & Poor's downgrading of U.S. Treasury bonds, Guo Shuqing, the chairman of the China Construction Bank and former head of the State Administration of Foreign Exchange, opined that "[h]olding U.S. Treasuries contains certain risks, but at a time when the global economy is volatile and the euro zone is in deep difficulties, U.S. Treasuries, among all the not-so-ideal products, remain as the best product in

terms of safety and returns.”<sup>20</sup> Mr. Guo’s comment reflects the fact that China is committed to the outsized ownership of U.S. Treasuries by its choice of methodology in controlling the price of the RMB. In addition, as U.S. interest rates have declined, the market value of China’s Treasury holdings has increased. Standard & Poor’s downgrade of U.S. Treasuries did not affect this trend.

As a result of growth in foreign exchange reserves, China’s domestic money supply has skyrocketed, which has added to inflationary pressures. In May and June 2011, China’s M2 money supply, which includes checking, savings, and money market accounts, grew by more than 15 percent.<sup>21</sup> From 2000 to 2010, aggregate M2 growth amounted to 434 percent, totaling more than \$10 trillion in U.S. dollars.<sup>22</sup> By way of comparison, from 1996 to 2008, the U.S. money supply grew at an average annual rate of 3.5 percent and currently stands at \$1.005 trillion.<sup>23</sup> Considering that the U.S. gross domestic product (GDP) is still roughly three times greater than the Chinese GDP, this means that the Chinese money supply has grown to be roughly 30 times greater than the U.S. money supply when normalized to scale (see figure 5, below). Figure 5 depicts the growth over time of U.S. and Chinese M1 money supplies, which is equivalent to M2 minus savings deposits and time deposits.

**Figure 5: Chinese M1 Money Supply by Year (100 Million RMB) 2004–2010**



Source: Economics Junkie, November 18, 2010. <http://www.economicjunkie.com/inflation-money-supply-in-china/>.

Derek Scissors, an expert in the Chinese economy at The Heritage Foundation, characterized growth in the Chinese money supply in the following terms: “There are occasional, loud claims in China that the current bout of inflation was caused by quantitative easing in the United States. This is like blaming your brother-in-law’s binge eating for your weight gain. China’s 2008 stimulus package led to a 30-percent increase in the money supply in 2009. The

PRC's (People's Republic of China) monetary base is bigger than America's, even though its economy is less than half the size. Chinese inflation is home-made, and the recipe is simple."<sup>24</sup>

Citing the danger that such money growth can pose, the Chinese government has pronounced the curtailment of inflation as one of its top economic priorities. But because the Chinese government relies upon issuing debt in order to carry out its managed exchange rate policy, it has limited options. Raising interest rates would require the government to pay higher interest on the sterilization bonds. Consequently, the only inflation-fighting weapon fully available to the government is raising the reserve requirement for banks in order to remove money from circulation, which it has done several times over the last year.<sup>25</sup> Beijing also initiated a campaign to rein in off balance sheet lending, a hallmark practice of Chinese banks.<sup>26</sup>

In June 2011, Chinese Premier Wen Jiabao published an op-ed in the *Financial Times* claiming that these measures had succeeded in taming inflation.<sup>27</sup> Despite Premier Wen's assurances, inflation continued to rise. In September 2011, China's consumer price index hovered at 6.1 percent.<sup>28</sup> Food prices, the single largest driver of inflation, were up 13.4 percent. In the same period, housing prices went up 5.9 percent year on year, indicating the formation of a real estate bubble.

Not all of this inflationary activity is attributable to growth in money supply. Other factors play a role as well. For example, as rural-to-urban migration tapers off, manufacturers are finding it more difficult to keep their factories staffed. As labor shortages mounted, wages were increased in order to attract workers.<sup>29</sup> Consequently, households can afford to spend more on meat and grain, which drives up the price of agricultural commodities. China is also facing growing shortages of water, which further exacerbates inflation in farm goods. For a country that is increasingly reliant upon hydroelectric power, water shortages place upward pressure on the price of electricity.<sup>30</sup> This, in turn, drives up the cost of production in secondary industries.

Until recently, the greatest inflationary threat facing the Chinese government was rapid increases in the price of fixed assets, particularly real estate. In response to popular discontent, the Chinese government placed a priority on taming real estate prices, with some success.<sup>31</sup> According to data released in mid-August, prices for newly built homes stayed level or decreased in 31 out of China's top 70 cities, including Shanghai, Beijing, Shenzhen, and Guangzhou.<sup>32</sup> At the same time, the liabilities of China's property developers increased by 43 percent year on year, and the Guggenheim China Real Estate Fund, a popular exchange traded fund that tracks the performance of the Chinese property development industry, fell 28 percent from a year-long high of \$30.37 per share in November 2010 to \$21.96 in October 2011.<sup>33</sup>

China's response to its inflation problem has drawn criticism because it failed to deal with China's capital controls as a cause of inflation. Economist Nigel Chalk of the International Monetary Fund likened China's Pyrrhic victory over property prices and subsequent surge in the consumer price index to an economic game of *Whack-a-Mole*.<sup>34</sup> Benjamin Simfendorfer, former chief China econo-

mist at the Royal Bank of Scotland, predicted that China's consumer price index will remain between 5 percent and 10 percent for the next decade.<sup>35</sup> And Nouriel Roubini, professor of economics at New York University, decried China's dependence on fixed asset investment as the principal driver of China's GDP growth and a factor in its inflation.<sup>36</sup> All noted that the Chinese government is merely treating the symptom, rather than the cause, of the inflation problem. Until the Chinese government fully liberalizes its capital account, and ceases manipulating its currency, China's trade surpluses will continue to inflate the supply of RMB in circulation. Until the Chinese government eliminates its reliance on sterilization bonds, Chinese savers will prefer the volatile real estate market as an investment vehicle over the negative real returns from bank deposits and bonds. Finally, until the Chinese government fully subjects the RMB to the dictates of market forces, the consumption share of China's GDP will remain stunted at around 35 percent—half the rate in the United States, according to many commentators.<sup>37</sup>

On the positive side, the Chinese government allowed the RMB to rise by roughly 6 percent in nominal terms over the last year, from 6.775 RMB per dollar on July 16, 2010, to 6.370 RMB per dollar on October 17, 2011.<sup>38</sup> This is the second-fastest rate of appreciation since the Chinese government eliminated its hard peg to the dollar in 2005. Nonetheless, the US Treasury Department reports that the RMB remains “substantially undervalued.”<sup>39</sup> There is also nascent acknowledgement by Chinese academics that Beijing's intervention in the foreign exchange market has a measurable effect on the balance of trade, at least in certain sectors. For example, in a scholarly article published in the Chinese journal *Advances in Informational Sciences and Service Sciences*, researchers from Huazhang Agricultural University found that every 1 percent increase in the exchange rate between the RMB and the U.S. dollar leads to a 0.498 percent decrease in Chinese exports of citrus fruits.<sup>40</sup> Moreover, there is growing support among the engineers of China's monetary policy to expanding the range of the daily trading band beyond the current 0.5 percent, potentially accelerating the rate of appreciation.<sup>41</sup>

Meanwhile, the Chinese government is increasing its efforts to reduce its reliance on the dollar and nudge international debt markets toward the RMB.<sup>42</sup> Last year, McDonald's became the first major multinational to issue an RMB-denominated corporate bond in Hong Kong, referred to by the financial community as *dim sum bonds*, which brought in RMB 200 million at a 3 percent yield.<sup>43</sup> Caterpillar followed with a much larger issue of RMB 1 billion at 2 percent.<sup>44</sup> In March 2011, Unilever paid an even lower yield of 1.15 percent in an issuance of RMB 300 million.<sup>45</sup> Morgan Stanley issued its own RMB 500 million round at 1.625 percent (see table 3, below).<sup>46</sup> Finally, the Chinese Ministry of Finance issued RMB 20 billion of sovereign debt, the largest RMB-denominated bond in history.<sup>47</sup>



**Table 3: RMB Bond Issuances by Multinational Companies, 2010–2011**

	Issuer	Round	Yield
Aug-10	McDonald's	¥ 0.2 bn	3.000%
Nov-10	Caterpillar	¥ 1.0 bn	2.000%
Mar-11	Unilever	¥ 0.3 bn	1.150%
May-11	Morgan Stanley	¥ 0.5 bn	1.625%
May-11	Volkswagen	¥ 1.5 bn	2.000%
Total		¥ 3.5 bn	

Source: Fiona Law et al., “Caterpillar Yuan Bond Issue Draws Strong Demand,” *Wall Street Journal*, November 24, 2010. <http://online.wsj.com/article/SB10001424052748703572404575634532182318468.html>.

¥ = yuan or renminbi

The low yields reflect the lack of alternatives available to Chinese retail investors. Some Chinese commentators have dismissed such corporate bond sales as publicity stunts by multinationals designed to appease the Chinese government. One financial analyst described McDonald's RMB bond as a “McGesture.”<sup>48</sup> Others believe that these issuances are neither about fundraising nor politics but, rather, a method of benefitting from the appreciation of the RMB.<sup>49</sup>

Still, others point out that the fledgling RMB debt market, despite having been in existence for only one year, has already achieved greater liquidity than the well-established debt markets of the Philippines, Indonesia, and Malaysia, with daily trading volume in excess of \$2 billion.<sup>50</sup> To put these numbers into perspective, during the first two quarters of 2011, the U.S. corporate bond market saw \$630 billion of new issuances (RMB 4 trillion), and the average daily trading volume was \$17.3 billion.<sup>51</sup> Thus, the United States maintains an overwhelming lead in the issuance of new corporate bonds but only a modest lead in daily trading volume (see table 4, below).

**Table 4: US and Chinese Corporate Bond Market Activity (\$ billion) 2011 Q1–Q2**

	New Issuances	Daily Trading Volume
US	\$ 630.90	\$ 17.30
China	\$ 0.50	\$ 2.00

Source: Securities Industry and Financial Markets Association (New York, NY).

Meanwhile, a greater share of China's foreign trade is settled in RMB. In the first four months of 2011, cross-border, RMB-denominated trade exceeded the total amount of RMB-denominated trade conducted in all of 2010, 500 billion.<sup>52</sup> Put in relative terms, RMB-denominated trade in the first quarter of 2011 represented 7 percent of China's overall foreign trade.<sup>53</sup> However, according to Yin Jianfeng, a financial researcher with the Chinese Academy of Social Sciences, as of the close of 2010, 80 percent of RMB-denominated trade concerned foreign companies importing into China.<sup>54</sup>



Whereas using RMB to settle export trade helps to alleviate China's problems with foreign exchange, exchange rates, and inflation, using RMB to settle import trade actually aggravates those problems.<sup>55</sup> For example, if IBM uses RMB to settle import trade, it implies that at some time prior to the import transaction, IBM used dollars to buy RMB. It also implies that following the import transaction, the Chinese economy is left with more U.S. dollars and more RMB than before. The increased volume of RMB leads to further inflationary pressure for China, and the increased volume of U.S. dollars has the same effect as purchasing Treasury securities: It artificially decreases the supply of dollars in circulation in the United States, creates greater dollar scarcity, and promotes a low exchange rate with the RMB.

China has also made significant progress toward opening the door to RMB-denominated foreign direct investment (FDI).<sup>56</sup> Chinese policymakers are concerned about the magnitude of RMB deposits in Hong Kong, which stood at RMB 548 billion as of May 2011.<sup>57</sup> In relative terms, this represents 5 percent of the total volume of all RMB in circulation. Liberalizing RMB-denominated FDI on the mainland raises the prospect that some significant percentage of this money would be repatriated into the mainland, where it might go into speculative investments in real estate, thereby creating a bigger bubble.

### China's Role in the WTO

The United States has brought three new, China-related disputes to the WTO since the date of the Commission's last Report. On December 22, 2010, the United States requested consultations with China over its subsidies for domestic manufacturers of wind power equipment (DS419). The European Union (EU) and Japan joined the consultations in January. The case has not yet advanced to the hearing stage. In the second pending case initiated this year, the United States on September 20 requested consultations with China regarding its imposition of antidumping duties on chickens imported from the United States. In addition, on October 6, 2011, the U.S. Trade Representative submitted information to the WTO identifying nearly 200 subsidies that China, in contravention of WTO rules, failed to notify to the WTO.<sup>58</sup>

Three previous WTO cases involving U.S.-China trade are both open and active. The *Raw Materials* case, which resulted in a decision favorable to the United States, is under appeal as of August 31, 2011. The *Flat-rolled Electrical Steel* case and the *Electronic Payments* case have both advanced to formal dispute settlement, though no decision has been reached (see table 5, below).

**Table 5: Open and Active WTO Cases Between the United States and China**

Date Brought	Number	Title	Status
15-Sep-10	DS413	Electronic Payments	Panel established
15-Sep-10	DS414	Flat-rolled Electrical Steel	Panel established
23-Jun-09	DS394	Raw Materials	Under Appeal

Source: World Trade Organization Dispute Settlement Gateway. [www.wto.org](http://www.wto.org).

The United States has brought a total of seven cases against China at the WTO concerning subsidies or grants. Of the seven, four were settled through consultation, two were decided in favor of the United States, and one remains undecided (see table 6, below).

**Table 6: WTO Subsidies Cases Brought by the United States Against China**

<b>Date Brought</b>	<b>Dispute</b>	<b>Short Title</b>	<b>Resolution</b>	<b>Date Resolved</b>
18-Mar-04	DS309	Integrated Circuits	Settled	6-Oct-05
30-Mar-06	DS340	Auto Parts	Holding for US sustained on appeal	15-Dec-08
2-Feb-07	DS358	Taxes	Settled	19-Dec-07
10-Apr-07	DS362	Intellectual Property Rights	Held for US	26-Jan-09
3-Mar-08	DS373	Financial Services	Settled	4-Dec-08
19-Dec-08	DS387	Grants and Loans	No resolution	N/A
22-Dec-10	DS419	Wind Power	Settled	N/A

Source: World Trade Organization Dispute Settlement Gateway. [www.wto.org](http://www.wto.org).

### **China's WTO Probationary Period Ends This Year**

During the negotiations leading up to China's accession, the United States and the European Union expressed concern about potential negative consequences that might befall the WTO due to China's sheer size and lack of a market-based economy.<sup>59</sup> Thus, they insisted on a series of China-specific admission requirements. The centerpiece of this "WTO-Plus" admission package was the Transitional Review Mechanism, which required China to submit to an annual review for the first eight years of its membership in the organization as well as a final review in the tenth year.<sup>60</sup> The Transitional Review Mechanism is in addition to, rather than in lieu of, the normal review procedure, known as the Trade Policy Review Mechanism, which all WTO members must undergo every few years in perpetuity.<sup>61</sup>

On paper, the temporary Transitional Review Mechanism appeared to be more stringent than the Trade Policy Review Mechanism. However, the procedural aspects of the Transitional Review Mechanism rendered it a paper tiger.<sup>62</sup> Reports produced by the Transitional Review Mechanism require the unanimous consensus of all members involved, including China.<sup>63</sup> This puts China in the position of acting as judge in its own trial. According to trade scholars such as William Steinberg, the result consistently has been "light and generally unspecific criticism."<sup>64</sup>

Nevertheless, the Transitional Review Mechanism has provided the United States with a somewhat useful tool for fact-finding and casting attention on controversies within the U.S.-China trade relationship. This is the tenth year of China's membership in the WTO and, therefore, the final year of the Transitional Review Mechanism. The consequences of this are twofold. First, the tools available to the United States to carry out fact-finding related to China's compliance with WTO obligations will now be limited to the

Trade Policy Review Mechanism and the various review channels of individual subsidiary bodies.<sup>65</sup> Second, China's membership in the WTO has reached a point of chronological maturity at which China was expected to be in full compliance with its WTO obligations.

When China initially acceded to the WTO, it accepted the China-specific rules contained in the protocol of accession, avoided litigation within the WTO, and was quick to comply with all demands of the WTO's dispute resolution process. Trade law scholars such as Henry Gao of Singapore Management University have characterized the first several years of China's membership in the WTO as a *rule taker*.<sup>66</sup> But after ten years of observing and learning the subtleties of WTO procedural law, Beijing's behavior has transformed into a *rule shaper*. Beijing has become much more aggressive about bringing claims against trading partners, appealing decisions that are rendered against its favor, and pushing the envelope of noncompliance. Additionally, China has grown very savvy about using the dispute settlement process and bilateral free trade agreements to undermine the effectiveness of China-specific rules.

According to a recent study by international trade law scholars at the University of Hong Kong, of the five WTO cases filed by China between September 2008 and March 2011, four of them were designed to use the dispute settlement process to change or undo rules contained in China's Accession Protocol.<sup>67</sup> These cases purposely turn on vague terminology found in the Accession Protocol. China has exploited this weakness by using a creative interpretation to render entire provisions inapplicable.

Since 2002, China has concluded nine free trade agreements and commenced negotiations for five more.<sup>68</sup> In all 14, a precondition to negotiation has been agreement by the other party to grant China market economy status. These preconditions are targeted toward eliminating certain restrictions placed upon China during accession to the WTO. In particular, when antidumping proceedings are instituted against China, the instituting party is allowed to draw price comparisons from third-party countries, in lieu of China, in order to show dumping behavior by Chinese companies.<sup>69</sup> Similarly, for purposes of identifying illegal subsidies and calculating countervailing measures, the instituting party may act with reference to prices and conditions prevailing in third-party countries in lieu of China.<sup>70</sup> Chinese trade officials view these provisions as a substantial drag on China's freedom of action within the international trading system. Under the terms of the Accession Protocol, however, China's nonmarket-economy status is set to expire in 2016, at which time these provisions will cease to have effect.<sup>71</sup> It must be noted that the expiration in 2016 of China's status as a nonmarket economy under the Accession Protocol does not negate applicable U.S. domestic law, which will continue to have effect beyond 2016.

If enough WTO members accord market economy status prematurely to China, it will diminish support for Washington's position that China has a long way to go to merit market economy status. China has more bargaining power in bilateral negotiations with smaller nations than it does in multilateral negotiations at the WTO. It appears that by pushing for concessions from a series

of bilateral negotiations under the auspices of free trade agreements, China hopes gradually to undermine the Washington consensus, strong-arm its way into market economy status, and shake free of restrictive terms and obligations in its accession agreement.

Moreover, China is not willing to comply fully with the decisions of the WTO dispute settlement process and prioritizes the preservation of its own political system above fidelity to WTO commitments. This can be seen most clearly by examining a recent case study of China's failed compliance with WTO commitments.

### **Stonewalling the WTO: A Case Study in China's Intransigence**

On April 10, 2007, the United States brought a complaint at the WTO alleging that China's state monopoly on imports of cultural products (such as movies, music, and magazines) was inconsistent with China's WTO obligation to permit, within three years of accession, all persons and enterprises, both foreign and domestic, to import and export all goods throughout the territory of China, except for a specific list of products reserved for monopoly by state-owned enterprises (SOEs).<sup>72</sup> The cultural products at issue were not included in the list of exceptions negotiated by China and agreed to by the WTO. Thus, the United States claimed that the continued SOE monopoly over importing cultural products constitutes a violation of China's obligations. China attempted to defend itself by invoking Article XX(a) of the General Agreement on Tariffs and Trade, which allows members to adopt or enforce measures "necessary to protect public morals." China claimed that censorship of imported cultural products is critical to protecting public morals and that only SOEs could be relied upon to carry out censorship, therefore SOE monopoly on importation of cultural products should be allowed under the General Agreement on Tariffs and Trade.

The United States responded to this defense by proposing an alternative arrangement, which was to allow all persons and entities to import cultural products but require them to submit to China's Central Propaganda Department for censorship of each individual import. China rejected this proposal on the grounds of cost. Under the status quo, SOEs practice self-censorship, which leaves the workload of the Central Propaganda Department quite limited. Under the U.S. proposal, the Central Propaganda Department's workload would increase dramatically, thus requiring a significant expansion of payroll. On August 12, 2009, the dispute panel issued a ruling rejecting China's defense, finding that the U.S. proposal constituted a reasonable alternative to the status quo and mandating China to modify its policies accordingly. China appealed, and the appellate body upheld the ruling. China then announced its intention to comply with the ruling but requested a reasonable period of time to do so. In July 2010, the United States and China reached an agreement to set a deadline of March 19, 2011, for implementation.

**Stonewalling the WTO: A Case Study in China's  
Intransigence—Continued**

On March 19, 2011, the State Council of China published amendments to the *Regulations on the Management of Publications* and the *Regulations on the Management of Audiovisual Products*.<sup>73</sup> The effect of the amendments was to eliminate the requirement that importers be SOEs and, instead, create a process whereby any individual or entity, private or public, foreign or domestic, can apply to the Central Propaganda Department for a license to import cultural products. Because the government still retains unbridled discretion over which applications will be approved and which will be denied, in practical terms the amendments were empty and meaningless. The new process could just as well be used to grant licenses only to SOEs. Indeed, there is no record of any non-SOE receiving a license under the new rule. For this reason, scholars of international trade have opined that the March 2011 amendments fell far short of what would be required to constitute full compliance with the ruling in this case or the protocol commitment on which it was predicated.<sup>74</sup> Procedurally, the United States has the right to initiate further WTO proceedings to compel compliance or issue sanctions.

The full importance of this development becomes clearer in light of two elements. First, the issue in this case was not whether China should be allowed to practice censorship. The issue was whether China's self-professed censorship imperative is sufficient grounds to justify a state monopoly on importation of cultural products. Contrary to China's public insistence, the real reasons why China rejected the U.S. proposal have nothing to do with cost. First, China wishes to protect its domestic filmmaking industry. Second, adopting the U.S. proposal would set in motion a process that would destroy the effectiveness of China's censorship regime.<sup>75</sup> The reasoning behind this claim bears brief explanation.

The Central Propaganda Department relies upon SOEs to practice self-censorship. The department frequently sends notifications to the SOEs advising them which topics are politically sensitive, which news stories to delete, etc. Those notifications are actually considered state secrets, and publication can lead to severe punishment.<sup>76</sup> If the notifications were available to the public, it would undermine the censorship regime by creating a demand for the forbidden fruit. Additionally, by limiting the circulation of the notifications to SOEs and party members, the Central Propaganda Department retains maximum flexibility in what is considered off limits. If the U.S. proposal were adopted, then each time the Central Propaganda Department would reject a particular import, the private party applying to import that product would have actual knowledge of the fact that the product is being censored. Given the high degree of interaction between importers and the outside world, there would be no effective way to contain the spread of this knowledge. Moreover, private importers, particularly foreign importers, would demand some degree of predictability, which would necessarily come at the expense of the flexibility of the Central Propaganda Department.



**Stonewalling the WTO: A Case Study in China's  
Intransigence—Continued**

In sum, if the Central Propaganda Department were required to liaise with private parties, as the U.S. proposal called for, the genie would be let out of the bottle, and the subversion of the censorship regime would only be a matter of time.<sup>77</sup> For this reason, the WTO's decision in the *Publications* case, and China's failure to honor the decision, is critically important. It suggests that in cases of conflict between internal political preferences and international trade commitments, China will choose the former over the latter.

**Implications for the United States**

The U.S. trade deficit with China has ballooned to account for more than half of the total U.S. trade deficit with the world and creates a drag on future growth of the U.S. economy. This problem has many causes, among which are barriers to U.S. exports and continued undervaluation of the RMB. The result is lost U.S. jobs.<sup>78</sup> While the exact number of U.S. jobs lost to China trade is hotly disputed—economist C. Fred Bergsten has estimated 600,000 jobs on the low end, while the Economic Policy Institute has estimated 2.4 million jobs on the high end—many parties agree that the costs are staggering.<sup>79</sup>

Although the RMB has appreciated by roughly 6 percent over the course of the last year, there is widespread agreement among economists that it remains deeply undervalued. As a result, U.S. exports to China remain subject to a de facto tariff, Chinese exports to the United States remain artificially discounted, and Chinese household consumption remains suppressed. This contributes to a persistent pattern of massive and dangerous trade distortions, unnatural pools of capital, and dangerous inflationary pressures that threaten the stability of the global economy.

Gone are the days when Beijing was content to be the low-end factory of the world. The central planners behind China's economy are intent on moving up the value chain into the realm of advanced technology products, high-end research and development, and next-generation production. This ambition will come at the expense of America's high-technology industries.

Similarly, it no longer seems inconceivable that the RMB could mount a challenge to the dollar, perhaps within the next five to ten years. Chinese financial authorities are laying the groundwork for these ambitions via a series of bilateral arrangements with foreign companies and financial centers. While dollar-denominated financial markets retain a substantial advantage over their RMB-denominated counterparts in terms of new issuances, the RMB markets have made remarkable progress in less than one year to achieve 11 percent of the daily trading volume of dollar-denominated markets. Still, of the \$4 trillion that is traded each day in international currency markets, trade in RMB accounts for only 0.3 percent. The dollar is one side of 85 percent of all currency trades.<sup>80</sup>



Finally, the Chinese government is growing increasingly assertive in international fora such as the WTO. The United States and the European Union went to considerable lengths to design and negotiate a system of checks and balances that would permit China to accede to the WTO without jeopardizing the smooth functioning of the organization or endangering the position of existing members in the international trading system. From start to finish, that negotiation process took 15 years. In less than ten years, China has learned the nuances of WTO law and has begun to use it systematically to undo the finely wrought balance that U.S. and EU negotiators designed. At the same time, China has shown that it will subordinate its international commitments to its domestic political preferences and deny to its trading partners the benefit of their bargain.

### **Conclusions**

- The U.S.-China trade deficit in 2010 set a record high of \$273 billion. The U.S.-China trade deficit now accounts for more than 50 percent of the total U.S. trade deficit with the world.
- Over the last 12 months, the RMB has appreciated by 6 percent. Economists estimate, however, that it remains substantially undervalued. There is increasing grassroots pressure in China to widen the trading band of the RMB and increase the pace of appreciation.
- The Chinese economy, generally, and Chinese exports, in particular, are moving up the value chain. On a monthly basis, the United States now imports roughly 560 percent more advanced technology products from China than it exports to China. Exports of low-cost, labor-intensive manufactured goods as a share of China's total exports decreased from 37 percent in 2000 to 14 percent in 2010.
- China's foreign currency reserves are skyrocketing. A major contributor to this phenomenon is China's continued policy of maintaining closed capital accounts. China's foreign currency reserves currently exceed \$3 trillion, three times higher than the next largest holder of foreign currency reserves, Japan.
- Commensurate with growth in foreign currency reserves, China's domestic money supply is ballooning out of control. Between 2000 and 2010, China's money supply grew by 434 percent. China's money supply is now ten times greater than the U.S. money supply, despite the fact that China's GDP is only one-third as large.
- Such rapid growth in China's domestic money has created strong inflationary pressure. This has helped create a real estate bubble, which resulted in price increases of more than 100 percent in some cities within a handful of years. In September, China's consumer price index topped 6.1 percent across the board and higher in rural areas.
- China has grown more assertive and creative in using WTO procedures to alleviate, eliminate, and avoid certain restrictions in the Accession Protocol. At the same time, the WTO has ruled

that China's existing system of state monopoly over imports of cultural products is inconsistent with WTO obligations. China has not yet complied fully with the WTO ruling, and the United States has the right to initiate further proceedings to compel China to do so.

## **SECTION 2: CHINESE STATE-OWNED ENTERPRISES AND U.S.-CHINA BILATERAL INVESTMENT**

### **Introduction**

The state's influence over China's economy takes many forms and covers a whole spectrum of companies from fully state owned to those that are nonstate but maintain close ties to the government. China's state-owned and state-controlled companies and industries are generally the largest ones in China and are operated and managed by the central government of the People's Republic. They are an instrument of state power as well as the centerpiece of China's industrial policy. They receive massive government subsidies and are protected from foreign competition. In addition, there are more than 100,000 smaller companies that are owned or operated by provincial and local governments. These companies also receive many benefits from their government ownership.

Because China's regulatory systems are opaque, it can be difficult to trace the real ownership of any enterprise in China. Though the number of state-owned companies has declined following years of reform and privatization, they continue to dominate major sectors of the economy, and in many sectors they have become stronger. There are also millions of firms whose ownership is unclear. These include enterprises where the state holds some, though not all, assets; joint venture arrangements involving state-owned enterprises (SOEs), private and semiprivate companies and foreign entities; and companies that, while nominally private, are still subject to the influence of the state because they are in the sectors the government has deemed strategically important.

During the 2011 hearing cycle, the Commission undertook a thorough examination of China's industrial policies, particularly the government's control of China's economy. In addition, this section examines the bilateral investment flows between the United States and China, where a new pattern is emerging. Flush with export profits and foreign exchange reserves, China is starting to flex its investor muscles. Though the cumulative Chinese investment in the United States remains very small, recent trends indicate a potential for great growth. This section will examine this and other issues and will conclude with the implications for the United States of the continued dominance of the Chinese economy by the state and of the growth in bilateral investment.

### **Chinese State-owned Enterprises**

In its 2004 Report to Congress, the Commission noted that:

*China was not a market-based economy at the time of its accession to the WTO [World Trade Organization] nor is it*

*now. Because the structures of the WTO rely on the functioning of market-based economies, China's accession required a unique agreement allowing China's early entry in exchange for firm commitments to implement a broad range of legal and regulatory reforms as well as tariff reductions. China also agreed to special safeguard mechanisms that other WTO members could utilize to protect domestic industries significantly injured by surges of imports from China's nonmarket economy. Assuring that China implements its WTO commitments is a large and important task for the U.S. government.*<sup>81</sup>

Ten years after joining the WTO, China has taken significant steps toward economic liberalization in order to meet the many obligations it assumed upon accession to the 153-member organization. But the process has reversed in the past five years. Rather than continue along a path of market reforms, Beijing has indicated that it has no intention of giving up direct command over large portions of the economy or of relinquishing its ownership of key industrial, financial, and high-technology sectors. China's approach is particularly apparent in the government's retention of control over a large number of SOEs and other state-favored actors and its strengthening of them through subsidies and other policies to create dominant domestic and global competitors.

The consolidation and concentration of power in a group of 121 very large SOEs represents a reversal of a trend toward reducing government control of the economy and greater market openness that had been the hallmark of China's economic policy since the 1978 reforms of Deng Xiaoping.\* Though this shift has been gathering strength for half a decade, it has accelerated as a consequence of China's large-scale stimulus in 2008–2009, which directed massive loans from the state-owned banks to many state-owned companies. In 2009 alone, of the 9.59 trillion renminbi (RMB) (\$1.4 trillion) in bank loans, 85 percent were granted to SOEs.<sup>82</sup> Meanwhile, China's less-favored private sector is struggling to compete. The trend has given rise to a catch-phrase among Chinese entrepreneurs: “The state advances, the private [sector] retreats.”<sup>83</sup>

In its annual review of China's compliance with its obligations, the WTO reported in 2010 that SOEs have been “benefitting disproportionately from the [g]overnment's recent measures to boost the economy, particularly the economic stimulus. At the same time, domestic private enterprises are finding it more difficult to access credits from banks.”<sup>84</sup>

The government also gives SOEs a variety of subsidies and favorable access to credit. The June 2010 *China Quarterly Update* from the World Bank shows SOEs crowding out private enterprises, following the introduction of the economic stimulus, which was heavily weighted toward the construction and infrastructure sectors already dominated by SOEs.<sup>85</sup> By some estimates, local governments established 8,000 state-owned investment companies in 2009 alone

\*A list of major companies owned by the central government appears in Addendum I: SASAC [State-owned Assets Supervision and Administration Commission] Companies, Large State-owned Banks, and Insurance Companies (2011).

to take advantage of central government financing for business and industrial deals.<sup>86</sup> The World Bank also noted that a decline of the role of the SOEs in the Chinese economy earlier in the decade has reversed in recent years.<sup>87</sup> Two experts on China's industrial policy, Victor Shih of Northwestern University and Yasheng Huang of the Massachusetts Institute of Technology, have also noted that some of the reforms introduced in the past two decades to promote China's private sector are now being undone by the shift of government support to the state-owned sector.<sup>88</sup>

### ***Overview of the Chinese State-owned Sector***

The Chinese government continues to eliminate or consolidate the least profitable SOEs.<sup>89</sup> As a result, the current group of operating SOEs is composed primarily of very large and comparatively more profitable SOEs than in the past.<sup>90</sup> The number of Chinese SOEs, at both the central and provincial levels, has decreased significantly since 2000 as part of a policy to “grasp the big, let go of the small.”\* The overall effect has been to reduce the number of companies under government control while strengthening the remainder in order to produce global competitors to European-, American-, and Japanese-based multinationals.<sup>91</sup> This goal is part of an effort to create “national champions.” The WTO noted in its 2010 *Trade Policy Review of China* that:

*‘guided’ by the State Council’s Opinions issued in December 2006, SOEs have been retreating from some of the more competitive industries, but remain concentrated in other industries with a state monopoly. . . . The associated monopoly position gives these SOEs competition advantage over private enterprises. Profits of SOEs continued to rise (they increased by 9.8 [percent] in 2009).<sup>92</sup>*

The largest 121 nonfinancial companies owned by the central government<sup>93</sup> are supervised by the government equivalent of a holding company, the State-owned Assets Supervision and Administration Commission (SASAC), which reports to the State Council.† These, however, typically each have dozens of subsidiaries, “including nearly all the Chinese companies most people are familiar with,” according to testimony before the Commission by economist Derek Scissors of The Heritage Foundation.<sup>94</sup> There are an additional 114,500 SOEs owned by provincial and municipal governments, according to World Bank estimates.<sup>95</sup> Meanwhile, truly private firms number in the millions, though they are comparatively very small in size. There are also millions of firms whose ownership is unclear.<sup>96</sup>

\*The “grasp the big, let go of the small” policy, adopted by the Communist Party Congress in 1997, remains the guiding principle for SOE restructuring. These reforms included efforts to corporatize SOEs and to downsize the state sector. The “grasp the big” component indicated that policymakers should focus on maintaining state control over the largest and most important SOEs, which were typically controlled by the central government. “Let go of the small” meant that the central government should relinquish control over smaller SOEs through a variety of means (e.g., giving local governments authority to restructure the firms, privatizing them, or shutting them down). See Barry Naughton, *The Chinese Economy: Transitions and Growth* (Cambridge, MA: MIT Press, 2007), pp. 301–302.

†The State Council of the People's Republic of China is the chief administrative authority of the People's Republic of China. It is chaired by the premier and includes the heads of each governmental department and agency. For more information, see *People's Daily Online*, “The State Council,” <http://english.peopledaily.com.cn/data/organs/statecouncil.shtml>.

### How Big Is China's State Sector?

The opaque nature of ownership makes estimating the SOEs' share of China's gross domestic product (GDP) difficult. There is no definitive published value for SOEs. A 2011 study prepared for the Commission has noted that:

*The Chinese government publishes several statistical measures which can be used to assess the size of state-owned enterprises relative to other forms of ownership according to various dimensions. In many cases, the measures of SOE activity consider only wholly-owned SOEs. That is, these SOE measures do not treat entities in which the state ownership share is less than 100 percent, but greater than 50 percent, as being state-owned. Further, the official estimates often do not track ultimate ownership, thereby ignoring enterprises that are not registered as SOEs or state controlled enterprises even when indirect state ownership is present.*<sup>97</sup>

In other words, in official statistics, the SOE category includes only wholly state-funded firms. This definition excludes shareholding cooperative enterprises, joint-operation enterprises, limited liability corporations, or shareholding corporations whose majority shares are owned by the government, public organizations, or the SOEs themselves.<sup>98</sup> A more encompassing category is "state-owned and state-holding enterprises." This category includes state-owned enterprises plus those firms whose majority shares belong to the government or other SOE.<sup>99</sup> This latter category, also referred to as state-controlled enterprises, can also include firms in which the state- or SOE-owned share is less than 50 percent, as long as the state or SOE has a controlling influence over management and operations.<sup>100</sup>

A 2009 study by the Organization for Economic Cooperation and Development (OECD), using data from 2006, estimated the SOE share of China's gross domestic product (GDP) to be 29.7 percent, implying that the nonstate sector is about 70 percent of the economy.<sup>101</sup> However, this does not mean that the private sector accounts for the remaining 70 percent of China's economy (see box on China's private sector). In his testimony before the Commission, Dr. Scissors suggested that the state sector accounts for 30 to 40 percent of China's economy.<sup>102</sup>

A study prepared for the Commission in 2011, which used various economic measures to estimate the true economic footprint of the Chinese state has concluded that the state's share of the economy exceeds 50 percent:



**How Big Is China's State Sector?—Continued**

*The observable SOE sector under reasonable assumptions accounts for nearly 40 percent of China's economy. Given additional information on the prevalence SOE ownership in China's capital markets, anecdotal and observed data on the prevalence of SOE ownership among [limited liability corporations] and other ownership categories, the likely SOE role in round-tripped FDI [foreign direct investment], it is reasonable to conclude that by 2009, nearly half of China's economic output could be attributable to either SOEs, [state-holding enterprises], and other types of enterprises controlled by the SOEs. If the output of urban collective enterprises and the government-run proportion of [township and village enterprises] are considered, the broadly defined state sector likely surpasses 50 percent.*<sup>103</sup>

The national or central SOEs can be further categorized. The first major grouping is the SASAC companies, which consist of the companies that provide public goods such as defense, communication, transportation, and utilities; the firms that specialize in natural resources such as oil, minerals, and metals; and the enterprises that concentrate on construction, trade, and other industrial products. The SASAC companies are the largest among these three groupings of national SOEs, despite the fact that the total number of the SASAC companies has fallen significantly over the past few years—from 196 in 2003 (when the SASAC was established) to 121 in 2010—as a result of mergers and acquisitions among themselves intended to enlarge and strengthen several flagship companies. The total assets of the SASAC companies, however, increased from 3 trillion RMB (about \$360 billion) in 2003 to 20 trillion RMB (about \$2.9 trillion) in 2010.<sup>104</sup> (According to the National Bureau of Statistics of China, in 2003 and 2010, China's GDP was \$1.64 trillion and \$5.88 trillion, respectively.)

The second grouping includes the companies that specialize in banking, finance (securities), and insurance under the administration of the China Banking Regulatory Commission (CBRC),<sup>105</sup> the China Securities Regulatory Commission (CSRC), and the China Insurance Regulatory Commission (CIRC),<sup>106</sup> respectively.

The third grouping consists primarily of companies specializing in broadcast media, publications, culture, and entertainment. These are administrated by the various agencies under the State Council and national mass organizations such as the All-China Federation of Trade Unions, which is itself controlled by the Chinese Communist Party (CCP).<sup>107</sup>

Most of these large companies are horizontally integrated and engaged in business activities that include more than one industry. Many of them are concentrated in the industries that are largely controlled by the state, but not exclusively.<sup>108</sup> For example, the SASAC reported in 2010 that about 74 percent of the SASAC-run companies are engaged in the real estate business.

In 2010, of 42 mainland Chinese companies listed in the Fortune Global 500, all but three were state owned.<sup>109</sup> By revenues, three Chinese state-owned companies ranked among the top ten in the

Fortune Global 500, compared to just two American companies.<sup>110</sup> China's own list of the 500 biggest Chinese companies showed that among the top 100 firms traded on the stock exchange, the government controlled the majority of the stock in 75.<sup>111</sup>

### **Chinese SOEs and Government Procurement**

The U.S. government has taken the position that China's SOEs as well as provincial and local government agencies should be considered as part of the Chinese government when procurement decisions are being made. China has responded by insisting that central, provincial, and local SOEs, and provincial and local government agencies should not be considered as part of the government under the WTO's Agreement on Government Procurement (GPA). This would allow China to limit foreign companies' access to the lucrative procurement market. A country's accession to the GPA is subject to negotiation between the applicant and GPA members. China's refusal, so far, to include SOEs has been one of the impediments to China's accession to the 40-member GPA, despite China's promise in 2001 that it would sign the GPA "as soon as possible."

By refusing to consider China's state-owned sector as part of the government, China seeks to wall off a large portion of its economy from the GPA rules that members have agreed to abide by. These rules generally ensure foreign companies equitable access to central and local government procurement for goods and services. By seeking to exclude foreign firms from government and SOE contracts, China puts U.S. manufacturers and service providers at a disadvantage.

China's latest offer to join the GPA was issued in July 2010. While the latest offer made certain improvements, there remained significant shortcomings. For example, while the new offer expanded the coverage of central government entities, it still would not cover provincial or local government agencies or SOEs.<sup>112</sup> In 2009, the Chinese government estimated that its procurement market surpassed \$100 billion, but this is a significant understatement of its true size. For example, the Chinese Ministry of Finance's limited definition of government procurement spending does not include most government infrastructure projects, and procurement by SOEs is not included, even when SOEs perform government functions.<sup>113</sup> Factoring in all of these considerations, the European Union Chamber of Commerce in China estimates the size of China's government procurement market at \$1 trillion.<sup>114</sup>

**Chinese SOEs and Government Procurement—Continued**

The issue of Chinese SOE procurement is further complicated by the fact that projects undertaken by SOEs fall under the China Bidding Law rather than China's government procurement law, notes Gilbert Van Kerckhove, chairman of the Public Procurement Working Group of the European Chamber of Commerce. The China Bidding Law covers construction projects in China, including surveying and prospecting, design, engineering, and supervision of such projects, as well as procurement of major equipment and materials related to the construction of such projects—in other words, all projects, massive in scope and value, that are of significant interest to foreign companies.<sup>115</sup>

Membership in the WTO Agreement on Government Procurement is voluntary; a country can be a WTO member without ever acceding to the agreement. Until China signs the agreement, it is not a WTO violation for China to discriminate against foreign goods or services in its government procurement nor for other WTO members to discriminate against Chinese goods and services in their government purchases.

The Chinese state-owned sector derives important advantages from its government affiliations. China's largest banks are state owned and are required by the central government to make loans to state-owned companies at below market interest rates and, in some cases, to forgive those loans. Dr. Scissors testified at the Commission's March 30, 2011, hearing that every aspect of the financial system is dominated by the state:

*All large financial institutions are state-owned, the People's Bank assigns loan quotas every year, and, within these quotas, lending is directed according to state priorities. Interest rates are also controlled, and last year real borrowing costs were barely above zero. Conveniently, then, loan quotas and bank practices strongly inhibit nonstate borrowing. Securities markets are also dominated by the state. As an illustration, the volume of government bond issuance utterly dwarfs corporate bonds and is growing relentlessly, crowding out private firms.*<sup>116</sup>

According to a 2011 study by the Beijing think tank Unirule Institute of Economics, the profits of state-owned industrial companies had increased nearly fourfold between 2001 and 2009, but their average return on equity was less than 8.2 percent, versus 12.9 percent for larger, nonstate industrial enterprises.<sup>117</sup> As more evidence that SOEs enjoy special advantages over private sector companies, Unirule found that the average annual interest rates charged to SOEs were 1.6 percent from 2001 to 2008, while those charged to private companies during the same period were 5.4 percent.<sup>118</sup> During that period, according to the report, subsidies to SOEs amounted to 6 trillion RMB—more than the profits generated by the companies. A 2009 study on Chinese subsidies prepared for the Commission likewise concluded that state-owned com-

panies are less profitable, after adjusting for the cost of subsidies.<sup>119</sup>

Low interest loans, debt forgiveness, and access to credit are among the methods the government uses to subsidize its business sector.<sup>120</sup> Some of the other subsidies, frequently administered through the provincial and municipal governments, include regulatory barriers to competitor entry, special treatment from regulatory compliance monitors,<sup>121</sup> tax breaks,<sup>122</sup> preference in land allocation,<sup>123</sup> bankruptcy alternatives,<sup>124</sup> and de facto debt forgiveness.<sup>125</sup>

### ***State Control vs. Private Control***

The extent of the state's control of the Chinese economy is difficult to quantify. In addition to the companies held directly by the central government or local government (see above), there are a variety of enterprises whose ownership is unclear. A common mistake is to assume that any entity that is not an SOE belongs to the private sector.<sup>126</sup> In reality, the nonstate sector includes firms with other forms of ownership, including purely private ownership by domestic and foreign actors and mixed ownership entities in which SOEs are part owners and/or controlling owners.<sup>127</sup> There is also a category of companies that, though claiming to be private, are subject to state influence. Such companies are often in new markets with no established SOE leaders and enjoy favorable government policies that support their development while posing obstacles to foreign competition. Examples include Chinese telecoms giant Huawei and such automotive companies as battery maker BYD and vehicle manufacturers Geely and Chery.<sup>128</sup>

### **A Private Sector with Chinese Characteristics**

China's National Bureau of Statistics defines private enterprises as "economic units invested or controlled (by holding the majority of the shares) by natural persons who hire laborers for profit-making activities."<sup>129</sup> Included in this category are private limited liability corporations, private share-holding corporations, private partnership enterprises, and private sole investment enterprises. Estimating the contribution of the private sector to China's economy is hampered by the same data problems affecting the state-controlled sector. The difficulty stems, too, from the fact that much of China's private sector is informal and exists in the gray area of mom-and-pop shops and subcontracting factories with ambiguous legal standing.

Some estimates are available, however. According to a 2011 China Europe International Business School study, China has 8.4 million private enterprises, accounting for 74 percent of the country's total number of firms.<sup>130</sup> A 2011 study on the Chinese state-owned sector prepared for the Commission had several estimates of the size of China's private sector (from 20 percent to 38.5 percent of the economy), based on various alternative indicators, including gross output value and fixed-asset investment.<sup>131</sup>

**A Private Sector with Chinese Characteristics—Continued**

Regardless of the total number of private enterprises, the state-owned or -controlled sector still dwarfs the private sector in size, with the average listed private company generating only about 25 percent of the total net profit of an average listed state-owned firm.<sup>132</sup> The rest of the economy is characterized by mixed and joint ownership arrangements and involves Chinese state-owned and private firms, as well as foreign enterprises. Even the firms that appear to be fully private, however, still are frequently subject to state interference.

In the mid-2000s, after more than 30 years of opening up the economy to private enterprise, the Chinese government reversed the policy, and the state began to reassert its economic control. In December 2006, the SASAC and China's State Council jointly announced the "Guiding Opinion on Promoting the Adjustment of State-Owned Capital and the Reorganization of State-Owned Enterprises." The guiding opinion identifies seven "strategic industries" in which the state must maintain "absolute control through dominant state-owned enterprises" and five "heavyweight" industries in which the state will remain heavily involved (see the box below).<sup>133</sup>

**Industries that the Chinese Government Has Identified as "Strategic" and "Heavyweight"**

**Strategic Industries:**

- 1) Armaments
- 2) Power Generation and Distribution
- 3) Oil and Petrochemicals
- 4) Telecommunications
- 5) Coal
- 6) Civil Aviation
- 7) Shipping

**Heavyweight Industries:**

- 1) Machinery
- 2) Automobiles
- 3) Information Technology
- 4) Construction
- 5) Iron, Steel, and Nonferrous Metals

This list "omits state dominance in banking, insurance, and the rest of finance, media, tobacco, and railways," which had long been owned by the government in China.<sup>134</sup>

Although the state's share of the economy has fallen since the start of the reforms, the government has kept these key industries for SOEs. The turn away from privatization was codified in 2011 by Wu Bangguo, chairman and CCP secretary of the Standing Committee of the National People's Congress, when he listed privatization with other intolerable developments:

*We have made a solemn declaration that we will not employ a system of multiple parties holding office in rotation; diversify our guiding thought; separate executive, legislative and judicial powers; use a bicameral or federal system; or carry out privatization [emphasis added].*<sup>135</sup>

Foreign companies are not allowed to participate in the markets reserved for strategic industries and are heavily regulated in those designated for the heavyweight industries. "The requirement that the state predominate in so many sectors is meant to sharply confine competition, so that SOEs operate within markets but they op-



erate primarily within state-controlled markets,” said Dr. Scissors at a Commission hearing. “This regulatory protection is the most powerful subsidy many SOEs receive.”<sup>136</sup>

Under the “grasp the big, let go of the small” policy, scores of state companies have listed their shares on foreign stock exchanges, while the Chinese government has kept about 70 percent to 80 percent of the equity in its own hands (see Addendum I for a list of the central Chinese SOEs). Many foreign observers “often mistook these sales of minority stakes to be privatization,” because they assumed that the listing covered the entire ownership of the company. But the ultimate control remained in the hands of the state.<sup>137</sup> In addition, many companies in China whose stocks are traded on China’s exchanges are also SOEs in which the government keeps a majority stake. By offering only a limited portion of ownership of an SOE on domestic exchanges, the Chinese government is able to raise capital and still maintain control of the firm. As Dr. Scissors testified before the Commission:

*Neither specification of share-holders nor sale of stock by itself does anything to alter state control. The large majority of firms listed on domestic stock markets are specifically designated as state-owned. The sale of small minority stakes on foreign exchanges could be construed as recasting mainstays such as CNPC [China National Petroleum Corporation] (through its list vehicle PetroChina), China Mobile, and Chinalco as nonstate entities of some form. However, they are still centrally directed SOEs, as explicitly indicated by the Chinese government.*<sup>138</sup>

Moreover, the biggest private companies often get their financing from state banks and coordinate their investments with the government.<sup>139</sup>

Some analysts now believe that many of the early Chinese market liberalization reforms are being reversed. Zhiwu Chen of Yale University said during a presentation at The Brookings Institution that SOEs are crowding out private firms from various industries.<sup>140</sup> “The problem is that the reforms of the first 20 years, from 1978 to the end of the ’90s, actually did not touch on the power of the government,” said Yao Yang, a Peking University professor who heads the China Center for Economic Research. “So after the other reforms were finished, you actually find the government is expanding, because there is no check and balance on its power.”<sup>141</sup>

#### **Political Power of the State-owned Company Sector**

While provincial chiefs, cabinet ministers, and military leaders constitute the bulk of the Chinese Communist Party, SOEs are an increasingly significant cultivating ground for party leadership. There are currently 17 prominent political leaders who have held management positions in large SOEs, and 27 prominent business leaders currently serve on the 17th CCP Central Committee or the Central Commission of Discipline Inspection.<sup>142</sup>



**Political Power of the State-owned  
Company Sector—Continued**

The most recent manifestation of this trend came with the announcement, in March 2011, that China Petroleum and Chemical Corporation (Sinopec) Chairman Su Shulin was set to become the next governor of Fujian Province. The *Financial Times* noted that “China’s oil companies have been a breeding ground for state leaders, including current security chief Zhou Yongkang, formerly at CNPC. It is not uncommon for the heads of major Chinese state-owned companies to move in and out of government, and the role of energy companies underscores the role that China’s state-owned oil companies play in national security.”<sup>143</sup>

According to Cheng Li, senior fellow at The Brookings Institution, while the proportion of China’s large enterprises in the national leadership is still relatively small, the rise of state entrepreneurs may broaden the “channel of political recruitment” in China and become a new source of the CCP leadership.<sup>144</sup>

**U.S. Investment in China**

Over the past three decades, China has been the largest recipient among developing countries of FDI,\* with a cumulative \$854 billion (stock)† by 2008. In just 2010 alone, the amount of FDI flowing into China jumped to \$105.7 billion, up from \$90 billion in 2009.<sup>145</sup> “In the modern history of economic development, no other country has ever benefitted, and continues to benefit, from FDI as much as China,” notes a study by Yuqing Xing of the National Graduate Institute for Policy Studies in Tokyo.<sup>146</sup> The study estimates that “foreign-invested firms have been the major contributor to [China’s] drastic export expansion” and have accounted for 40 percent of China’s GDP since 1978.<sup>147</sup> “It is the technologies, product designs, brand names and distribution networks of multinational enterprises that have removed hurdles to made-in-China products, helped these products enter the world market, and strengthened the competitiveness of Chinese exports,” notes Dr. Xing’s study.<sup>148</sup>

\* FDI is investment to acquire a “long-term relationship and reflecting a lasting interest and control” in an enterprise operating in an economy other than that of the investor. It is the sum of equity capital, reinvestment of earnings, other long-term capital, and short-term capital as shown in the balance of payments. There are two types of FDI: inward FDI and outward FDI, resulting in a *net FDI inflow* (positive or negative) and stock of FDI, which is the cumulative number for a given period. FDI excludes most portfolio investment, which is usually investment through the purchase of shares of an insufficient number to allow control of the company or its board of directors. A foreign direct investor may acquire voting power or control of an enterprise through several methods: by incorporating a wholly owned subsidiary or company (e.g., a “greenfield” investment); by acquiring shares in an associated enterprise; through a merger or an acquisition of an unrelated enterprise; or by participating in an equity joint venture with another investor or enterprise. For more information, see UNCTAD [United Nations Conference on Trade and Development], *World Investment Report 2010: Investing in a Low Carbon Economy* “Methodological Note” (New York and Geneva: United Nations, 2010); and World Bank, “Foreign Direct Investment.” <http://data.worldbank.org/indicator/BX.KLT.DINV.CD.WD>.

† FDI stock is the cumulative value of the capital and reserves attributable to the parent enterprise (the investor). FDI flows comprise capital provided by a foreign direct investor to an FDI enterprise, or capital received from an FDI enterprise by a foreign direct investor (these data are commonly compiled for a given period, usually per annum). For details, see UNCTAD [United Nations Conference on Trade and Development], *World Investment Report 2010: Investing in a Low Carbon Economy* “Methodological Note” (New York and Geneva: United Nations, 2010). [http://www.unctad.org/en/docs/wir2010meth\\_en.pdf](http://www.unctad.org/en/docs/wir2010meth_en.pdf).

The largest FDI to mainland China flows through or from Hong Kong, with \$67.5 billion in 2010, according to official Chinese statistics. This represents more than half of the total FDI inflows in 2010. The Ministry of Commerce of the People's Republic of China reported that in 2010 the United States came in fifth among nations investing directly in China, with \$4.1 billion, which represents only 3.8 percent of total inflows.<sup>149</sup> In recent years, tax haven economies such as the Virgin Islands and the Cayman Islands have become more and more prominent as sources of FDI into China, although they are not believed to be the source of the actual investment. The large proportion of FDI flowing into China from Hong Kong and other tax havens can be attributed to round-tripping, the practice of taking money out of China and then “investing” it back as new investment in order to qualify for special tax breaks and other incentives reserved for foreign investment.<sup>150</sup>

**Table 1: U.S. FDI to China, 2000–2010**  
(U.S. \$ million)

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
<b>Flow</b>	1,817	1,912	875	1,273	4,499	1,955	4,226	5,243	15,971	-7,853	\$9,565
<b>Stock</b>	11,140	12,081	10,570	11,261	17,616	19,016	26,459	29,710	52,521	49,403	60,452

Source: U.S. Bureau of Economic Analysis, *U.S. Direct Investment Abroad: Balance of Payments and Direct Investment Position Data* (various years) (Washington, DC: U.S. Department of Commerce).

Official U.S. statistics show that U.S. cumulative FDI in China was \$60.5 billion in 2010 (stock), a 22 percent increase from 2009 (see table 1, above).<sup>151</sup> This represents only 1.7 percent of the total U.S. FDI abroad. Of the U.S. FDI in China, the bulk was in manufacturing, with 48.8 percent in 2010 (for a complete breakdown of U.S. FDI in China by Industry, see Addendum II). As with other statistics, the official U.S. and Chinese figures on U.S. investment in China do not match; the situation is similar for official statistics on Chinese FDI in the United States (see below). According to the U.S. Commerce Department's Bureau of Economic Analysis, U.S. majority-owned nonbank affiliates in China employed 774,000 workers in China in 2008 (latest figures available).<sup>152</sup> A significant number of people are also employed by joint ventures formed by U.S. companies with Chinese partners, though those figures are difficult to track.

The relative amount that Americans contributed to the Chinese pool of direct investment is not immediately clear from the raw statistics. The United States was an early investor in China, so its investment, still registered as book value, has had more time to appreciate in value. In addition, U.S. companies often reinvest profits in productive capacity in China, which does not show up in the statistics as FDI. The comparatively small size of U.S. investment flows to China can also be explained, in part, by the routing of investment by unnamed investors to China through Hong Kong and various tax havens (e.g., the British Virgin Islands, the Cayman Islands, etc.). These nations consistently appear among the top ten investors in China, but they are not the original source of the funds.

Some of the reinvestment of the profits of U.S.-based multinational companies in China is likely done to avoid paying U.S.

corporate income taxes, which come due when a U.S.-based multinational corporation repatriates the profits to the United States. U.S. companies invested abroad face a 35 percent tax rate, one of the world's highest, should they decide to repatriate profits to America. Keeping the money abroad allows a U.S.-based company to avoid the higher U.S. corporate rates. If these funds are reinvested in plant and equipment in China, they face lower rates and, often, additional tax breaks that the Chinese government offers to encourage foreign investment in China. Foreign investment in technology in particular receives special benefits. Such benefits include exemptions from taxes if qualified foreign technology is transferred to China, and a 150 percent tax deduction for foreigners making qualified research and development expenditures in China.<sup>153</sup>

#### **Chinese Government Tax Incentives for Foreign Investment in China**

Prior to 2008, profits of foreign investors in China were taxed at a 15 percent rate, while domestic investors faced a statutory income tax rate of 33 percent.<sup>154</sup> This disparity was eliminated with the implementation of China's 2008 Enterprise Income Tax Law, which saw tax rates unified at 25 percent in 2008. However, existing foreign investors were "grandfathered" in and will continue to receive preferential tax rates until 2012.<sup>155</sup> Many other incentives remain:

- Income from cultivating basic crops and agricultural products (including grain, vegetables, and natural Chinese medicines), animal husbandry, and certain fishery operations is exempt from the Enterprise Income Tax. Income from planting flowers, tea, other beverage crops and spice crops, seawater fish farming, and fresh water fish farming enjoys a 50 percent reduction in the Enterprise Income Tax rate.
- Preferential tax treatment for income earned by enterprises from transfers of technology is extended to foreign-invested enterprises. Specifically, the first 5 million RMB of income earned in a taxable year from transferring ownership of technology is exempted from the Enterprise Income Tax, and any excess amount is allowed to be taxed at one-half the normal 25 percent rate. The preferential tax rate of 15 percent applicable to eligible "high and new technology" enterprises is retained, but only if they receive priority support from the state and possess substantial or key ownership of core proprietary intellectual property rights.
- Enterprises are entitled to an extra income tax deduction of up to 100 percent of the current year's wages paid to disabled employees or other employees whom the state encourages enterprises to hire.

**Chinese Government Tax Incentives for Foreign Investment in China—Continued**

- Additional preferential tax treatment is granted to venture capital enterprises investing in medium- and small-sized high-technology enterprises (a deduction of 70 percent of the total investment is allowed against an enterprise's annual taxable income in the year after its initial two-year holding period) and to enterprises that utilize resources in an environmentally friendly and health-conscious way.

The pre-2008 system providing a host of preferential tax rates for qualified foreign-invested enterprises located in special zones and regions is abolished, with limited exceptions. One special dispensation is that enterprises located in more remote areas where the state has encouraged development (the Western Development Region) seemingly will continue to enjoy concessionary tax rates.<sup>156</sup>

According to the U.S. Trade Representative's (USTR) *2010 Report to Congress on China's WTO Compliance*, certain aspects of China's taxation system have raised national treatment concerns. China has used its taxation system to discriminate against imports in certain sectors (although the issue of discriminatory value-added tax (VAT) rates applied to imports of integrated circuits was resolved in 2004, others, like VAT policies to benefit domestic Chinese producers of fertilizer, remain).<sup>157</sup> U.S. industries continue to express concerns over the unfair operation of China's VAT system, which includes irregular VAT rebates for Chinese producers in favored sectors.

Foreign-invested enterprises (both joint ventures and wholly owned subsidiaries) were responsible for 55 percent of China's exports and 68 percent of its trade surplus in 2010.<sup>158</sup> Bureau of Economic Analysis estimates show that U.S. investment in China was responsible for 0.6 percentage points of the 9.6 percent increase in Chinese GDP in 2008.<sup>159</sup> Commission witness K.C. Fung estimated that in 2009, the rate of return on U.S. FDI abroad to all destinations was 9.7 percent, while the rate of return on investment for U.S. multinationals in China was 13.5 percent.<sup>160</sup>

***China's Investment Regime for Foreign Firms***

U.S. trade officials and business associations have long urged China to liberalize its investment restrictions, but Chinese officials have resisted. While some Chinese industries have become open to foreign investment and sales, huge swathes of the economy, such as construction and telecommunications, are reserved for Chinese firms, both state owned and private. Various government interventions, like "indigenous innovation" policies and catalogues guiding government and state-owned company procurement officers to domestically produced goods and services are used to discriminate against foreign competitors (for more on indigenous innovation, see chap. 1, sec. 3, of this Report). The American Chamber of Commerce in China's *2011 Business Climate Survey* complained of "regulatory obstacles that give local firms a competitive advantage."<sup>161</sup>

Addressing complaints about China's backtracking on promises to make its economy friendlier to foreign companies, Gary Locke, then U.S. Department of Commerce secretary and currently U.S. ambassador to China, said that U.S. firms are frequently shut out of the Chinese market or forced to share technologies to gain access.<sup>162</sup> Ambassador Locke said the "fundamental problem boils down to the distance between the promises of China's government and action."<sup>163</sup>

Over the last several years, the Chinese government has created new policies and government bodies to guide foreign investment and safeguard the domestic economy and national security in the face of FDI inflows:

*The 2011 Catalogue Guiding Foreign Investment in Industry:* The draft *2011 Catalogue Guiding Foreign Investment in Industry* identifies sectors and industries of the Chinese economy in which foreign investment is encouraged, restricted, or prohibited.<sup>164</sup> An update of the catalogue published in 2007, the *2011 Catalogue* is focused on encouraging foreign investment in industries related to China's goal of developing cutting-edge industries with higher-value-added ones, including sophisticated manufacturing, new technologies, and clean energy.<sup>165</sup> Book, newspaper publishing, audiovisual products, and "Internet culture businesses" (excluding music) are among those that will remain off-limits to foreign investment.<sup>166</sup> The U.S. Chamber of Commerce and the American Chamber of Commerce in China called China's use of catalogues to guide foreign investment "at odds with the ... principles of open and market-based economies."<sup>167</sup>

*National Security Review Process:* The State Council promulgated the *Notice of the General Office of the State Council on Establishment of a Security Review System for the Merger and Acquisition of Domestic Enterprises by Foreign Investors* (Notice) in February 2011. The following month, China's Ministry of Commerce issued interim provisions for implementing the notice.<sup>168</sup> The new foreign-investment security review regime sets up an interministerial panel under the State Council. The National Development and Reform Commission and the Ministry of Commerce are assigned lead roles in coordinating the ministries and agencies that would review proposed transactions.<sup>169</sup> Transactions in the following sectors or areas could be subject to review if they lead to foreign investors obtaining "actual control" of a domestic enterprise: military and military support enterprises; enterprises near key and/or sensitive military facilities; other entities associated with national defense and security; and domestic enterprises in sectors that "relate to national security," which are listed as "important" agriculture products, energy and resources, infrastructure, and transportation services, as well as key technologies and major equipment manufacturing industries.<sup>170</sup> A final rule published in August 2011 by China's Ministry of Commerce clarified certain aspects of the security review system but still utilized a broad definition of national security and provided little guidance in assessing whether a transaction could be subject to a review.<sup>171</sup>

The United States and China currently are negotiating a bilateral investment treaty with the goal of expanding investment opportunities. Supporters of the treaty hope it will improve the in-



vestment climate for U.S. firms in China by strengthening legal protections and dispute resolution procedures and by obtaining a commitment from the Chinese government to treat U.S. investors the same as Chinese investors. However, some U.S. groups have expressed reservations concerning a U.S.-China bilateral investment treaty, arguing that it will encourage U.S. firms to relocate to China.<sup>172</sup> Some also have raised questions about the treatment of the trade, investment, and competition issues posed by state capitalism. (For more information on the debate surrounding the U.S.-China bilateral investment treaty, see the report on “Evaluating a Potential U.S.-China Bilateral Investment Treaty,” prepared for the Commission by the Economist Intelligence Unit.<sup>173</sup>)

### **Chinese Investment in the United States**

Chinese investment in the United States deviates from the patterns in other countries where China concentrates more heavily on securing natural resources. In the United States, Chinese investments have focused on manufacturing and technology and are also notable for their emphasis on brand acquisition.<sup>174</sup> China does not have to spend decades building up brand names, because it can acquire existing well-known brands through government-funded firms. For example, Geely Automotive, one of China’s biggest automotive companies, acquired Ford Motor’s Volvo unit in 2010 in a \$1.8 billion deal.<sup>175</sup> A deal in 2009 involved Beijing Automotive Industry Holding Co, China’s fifth-biggest automaker, acquiring the rights to three vehicle platforms from General Motor’s Saab unit.<sup>176</sup> As in the natural resource sector (attempted acquisitions of Unocal and Rio Tinto are good examples), concerns over the involvement of the Chinese government can lead to failed transactions: In February 2011, the Committee on Foreign Investment in the United States (CFIUS) ruled that Huawei Technologies would have to divest its investment in 3Leaf Systems because of national security concerns about Huawei’s ties to the Chinese government and military and the security implications of integrating their equipment into critical U.S. telecommunications infrastructure.<sup>177</sup>

Chinese government policies encouraging outward foreign direct investment are far more recent than those encouraging foreign investment in China. In its Tenth Five-Year Plan (2001–2005), the Chinese government in 2001 officially adopted a policy encouraging Chinese companies to invest abroad.<sup>178</sup> This “going out” policy has started to show results, although outward investment still pales in comparison to inward investment. According to the latest available Chinese government statistics, outward investment in 2010 amounted to \$68.8 billion (an increase of 21.7 percent year on year), with the total accumulation at that time at \$317.2 billion.<sup>179</sup> Chinese companies have made major acquisitions of mining and other natural resource companies in Australia, Canada, South America, and Africa, while Chinese brands like Haier (home appliances), Huawei (telecommunications), and Lenovo (personal computers) are seeking to tap global markets, in part through direct investment abroad.<sup>180</sup>



**Table 2: China's Foreign Direct Investment in the United States, 2003–2010**  
(U.S. \$ million)

	2003	2004	2005	2006	2007	2008	2009	2010
<b>Flow</b>	65.05	119.93	231.82	198.34	195.73	462.03	908.74	1308.29
<b>Stock</b>	502.32	665.20	822.68	1,237.87	1,880.53	2,389.90	3,338.42	4,873.99

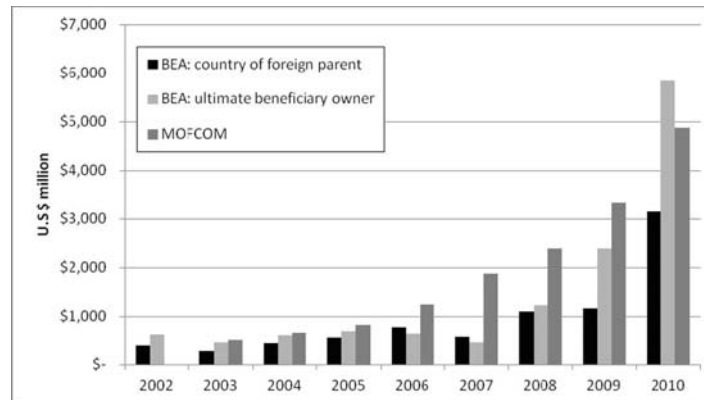
Source: Ministry of Commerce of the People's Republic of China, *2010 Statistical Bulletin of China's Outward Foreign Direct Investment* (Beijing, China: 2011).

Chinese overall nonbond investment has been very limited in the United States to date. China's Ministry of Commerce estimated that in 2010, cumulative Chinese FDI in the United States was \$4.9 billion (see table 2, above). According to the U.S. Bureau of Economic Analysis, the cumulative level of Chinese FDI in the United States through the end of 2010 was \$3.2 billion on a historical-cost (or book value) basis. According to the bureau, in 2009, China ranked as the 34th largest source of cumulative FDI in the United States. By comparison, China's investments in U.S. Treasury securities were an estimated \$1.2 trillion by July 2011, making China the biggest foreign holder.<sup>181</sup>

Several analysts note that China often uses offshore locations (such as Hong Kong or tax havens) to invest in other countries. China also uses London exchanges to buy U.S. Treasuries, in which case the investment is registered as being from the United Kingdom. The Bureau of Economic Analysis also reports cumulative FDI data according to the country of ultimate beneficial owner, which puts Chinese FDI in the United States through 2010 at \$5.9 billion (see figure 1, below).\*

\*The Bureau of Economic Analysis tracks geographic distribution of FDI in two forms: country of direct foreign parent, which attributes each investment to the direct parent company, and country of ultimate beneficiary owner, which tracks the investment to the country of the ultimate owner. The latter method generally is considered more accurate, as a large share of FDI transactions today are conducted through special-purpose vehicles in third countries. In this case, the \$5.9 billion figure represents the Chinese FDI in the United States in 2010 on the ultimate beneficiary owner basis. On the country of foreign parent basis, the cumulative Chinese FDI in the United States was \$3.2 billion by the end of 2010. For further information, see Daniel H. Rosen and Thilo Hanemann, *An American Open Door? Maximizing the Benefits of Chinese Foreign Direct Investment* (New York, NY: Asia Society Special Report, May 2011), pp. 81–88. For data, see U.S. Bureau of Economic Analysis, "Historical-Cost Foreign Direct Investment Position in the United States and Income Without Current-Cost Adjustment, by Country of Foreign-Parent-Group Member and of the Ultimate Beneficial Owner, 2002–2010" (Washington, DC: U.S. Department of Commerce). <http://www.bea.gov/international/di1fdibal.htm>.

**Figure 1: Chinese FDI Stock in the United States, 2002–2010**  
(U.S. \$ million; various official measures)



Source: U.S. Bureau of Economic Analysis; and Ministry of Commerce of the People's Republic of China [MOFCOM], *2010 Statistical Bulletin of China's Outward Foreign Direct Investment* (Beijing, China: 2011).

Despite China's substantial purchases of U.S. Treasury securities, China's role as a direct investor in the United States remains marginal. China's FDI stock of \$5.9 billion in 2010 (using the ultimate beneficiary owner figures) accounted for a mere 0.25 percent of total foreign investment in the United States (it is also lower than investment stock of other developing countries such as Brazil and India).<sup>182</sup>

There are indications that outward foreign direct investment from China is on the increase. Stock of Chinese FDI in the United States grew from \$1.2 billion in 2008 to \$5.9 billion (on the ultimate beneficial owner basis) in 2010, an increase of almost 400 percent.<sup>183</sup>

### Chinese Foreign Exchange Reserves

Over the last several decades, China has accumulated an enormous stockpile of foreign exchange reserves, around \$3.2 trillion by September 2011. To date, the vast majority of these reserves, managed by the State Administration for Foreign Exchange, has been invested in U.S. Treasury securities. However, China has shown interest in diversifying its reserves by moving some of its foreign exchange out of U.S. debt securities and into higher-yield investments.

### **Chinese Foreign Exchange Reserves—Continued**

China's official holdings of U.S. Treasury securities amounted to around \$1.2 trillion by July 2011<sup>184</sup> and far eclipse China's cumulative global outward FDI, which was around \$317.2 billion in 2010 (the latest figures available). For the purpose of comparison, Chinese holdings of U.S. Treasury securities at the time were \$1.1 trillion. China's official holdings of U.S. Treasuries are likely underreported, because China purchases many of its U.S. bonds through third parties, and those securities are registered to the location of purchase rather than the eventual owner.

To manage and diversify China's foreign exchange reserves beyond the traditional investment in U.S. Treasuries, in 2007 the Chinese government established the China Investment Corporation (CIC).<sup>185</sup> Although CIC endured some criticism over its performance after investing all of its initial \$200 billion (some of which resulted in paper losses during the global financial crisis), Chinese Vice Premier Li Keqiang endorsed CIC's role in diversifying China's foreign exchange reserves.<sup>186</sup> According to the latest financial reports available, CIC had total assets of \$332 billion at the end of 2009 and is one of the biggest sovereign wealth funds in the world.

In addition to China's FDI in the United States and its holdings in U.S. Treasury securities, China (as of June 2010) held \$127 billion in U.S. equities, up from \$3 billion in June 2005. It also held \$360 billion in U.S. agency securities, principally those of Fannie Mae and Freddie Mac.<sup>187</sup>

### **The Role of SOEs in China's Outward FDI**

SOEs in the energy, raw materials, and metals sectors have been major participants in the "going-out" strategy.<sup>188</sup> In other sectors, non-SOEs, such as Haier and Lenovo, have also been active in the international mergers and acquisitions market.<sup>189</sup> Dr. Scissors of The Heritage Foundation says that SOE involvement in the "going-out" strategy is "utterly dominant," noting that four state entities "alone account for half of all Chinese investment" (see table 3, below).<sup>190</sup>

**Table 3: Top Global Investments by Chinese SOEs<sup>191</sup>**

<b>Entity</b>	<b>Global Investment (U.S. \$ billion)</b>
CNPC	\$34.48
Sinopec	32.21
China Investment Corporation (CIC)	25.67
Chinalco (Aluminum Corporation of China)	20.62
<b>Subtotal</b>	<b>112.98</b>
<b>Chinese total FDI since 2005</b>	<b>\$215.9</b>

According to China's Ministry of Commerce, in 2009, SOEs provided about \$38.2 billion (67.6 percent) of China's cumulative FDI

abroad.<sup>192</sup> This is attributable to the head start SOEs had in getting approval to invest abroad in the past and the dominance of SOEs in natural resource acquisition deals.<sup>193</sup> These natural resource investors, however, are less involved in China's U.S. investment. Daniel Rosen and Thilo Hanemann of the Rhodium Group concluded in their research that between 2003 and 2010, 74 percent of the number of investment deals originated from private firms (which the authors define as having 80 percent or greater nongovernment ownership).<sup>194</sup> However, in terms of total deal value, the picture is reversed: SOEs account for 65 percent of the total.<sup>195</sup>

***National Security Issues Related to Chinese Investment in the United States***

The close ties between the Chinese government and Chinese corporations are relevant to Chinese companies' attempts to provide critical infrastructure to the U.S. government or to acquire U.S. firms that either perform work for the U.S. government or defense contractors that have intellectual property that would pose a national security risk if obtained by a foreign government. "The real concern—and it has to be case by case—is that many of these companies are so closely intertwined with the government of China that it is hard to see where the company stops and the country begins, and vice versa," Democratic Senator Jack Reed (D-RI) has noted.<sup>196</sup> Investigating the national security implications of mergers and acquisitions falls to CFIUS. Among other issues, CFIUS considers two elements when evaluating whether an investment warrants an investigation: (1) whether there is state control of the acquiring foreign company, and (2) whether the transaction could affect U.S. national security.<sup>197</sup>

For China, the question of state control can be particularly complicated, because the government's role is not always straightforward or disclosed. Despite economic reforms and moves toward privatization, much of the Chinese economy remains under the ownership or control of various parts of the Chinese government. In addition to outright ownership or direct control, the government or the Communist Party can also exert control by deciding the composition of corporate boards and the corporation's management team.<sup>198</sup> To some analysts, these questions are beside the point: Mr. Rosen told the Commission at its March 30 hearing that all Chinese companies were under the influence of Chinese government "to a greater extent than firms are here."<sup>199</sup>

In fact, the United States is relatively open to FDI, although some high-profile Chinese acquisition attempts have raised objections that have led to some investments being blocked or dropped. Most notable were the proposed investments by China National Offshore Oil Corporation (CNOOC) and two deals by Huawei (a bid for 3COM and for 3Leaf).

Despite some failures, recent investments, especially greenfield investments (new ventures), have been made without significant opposition. In many cases, such deals have benefitted from state and local government investment incentives.<sup>200</sup> For example, Tianjin Pipe is currently building a \$1 billion steel pipe mill near Corpus Christi, Texas, benefitting from a variety of state and local

incentives, including employment-based incentives, tax abatement, job training, and infrastructure.<sup>201</sup> A Suntech Power solar panel assembly plant was approved to operate in Arizona, which was attractive to the company because of the state's tax incentives to encourage renewables manufacturing in the state.<sup>202</sup> Late last year, state-owned China Huaneng Group Corp. agreed to buy a 50 percent stake in Massachusetts-based electric utility InterGen for \$1.2 billion in cash. CNOOC came back to the United States in recent months as well, with joint venture investments in Chesapeake Energy Corp. shale projects.<sup>203</sup>

In response to CFIUS blocking some high-profile deals by Chinese firms, Chinese officials have called U.S. investment policies "protectionist." In his testimony before the Commission, Mr. Rosen criticized what he views as a U.S. loss of control over the narrative concerning American openness to Chinese investment:

*Two years in a row of more than 100 percent year-on-year growth in Chinese investment, large Chinese investments across 16 U.S. industries, the story ought to be, 'my God, the United States is open to Chinese investment; we don't screw around with this the way some other countries do.' Instead, the narrative in China and here is why is the United States refusing to open up to Chinese investors, and what are we going to do to guarantee our friends in Beijing that we're going to play fair? It's just absurd, I think, that we've allowed the narrative to be lost in the way we have.*<sup>204</sup>

### **Implications for the United States**

During the 2008 financial crisis, China's leaders reaffirmed their approach to economic management in which private capitalism plays only a supporting role.<sup>205</sup> "The socialist system's advantages," Prime Minister Wen Jiabao said in a March 2010 address, "enable us to make decisions efficiently, organize effectively, and concentrate resources to accomplish large undertakings."<sup>206</sup>

This approach by one of America's largest trading partners carries negative consequences for U.S. economic interests. Subsidies in China can easily overcome the actual and comparative advantages of their trading partners. A country following free market principles can lose companies, product lines, and entire industries if its private sector economy is forced to compete with a foreign government that can sustain continued financial losses. That is why the WTO discourages and, in some cases, prohibits subsidies to exporting industries. Moreover, notification of subsidies is required under the WTO rules, but since its WTO accession in 2001, China has done so only once, in 2006, and the list was judged by China's trade partners to be incomplete. In 2011, the Office of the U.S. Trade Representative submitted a notification to the WTO identifying nearly 200 Chinese subsidy programs, which China failed to notify.<sup>207</sup>

An assessment of Chinese subsidies prepared for the Commission concluded that "eliminating Chinese subsidies would increase U.S. output, exports, worker earnings and economic welfare." The study further noted that "the stagnant level of equipment stock of U.S.

manufacturers, rising U.S. capital expenditures in China and the rapid expansion of imports from China suggest that Chinese subsidies have been diverting equipment investments from the United States to China, or otherwise limiting U.S. manufacturing investments ... reversing this pattern would have a beneficial effect on U.S. manufacturers that compete with Chinese firms, and on the overall U.S. economy.”<sup>208</sup>

SOEs have distinct advantages when competing internationally and within their home market. In addition to several varieties of subsidies that SOEs enjoy, Chinese companies benefit from government regulations that aid them to the detriment of foreign competition. Dr. Scissors testified on March 30 that “in most sectors, there is no market of 1.3 billion. Instead, there is what is left after the SOEs are handed the bulk. This applies, of course, to American companies looking to serve the Chinese market.”<sup>209</sup>

The competitive challenge that SOEs pose for U.S. companies may soon intensify. The U.S.-China Business Council’s 2010 report on company priorities named competition with SOEs as one of the top three concerns for its members in China.<sup>210</sup> The Obama Administration has also raised the issue of the effect on fair competition of Chinese government support provided to its state-owned enterprises. At the May 2011 Strategic and Economic Dialogue talks in Washington, the U.S. Treasury Department noted that:

*China and the United States discussed the principle of equivalent treatment for state-owned, controlled, or invested enterprises (SOEs), private enterprises, and foreign enterprises with respect to access to credit, tax treatment, regulatory applicability, and access to factors of production. The two countries also discussed the desirability of ensuring that SOEs seek a commercial rate of return and steadily increase their dividend payout.*<sup>211</sup>

However, there were no formal commitments on the part of the Chinese government to stop or decrease subsidies to the state-owned or -controlled sector.

On the investment side, opinions vary on the net benefits of U.S. investment in China and Chinese investment in the United States. Many U.S. analysts contend that greater Chinese FDI in the United States, especially in greenfield projects that manufacture products or provide services in the United States, will create new jobs for U.S. workers.<sup>212</sup> At a discussion hosted by the Woodrow Wilson Center, Daniel Rosen and Derek Scissors agreed that Chinese FDI is a positive for the U.S. economy but differed sharply in their opinions about the appropriate U.S. policy response to these investment inflows. While Mr. Rosen discouraged strengthening policy impediments to Chinese FDI and lauded traditional U.S. economic openness, Dr. Scissors characterized U.S. market access as a powerful bargaining chip for encouraging reform within Chinese economic policy.<sup>213</sup>

Some critics of China’s current FDI policies and practices contend that they are largely focused on acquiring and transferring technology and know-how to Chinese firms favored by the Chinese government for development but do little to help the U.S. economy. The U.S. Chamber of Commerce said China’s “investment protec-



tionism” serves as the “lynchpin” of its efforts to wring technology and other concessions from U.S. firms “in exchange for access [to] the Chinese market.”<sup>214</sup> (For more information on technology transfers, see chap. 1, sec. 4, of this Report.)

Lack of transparency about Chinese firms’ connections to the central government, through financial support or decision-making, is another major problem. Many U.S. policymakers are troubled by the possibility that Chinese SOEs’ efforts to acquire U.S. company assets could be part of the Chinese central government’s strategy to develop global Chinese firms that may one day threaten the economic viability of U.S. firms.<sup>215</sup>

### Conclusions

- China’s privatization reforms during the past two decades appear in some cases to have been reversed, with a renewed use of industrial policies aimed at creating SOEs that dominate important portions of the economy, especially in the industrial sectors, reserved for the state’s control.
- The Chinese government promotes the state-owned sector with a variety of industrial policy tools, including a wide range of direct and indirect subsidies, preferential access to capital, forced technology transfer from foreign firms, and domestic procurement requirements, all intended to favor SOEs over foreign competitors.
- The value and scope of U.S.-China bilateral investment flows have expanded significantly in the past ten years. However, U.S. direct investment in China is more than 12 times greater than Chinese direct investment in the United States. Official U.S. statistics show that U.S. cumulative FDI in China was \$60.5 billion in 2010. The Chinese Ministry of Commerce estimated that in 2010, cumulative Chinese FDI in the United States was \$4.9 billion.
- The Chinese government guides FDI into those sectors it wishes to see grow and develop with the help of foreign technology and capital. Foreign investors are frequently forced into joint ventures or other technology-sharing arrangements, such as setting up research and development facilities, in exchange for access to China’s market. Meanwhile, large swathes of the Chinese economy are closed to foreign investors. China’s investment policies are part of the government’s plan to promote the development of key industries in China through access to foreign technology and capital.
- Chinese FDI in the United States is a relatively recent phenomenon and remains very small compared to the U.S. investment in China, but there is great potential for growth. China has stated a desire to diversify its holdings of foreign exchange, estimated at \$3.2 trillion in mid-2011, the majority of which is invested in dollar-denominated debt securities. As with other statistics, there are discrepancies between official U.S. and Chinese statistics on bilateral investment.
- Due to the considerable government ownership of the Chinese economy, provision by Chinese companies of critical infrastructure to U.S. government or acquisition by Chinese companies of

U.S. firms with sensitive technology or intellectual property could be harmful to U.S. national interests. The Committee on Foreign Investment in the United States investigates the national security implications of mergers and acquisitions by foreign investors of U.S. assets.

- In areas where there are no national security considerations, Chinese FDI has the potential to create jobs and economic growth.
- China has recently introduced a national security investment review mechanism similar to the Committee on Foreign Investment in the United States, although there are concerns among foreign companies that the Chinese government may use the mechanism to derail investment by foreigners in those companies and sectors it wants to remain under government control.

**Addendum I: SASAC Companies, Large State-owned Banks, and Insurance Companies (2011)** <sup>216</sup>

	<b>Company name</b>	<b>Abbreviation</b>
1	China National Nuclear Corporation	CNNC
2	China Nuclear Engineering & Construction Corporation	CNECC
3	China Aerospace Science & Technology Corporation	CASC
4	China Aerospace Science & Industry Corporation	CASIC
5	Aviation Industry Corporation of China	AVIC
6	China State Shipbuilding Corporation	CSSC
7	China Shipbuilding Industry Corporation	CSIC
8	China North Industries Group Corporation	CNIGC
9	China South Industries Group Corporation	CSGC
10	China Electronics Technology Group Corporation	CETC
11	China National Petroleum Corporation	CNPC
12	China Petrochemical Corporation	Sinopec
13	China National Offshore Oil Corporation	CNOOC
14	State Grid Corporation of China	SGCC
15	China Southern Power Grid Company, Limited	CSG
16	China Huaneng Group	CHNG
17	China Datang Corporation	CDT
18	China Huadian Corporation	CHD
19	China Guodian Corporation	CGDC
20	China Power Investment Corporation	CPI
21	China Three Gorges (Project) Corporation	CTGPC
22	Shenhua Group Corporation Limited	Shenhua
23	China Telecommunications Corporation	China Telecom
24	China United Network Communications Group Company	China Unicom
25	China Mobile Group	China Mobile
26	China Electronics Corporation	CEC
27	China FAW Group Corporation	FAW
28	Dongfeng Motor Corporation	DFMC
29	China First Heavy Industries	CFHI
30	China National Erzhong Group Corporation	Erzhong

**Addendum I: SASAC Companies, Large State-owned Banks, and Insurance Companies (2011)—Continued**

	<b>Company name</b>	<b>Abbreviation</b>
31	Harbin Electric Corporation	HPEC
32	Dongfang Electric Corporation	DEC
33	Anshan Iron and Steel Group Corporation	Ansteel
34	Baosteel Group Corporation	Baosteel
35	Wuhan Iron and Steel (Group) Corporation	WISCO
36	Aluminum Corporation of China	Chalco
37	China Ocean Shipping (Group) Company	COSCO
38	China Shipping Group	China Shipping
39	China National Aviation Holding Company	AirChina
40	China Eastern Aviation Holding Company	China Eastern
41	China Southern Air Holding Company	China Southern
42	Sinochem Group	Sinochem
43	COFCO Corporation	COFCO
44	China Minmetals Corporation	Minmetals
45	China General Technology (Group) Holding, Limited	Genertec
46	China State Construction Engineering Corp.	CSCEC
47	China Grain Reserves Corporation	Sinograin
48	State Development & Investment Corporation	SDIC
49	China Merchants Group	CMHK
50	China Resources (Holdings) Company, Limited	CRC
51	The China Travel Service (HK) Group Corporation	HKCTS
52	State Nuclear Power Technology Corporation	SNPTC
53	Commercial Aircraft Corporation of China, Limited	COMAC
54	China Energy Conservation Investment Corporation	CECIC
55	China Gaoxin Investment Group Corporation	Gaoxin Group
56	China International Engineering Consulting Corporation	CIECC
57	Zhongnan Commercial (Group) Company, Limited	Zhongnan
58	China Huafu Trade & Development Group Corporation	HFJT
59	China Chengtong Group	CCT

**Addendum I: SASAC Companies, Large State-owned Banks, and Insurance Companies (2011)—Continued**

	<b>Company name</b>	<b>Abbreviation</b>
60	China Huaxing Group	Huaxing
61	China National Coal Group Corporation	ChinaCoal
62	China Coal Technology & Engineering Group Corporation	CCTEG
63	China National Machinery Industry Corporation	SINOMACH
64	China Academy of Machinery Science & Technology	CAM
65	Sinosteel Corporation	Sinosteel
66	China Metallurgical Group Corporation	MCC
67	China Iron & Steel Research Institute Group	CISRI
68	China National Chemical Corporation	ChemChina
69	China National Chemical Engineering Group Corp.	CNCEC
70	Sinolight Corporation	Sinolight
71	China National Arts & Crafts (Group) Corporation	CNACGC
72	China National Salt Industry Corporation	CNSIC
73	China Hengtian Group Company, Limited	CHTGC
74	China National Materials Group Corporation Limited	SINOMA
75	China National Building Materials Group Corp.	CNBM
76	China Nonferrous Metal Mining (Group) Company	CNMC
79	China International Intellectech Corporation	CIIC
80	China Academy of Building Research	CABR
81	China CNR Corporation Limited	CNR
82	China CSR Corporation Limited	CSR
83	China Railway Signal & Communication Corporation	CRSC
84	China Railway Group Limited	China Railway
85	China Railway Construction Corporation Limited	CRCC
86	China Communications Construction Company Limited	CCCC
87	China Potevio Company, Limited	China Potevio
88	Datang Telecom Technology & Industry Group	Datang
89	China National Agricultural Development Group Company	CNADC
90	Chinatex Corporation	Chinatex
91	China National Foreign Trade Transportation Corp.	SINOTRANS

**Addendum I: SASAC Companies, Large State-owned Banks, and Insurance Companies (2011)—Continued**

	<b>Company name</b>	<b>Abbreviation</b>
92	China National Silk Import & Export Corporation	Chinasilk
93	China Forestry Group Corporation	CFGC
94	China National Pharmaceutical Group Corporation	SINOPHARM
95	CITS Group Corporation	CITS
96	China Poly Group Corporation	POLY
97	Zhuhai Zhen Rong Company	Zhzrgs
98	China Architecture Design & Research Group	CAG
99	China Metallurgical Geology Bureau	CMGB
100	China National Administration of Coal Geology	CNACG
101	Xinxing Cathay International Group Company, Limited	XXPGroup
102	China Travelsky Holding Company	Travelsky
103	China Aviation Fuel Group Corporation	CNAF
104	China National Aviation Supplies Holding Company	CASC
105	China Power Engineering Consulting Group Corporation	CPECC
106	HydroChina Corporation	HYDROCHINA
107	Sinohydro Corporation	Sinohydro
108	China National Gold Group Corporation	CNGC
109	China National Cotton Reserves Corporation	CNCRC
110	China Printing (Group) Corporation	CPGC
111	China Lucky Film Corporation	Luckyfilm
112	China Guangdong Nuclear Power Holding Corporation	CGNPC
113	China Hualu Group Company, Limited	Hualu
114	Alcatel-Lucent Shanghai Bell Company Limited	Alcatel-sbell
115	IRICO Group Corporation	IRICO
116	FiberHome Technologies	WRI
117	OCT Enterprises Company	OTC
118	Nam Kwong (group) Company, Limited	Namkwong
119	China XD Group	XD Company
120	China Gezhouba Group Corporation	CGGC
121	China Railway Materials Commercial Corporation	CRM



**Addendum I: SASAC Companies, Large State-owned Banks, and Insurance Companies (2011)—*Continued***

	<b>Company name</b>	<b>Abbreviation</b>
122	Industrial & Commercial Bank of China	ICBC
123	China Life Insurance Group	China Life
124	China Construction Bank	CCB
125	Bank of China	BOC
126	Agriculture Bank of China	ABC
127	China Taiping Insurance Group Company	China Taiping
128	Bank of Communications	BOCOM
129	China Development Bank	CDB
130	People's Insurance Company of China	PICC

Notes and sources: The first 121 companies are listed in the order provided by SASAC. Data derived from <http://www.sasac.gov.cn/n1180/n1226/n2425/index.html>; <http://www.ceda.org.cn/china-500/>; and individual companies' websites.

**Addendum II: U.S. Direct Investment Position in China on a Historical-cost Basis by Industry,  
2000–2010**  
(U.S. \$ million)

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Total	11,140	12,081	10,570	11,261	17,616	19,016	26,459	29,710	52,521	49,403	60,452
Mining	1,404	1,791	1,179	1,263	1,966	2,039	1,958	1,772	3,022	3,648	3,595
Utilities	583	487	540	n.s.	n.s.	n.s.	n.s.	n.s.	n.s.	n.s.	n.s.
Total Manufacturing	7,076	7,727	5,554	5,499	9,008	9,346	14,759	18,461	22,584	22,618	29,477
• Food	286	329	425	528	388	402	401	544	2,659	2,874	3,290
• Chemicals	1,122	1,062	1,132	1,338	1,811	2,335	3,308	4,402	5,266	4,987	6,459
• Primary and Fabricated Metals	157	139	151	115	286	432	471	588	672	691	1,252
• Machinery	218	203	335	298	564	386	796	1,269	1,447	1,186	1,258
• Computers and Electronic Products	3,500	3,993	1,275	721	1,719	1,689	5,325	6,965	6,416	5,745	7,963
• Electrical equipment, appliances and components	458	625	521	376	510	531	433	487	556	493	576
• Transportation Equipment	652	650	802	1,209	1,879	1,501	1,665	1,738	2,007	2,736	4,150
• Other Manufacturing	n.s.	n.s.	n.s.	915	1,850	2,071	2,361	2,468	3,561	3,904	4,530
Wholesale Trade	378	576	1,144	1,538	1,705	2,147	3,318	2,015	2,781	2,899	4,018
Information	79	112	218	544	604	801	357	546	427	459	789
Depository Institutions	64	151	319	413	563	757	1,095	850	(D)	10,856	13,413
Finance (except depository institutions) and insurance	43	-30	(D)	-49	1,299	1,480	1,661	1,798	1,877	1,834	1,898
Professional, scientific, and technical services	245	121	406	171	597	523	1,159	227	359	605	890
Holding Companies (nonbank)	n.s.	n.s.	n.s.	1,063	1,452	1,159	1,220	1,644	3,099	3,882	3,445
Other Industries	1,267	1,146	(D)	819	422	763	932	2,397	(D)	2,602	2,928

Source: Bureau of Economic Analysis, *U.S. Direct Investment Abroad (USDIA): Operations of U.S. Parent Companies and Their Foreign Affiliates* (Washington, DC: U.S. Department of Commerce (Issues 2000–2010), <http://www.bea.gov/international/diitusbal.htm>).

**Legend:**

n.s.—Not shown. Data may not be shown for several reasons:

1. The data appear on another line in this table.

2. The data are not shown in this table but may be available in detailed country- or industry-level tables in this interactive system or in other Bureau of Economic Analysis published tables on direct investment.

3. The data are not available, do not apply, or are not defined.

(D)—Indicates that the data in the cell have been suppressed to avoid disclosure of data of individual companies.

### **SECTION 3: INDIGENOUS INNOVATION AND INTELLECTUAL PROPERTY RIGHTS**

#### **Introduction**

China's program for encouraging "indigenous innovation" has its origin in the central government's decades-old policy of favoring domestic goods and services over imports. A new element was added to the policy with the publication in 2009 of government procurement catalogues at the national, provincial, and local levels. The catalogues were written to exclude the services and products of foreign-based corporations, including those with foreign affiliates operating in China that have not transferred their technology. The move represented an escalation in China's longstanding efforts to substitute domestic goods and services for imports.

The Commission held hearings in Washington on May 4 and June 15 to examine China's indigenous innovation policy and the likelihood that it will require the transfer of critical technology to Chinese companies. In addition, the Commission examined China's intellectual property protections related to business software during the May 4 hearing. This section will trace the development of China's indigenous innovation policy in the context of China's industrial policy and its potential effect on the economy of the United States. This section will also examine China's failure to enforce intellectual property protections for business software.

U.S. and European-based companies raised two main objections to the new procurement catalogues. First, foreign-based companies as well as their affiliates operating within China would be excluded from sales to governments in China, since only domestic companies or those holding registered Chinese patents were eligible to be included in the procurement catalogues. Second, any attempt to qualify a foreign affiliate for the official procurement catalogue would likely require foreign companies to transfer or reveal sensitive and proprietary technology to Chinese companies.

The stakes for foreign companies hoping to sell to all levels of government in China are substantial. The indigenous innovation policy involves a number of separate requirements including patent and trademark filing and registration regulations that may lead to involuntary releases of proprietary information. The European Chamber of Commerce estimated in April 2011 that the discriminatory policy would cover more than \$1 trillion in goods and services purchases on an annual basis.<sup>217</sup> The international business community criticized the proposed indigenous innovation regulations by requesting that the U.S. government oppose the policy during future bilateral negotiations with China. In December 2009, the heads of 34 U.S., European, and Japanese companies and business associations wrote to Chinese leaders to protest the catalogues. In

January 2010, the heads of 19 U.S. business associations wrote to the Obama Administration to warn that the new Chinese policy posed “an immediate danger to U.S. companies.”

The government in Beijing subsequently responded by promising to modify the program and pledged to revoke the requirement that government purchases be made exclusively from the procurement catalogues. Despite such assurances by President Hu Jintao during his trip to Washington in January 2011, there are few signs that China intends to rescind its overall indigenous innovation policy and only inconclusive signs that the use of procurement catalogues will be abandoned.

The theft of intellectual property in China\* is a longstanding problem despite efforts by the Chinese central government over more than a decade to pass laws and regulations prohibiting such theft. In fact, Chinese officials are able to point to many Chinese statutes protecting copyrights, trademarks, and patents. And yet the problem persists because enforcement is ineffective. Administrative fines are low, and the threshold for criminal prosecution is high, according to U.S. government complaints. This allows Chinese pirates and counterfeiters to stay in business and pay fines out of their cash flow.

The cost to the United States of intellectual property violations in China is considerable. Based on a survey of U.S. companies operating in China, the U.S. International Trade Commission estimates that employment in the United States would increase by a range of 923,000 to 2.1 million jobs if China were to adopt an intellectual property system equivalent to that of the United States.<sup>218</sup>

### **Development of China’s Indigenous Innovation Policy**

Chinese leaders dating back to Deng Xiaoping have explicitly sought to bolster China’s high-technology industries by obtaining foreign technology and by favoring the products of China’s fledgling high-tech industries over foreign technology imports whenever possible. In 2002, for example, President Jiang Zemin proclaimed a Government Procurement Law limiting government purchases to domestically made goods.<sup>219</sup> China made a promise during the negotiations to allow China’s admission to the World Trade Organization (WTO) in 2001 to join the WTO’s Agreement on Government Procurement (GPA) “as soon as possible.” That agreement pledges the 41 GPA signatories to refrain from discriminating against foreign imports in government procurement. China still has not done so. (For more information on China’s refusal to join the WTO’s government procurement code, please see the Commission’s 2010 Annual Report, chap. 1, sec. 3.)

China’s current indigenous innovation policy was unveiled officially in the government’s *National Medium- and Long-Term Plan for the Development of Science and Technology (2006–2020)*.<sup>220</sup> That plan, known as the MLP and released in February 2006, directs government officials to “formulate policies that encourage independent innovation and restrict unscrupulous and redundant imports.”<sup>221</sup> Ma Kai, minister of the National Development and Re-

\*Counterfeiting refers to the violation of a trademark, while piracy is the violation of a copyright. Most seizures of such contraband at U.S. borders are for trademark infringements.

form Commission (NDRC), explained the need for the policy this way:

*China's competitive edge is to a great extent based on cheap labor, cheap water, land, resources, and expensive environmental pollution. [This] will be weakened with the rising price of raw materials and enhancement of environmental protection. Therefore, we must enhance independent innovation capability vigorously. ... [W]e will promote development by relying on enhancing independent innovation capability, and as a national strategy, shift economic growth from relying on the import of capital materials to relying on scientific and technological advancement and human resources."*<sup>222</sup>

#### **The Size of China's Public Procurement Market**

China's Ministry of Finance estimates the annual total of government contracts at \$103 billion at the government's official exchange rate.<sup>223</sup> But this estimate does not include purchases by China's state-owned enterprises, many of which are the largest in their industrial sector.

Also excluded from this total are almost all large-scale infrastructure and public utility projects.<sup>224</sup> These huge projects were estimated by the office of the United States Trade Representative (USTR) to represent at least one-half of China's total government procurement market.<sup>225</sup> These include such public projects as the Three Gorges Dam; the Bird's Nest, Water Cube, and other Olympic venues; and China's high-speed railroad network.

In addition, the official finance ministry figures exclude provincial and municipal government purchases. Once all those additional contracts are added in, the total is far larger. The European Chamber of Commerce included purchases by central and local governments as well as state-owned enterprises and public infrastructure projects in its estimate of \$1 trillion annually. If the European Chamber's figures are correct, China's indigenous innovation policy and official procurement catalogues would wall off 17 percent of China's \$5.9 trillion economy from foreign participation.<sup>226</sup>

The indigenous innovation plan specifically envisions reducing China's reliance on products containing foreign technology to 30 percent by 2020 from an estimated 60 percent in 2006.<sup>227</sup> To do so, the plan calls for "enhancing original innovation through 'co-innovation' and 're-innovation' based on the assimilation of imported technologies."<sup>228</sup> In 2007, the Ministry of Finance issued two notices providing implementation regulations for the indigenous innovation initiatives outlined in the MLP. The first, *Administrative Measures on Government Procurement of Imported Products*, established procedures and rules that severely limited the procurement of imported products. The second, *Administrative Measures for the Government to Initially and Selectively Purchase Indigenous Inno-*

vation Projects,\* promoted the development of domestic companies not currently competitive in the marketplace. This was to be accomplished during the evaluation process for government procurement through preferential treatment to “accredited indigenous innovation products.”<sup>229</sup>

The “chief aim” of the MLP and its subsequent regulations and guidelines “was to foster the development, commercialization, and procurement of Chinese products and technologies,” said John Neuffer, vice president for global policy at the Information Technology Industry Council.<sup>230</sup> “More precisely, it was developed to give a leg up to domestic producers by compelling government agencies to adopt rules and regulations favoring products that use Chinese-developed ideas and technologies,” Mr. Neuffer told the Commission.

Various agencies of the central government continued to promulgate rules and regulations to implement the MLP by discriminating against non-Chinese products. In November 2009, Beijing issued the *Notice of the Launch of National Indigenous Innovation Product Accreditation Work for 2009* (Circular 618).† Circular 618 defined an “indigenous innovation product” as one with intellectual property fully owned by a Chinese company and a trademark initially registered within China. At this point, the intent of the indigenous innovation goal became clear: Chinese government agencies at all levels were to shun even those goods manufactured in China by joint ventures with foreign affiliates and to demand that original patents be filed first in China, a particular requirement of Chinese patent law. Because Chinese patent law is less protective of proprietary information contained in patent applications, foreign affiliates risk having their intellectual property compromised. In addition, the Chinese government in 2010 expanded the conditions under which the government can require a company to license its patent to other companies.<sup>231</sup> For example, Chinese patent law allows the government to grant a compulsory license on a patent involving semiconductor technology if the government rules that expanding production to other producers would be “in the public interest.”<sup>232</sup>

In December 2009, the central government produced a list of 240 types of industrial equipment in 18 categories that the government wished to support and offered domestic producers a range of tax incentives and government subsidies as well as priority status in indigenous innovation product catalogues.<sup>233</sup>

U.S., European, Canadian, and Japanese business groups complained in a December 2009 letter to the heads of four relevant Chinese ministries that “the very restrictive and discriminatory program criteria would make it virtually impossible for any non-Chinese supplier to participate—even those non-Chinese companies that have made substantial and long-term investments in China, employ Chinese citizens, and pay taxes to the Chinese govern-

\* Along with these broader policies, the Finance Ministry issued a number of other measures in 2006 and 2007 detailing the accreditation for indigenous innovation products as well as administrative measures on budgeting, contract requirements, and evaluation of the government procurement of indigenous innovation products.

† For a more detailed discussion of Circular 618, see U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), pp. 47–48.



ment.”<sup>234</sup> In response, the Chinese government revised Circular 618 in April 2010 to remove the requirement that trademarks and brands must first be registered in China and that the intellectual property be owned entirely by the Chinese company.<sup>235</sup>

Despite the revisions to Circular 618 in 2010, many local policies on government procurement and indigenous innovation product accreditation still contain references to intellectual property requirements and the substitution of domestic goods for imports.\* Of the 31 provincial and municipal accreditation rules and guidelines for indigenous innovation product certification identified in a February 2011 report by the U.S.-China Business Council, all 31 contained intellectual property qualifications, and 23 contained references to requirements for import substitution.<sup>236</sup>

The apparent discrepancy between the central government’s promised revisions and the continued publication of discriminatory local product catalogues indicates a struggle between the two levels of government that is familiar to close observers of China. An alternative interpretation is that Beijing uses the excuse that it cannot control localities as a justification to do business as usual. Another theory ascribes Beijing’s lax enforcement to a deliberate decision to enforce only those laws and regulations that benefit China at the expense of foreigners. For example, because revisions to Circular 618 refer only to the proposed national product catalogue, there is no guarantee that such reforms will apply at a provincial or local level. Furthermore, circulars issued by the government “do not require that its content be implemented,” according to Kenneth Lieberthal of The Brookings Institution.<sup>237</sup>

Provincial and municipal governments continue to grant strong preferential treatment to domestic firms in their indigenous innovation product catalogues. In a 2011 article published on the Ministry of Finance government procurement website, an unnamed source within a provincial-level government procurement office explained that, while the establishment of a national indigenous innovation catalogue is unlikely, local government catalogues exist regardless.<sup>238</sup> The composition of these catalogues often reflects the strong barriers to entry for foreign-invested enterprises seeking government procurement contracts at the provincial and municipal level.

The U.S.-China Business Council report identified 61 separate indigenous innovation catalogues released by 22 provincial- and municipal-level governments by mid-November 2010.<sup>239</sup> Among the 59 products listed in Beijing’s government procurement catalogue through November 2010, only one is produced by a foreign company.<sup>240</sup> Nanjing’s draft catalogue, published in June 2010, is comprised of 42 products, not one of which is produced by a foreign-invested enterprise.<sup>241</sup>

The persistence of local catalogues indicates that the promised reforms of the central government are not reflected in the provinces. Without strong support at the provincial and municipal levels for delinking government procurement from indigenous innova-

---

\*“IP [intellectual property] Qualification” refers to the inclusion of certain intellectual property conditions such as origin or country of ownership. “Import substitution” refers to policies that encourage the development of domestic products that can replace imports.

tion catalogs, foreign affiliates of U.S. and European companies will continue to face discrimination, according to U.S. business groups.<sup>242</sup>

### **Policies Favoring Chinese Enterprises**

Although China's government procurement policies have garnered the greatest attention from the international media and business community, Chinese indigenous innovation strategy is multifaceted, incorporating numerous other laws and regulations that promote domestic industry.

#### **Tax Incentives**

China has implemented a number of tax laws that favor innovative domestic industries. In September 2006, China's Tax Bureau issued the *Circular on Preferential Tax Policies for Innovation Enterprises*, which offers "innovation enterprises" a two-year exemption from the enterprise income tax.<sup>243</sup> In January 2008, the National People's Congress issued the *Enterprise Income Tax Law of the People's Republic of China*, Article 28 of which states, "Enterprise income tax for State-encouraged high and new technology enterprises shall be levied at a reduced rate of 15 percent" rather than the standard 25 percent top corporate tax rate.<sup>244, 245</sup>

#### **Subsidies and Loans**

The Chinese government has long provided extensive subsidies to favored industries and companies, both private and state owned. The direct subsidies include low-interest-rate loans and loan forgiveness, discounted or free land, electricity, fuel, water, and sewerage. Indirect subsidies can include lax enforcement of environmental standards and workers' rights laws. The Chinese government in particular provides subsidies to a large number of designated "strategic industries" and included \$216 billion in subsidies for its green technology sector as part of its economic stimulus package.<sup>246</sup>

At the May 5, 2011, hearing before the Commission, Thea Lee of the American Federation of Labor and Congress of Industrial Organizations (AFL-CIO) characterized Chinese industrial policy as "targeting favored sectors and technologies through below-market loans and subsidies."<sup>247</sup> (For more on subsidies, see the Commission's *2009 Annual Report to Congress*, chap. 1, sec. 3, "China's Industrial Policy and its Impact on U.S. Companies, Workers, and the American Economy.")

#### **Patent Regulations**

The development of the Chinese patent system follows the goals specified in the 15-year MLP and the 12th Five-Year Plan (2011–2015). Provincial and municipal governments provide technical assistance for preparing patent applications as well as subsidies for patent application fees.<sup>248</sup> The Chinese government has encouraged state-owned enterprises (SOEs) to file numerous patents.<sup>249</sup> These measures have already made China's State Intellectual Property Office "the 3rd largest patent office in the world in terms of the number of invention patent applications received per year" and put it on track to become the largest patent office in the world by 2010.<sup>250</sup>

### **Policies Favoring Chinese Enterprises—Continued**

Skeptics have noted that many of these patents represent only small adjustments or changes from previous patents and are unlikely to foster substantial innovation. In the May 5, 2011, hearing before the Commission, Alan Wm. Wolff described many of these patents as “utility model patents, just having incremental technology change, requiring and getting no review.” In fact, even these seemingly mundane patents serve a particular purpose. According to Dieter Ernst, senior fellow at the East-West Center, “Chinese firms regularly file ‘utility patents’ on known products in order to prevent their original foreign developers from selling these products within China.”<sup>251</sup> Commissioners have also heard from American businesses in Beijing that Chinese companies can use these utility patents as reprisals for litigation in other areas. Chinese holders of utility patents can file a patent infringement case against a foreign competitor who has filed an infringement lawsuit outside of China.<sup>252</sup> The Chinese holder might expect to win in Chinese courts even if the case has no merit.

### **Technical Standards**

China has sought to impose Chinese technical standards on foreign competitors even in cases where widely accepted technical standards already exist. For example, China’s government created a third-generation mobile telecommunications standard, the Time Division Synchronous Code Division Multiple Access to compete with the U.S. CDMA (Code Division Multiple Access) and the European GSM (Global System for Multiple Communications) standards. The Chinese standard “requires firms to incur large costs to obtain access to the Chinese market as well as reduce the royalties that would otherwise accrue to U.S. firms and shift some royalties to Chinese firms,” according to Karen Laney, acting director of operations at the U.S. International Trade Commission.<sup>253</sup>

More recently, the Chinese government developed regulations to require testing and certification to Chinese standards for information and computer technology sold to Chinese government agencies. “These regulations require sellers to provide Chinese regulators with complete details of the inner workings—including information security functions such as encryption codes—of computer products in 13 product categories,” said Ms. Laney.<sup>254</sup>

### **High-level Dialogues Address the Indigenous Innovation Dispute**

Complaints by the U.S. business community and the Obama Administration to Chinese officials over the indigenous innovation policy and its link to official procurement catalogues placed the issue on the agenda for three high-level meetings during the past year. In December 2010, the Joint Commission on Commerce and Trade concluded with a promise by China to submit a revised proposal to join the WTO’s Agreement on Government Procurement. Previous Chinese proposals were rejected by other members of the GPA be-

cause Beijing had sought to exclude subcentral governments and SOEs even when the companies were performing government functions. At the conclusion of the talks in Washington, China agreed to provide equal treatment to companies operating in China and to refrain from measures to make the location or ownership of intellectual property a condition for eligibility for government procurement.<sup>255</sup>

USTR Ron Kirk, a co-chair of the 2010 U.S.-China Joint Commission on Commerce and Trade, concluded:

*China's announcement that it will not discriminate in government procurement decisions based on where the intellectual property component of the products was developed is a valuable outcome for America's innovators and entrepreneurs who can continue to create American jobs and selling to the Chinese Government without concern that they will be unfairly blocked from the market.*<sup>256</sup>

One month later, during the January summit between President Barack Obama and President Hu Jintao in Washington, the Chinese leader made further commitments to opening the government procurement market to foreign firms. In a U.S.-China Joint Statement, China agreed to “not link its innovation policies to the provision of government procurement preferences.”<sup>257</sup> At a joint press conference, President Obama said:

*I did also stress to President Hu that there has to be a level playing field for American companies competing in China that trade has to be fair. So I welcomed his commitment that American companies will not be discriminated against when they compete for Chinese government procurement contracts.*<sup>258</sup>

The third round of the Strategic and Economic Dialogue in May 2011 strengthened these promises with a further commitment that “China will revise Article 9 of the Draft Regulations Implementing the Government Procurement Law\* to eliminate the requirement to link indigenous innovation products to the provision of government procurement preferences.”<sup>259</sup> However, the U.S. Information Technology Office reports that it “continues to find current provincial and municipal policies that still require domestic intellectual property for government procurement preferences or otherwise give preferences to domestic products and the thematic underpinnings of China’s indigenous innovation drive remains strong in official rhetoric.”<sup>260</sup>

### **Chinese Policy Adjustments Following the High-level Dialogues**

In recent months, central authorities have announced steps to break the link between indigenous innovation preferences and government procurement. On June 23, China’s Ministry of Finance rescinded a 2007 series of measures concerning the evaluation, budg-

\* Article 9 states, “Government procurement agencies should strictly enforce the government procurement product catalogue and carry out all relevant policies and regulations.”

eting, and contract management of government procurement of indigenous innovation projects.\* The revoked measures included:

- Price credits of 5 to 10 percent for indigenous products during the evaluation process.
- Extra credits in the evaluation of the price point and technology of indigenous products.
- Priority given to indigenous suppliers unless their products exceed the quoted price for nonaccredited goods by 5 to 10 percent.
- The transfer of core technology as a requirement for foreign suppliers entering government procurement contracts.<sup>261</sup>

On July 4, 2011, the Chinese Ministry of Finance, the Ministry of Science and Technology, and the NDRC announced the repeal of the 2006 measure *Trial Measures for the Administration of the Accreditation of National Indigenous Innovation Products*.<sup>262</sup> The policy established specific certification criteria for the accreditation of indigenous innovation products, including the Chinese ownership of core intellectual property and trademarks.<sup>263</sup>

U.S. and European Union (EU) business organizations applauded these repeals yet remained careful not to overstate their significance. In a June 29 press release, the U.S.-China Business Council noted that while “the measures represent only a portion of the full list of regulations that tie indigenous innovation and government procurement, the elimination of these measures is an important step towards fulfilling pledges made by PRC [People’s Republic of China] leaders during President Hu Jintao’s January 2011 visit to the United States and the May 2011 Strategic and Economic Dialogue.”<sup>264</sup> Paul Ranjard, chair of the European Chamber’s Committee on Intellectual Property Rights, noted that central policy shifts do not always precipitate change at the provincial and municipal levels but said the repeal was “especially important because it is addressed to all levels of government departments, including provincial and municipal levels.”<sup>265</sup>

In some cases, however, local governments responded immediately to the central policy repeals with corresponding adjustments to local policies or practices. A report summarizing the Jiangsu Province semiannual conference on the government procurement of indigenous products held in Nanjing on July 17 emphasized the provincial government’s commitment to incorporate national-level policy revisions into the province’s procurement protocol.<sup>266</sup> The vice minister of the Jiangsu Ministry of Finance, the conference’s most distinguished participant, called on all members of government in attendance to review the implementation of provincial procurement policies in light of the central policy revision.<sup>267</sup>

Some of China’s large municipalities also were quick to step in line with central policy adjustments. Following the repeals of the central-level policies, both Shanghai and Xiamen municipal authorities effectively suspended accreditation programs for indige-

---

\*The three measures are *Evaluation Measures on Indigenous Innovation Products for Government Procurement*, *Administrative Measures on Budgeting for Government Procurement Contracts for Indigenous Innovation Products*, and *Administrative Measures on Government Procurement Contracts for Indigenous Innovation Products*.



nous innovation products. The Shanghai Finance Bureau announced that on July 1 it would cease implementing the 2009 *Shanghai Municipality Operating Procedures on the Government Procurement of Indigenous Innovation Products*.<sup>268</sup> While the repeal of this law is significant, the Shanghai municipal government did not announce plans to repeal a more recent law dictating product accreditation, the 2010 *Shanghai Municipality Measures for the Administration of the Accreditation of Indigenous Innovation Products*. Among the accreditation requirements of the 2010 measure, products must hold indigenous intellectual property rights developed by Chinese companies.

### **Will the Promises Be Kept?**

U.S. politicians, businessmen, and academics have expressed doubt that China's central and subcentral governments will comply with commitments made during high-level dialogues. Following President Hu's visit, then Commerce Secretary Gary Locke noted that when he talked to U.S. business leaders, "they continue to voice significant concerns; the fundamental problem often boils down to the distance between the promise of China's government and its actions."<sup>269</sup>

Months later, in a speech before the Asia Society in May 2011, Mr. Locke noted a history of noncompliance by China: "The Chinese pledges—at the S&ED [Strategic and Economic Dialogue] two years ago and at last year's JCCT [Joint Commission on Commerce and Trade]—that they would lift prohibitions in the revised catalogue on many industries in which U.S. firms are world leaders and have much to offer the Chinese economy. . . . Well, the new foreign investment catalogue falls far short of that promise."<sup>270</sup>

At the Commission's March 30 hearing, Theodore Moran, who holds the Marcus Wallenberg Chair in International Business and Finance at Georgetown University's School of Foreign Service, also expressed skepticism: If China "heads in that direction, I think that would be spectacular," he said. "But there are so many interests trying to force technology transfer that I'll believe it when I see it."<sup>271</sup> Mr. Ernst warned at the Commission's June 15 hearing that China may instead follow a well-established pattern of promising much but delivering little:

*A detailed analysis of recent developments of China's innovation policies finds a fairly consistent pattern of China's response to foreign complaints. In round one PRC [People's Republic of China] government regulations start out with quite demanding requirements that exceed established international norms. This typically gives rise to a wave of criticism from foreign enterprises and business organizations, but also from Chinese companies that have established a significant position in the international market and that have begun to accumulate a reasonably broad portfolio of intellectual property rights. In response to this criticism, round two then leads to some adjustments in PRC government regulations that combine a selective relaxation of contested requirements with persistent ambiguity.*<sup>272</sup>



Despite these promising examples, many local governments may still favor domestic companies for government procurement contracts. Without a strict requirement that local government procurement policy reflect changes made at the central level, provincial and municipal governments can favor domestic products, partially nullifying the expected improvements to the procurement environment for foreign firms in China. An article on the Finance Ministry's website reported that many representatives of provincial-level government procurement offices believe repealing central government policies that discriminate against foreign firms will not change the propensity of local governments to favor domestic goods.<sup>273</sup> For example, only two days after the last central policy repeal went into effect, the Shenzhen Science, Industry, Trade and Information Technology Committee officially called for support of indigenous innovation policies. Specifically, it called on reporting enterprises—those applying for product accreditation—to adhere to the *Shenzhen Municipality Measures for the Administration of the Accreditation of Indigenous Innovation Products*, Shenzhen's municipal counterpart to the already repealed national regulation.

Commerce Secretary Locke, who is now the U.S. ambassador to the People's Republic of China, anticipated the difficulty of implementing agreements made with China's central government only. Ambassador Locke outlined five key steps for the China's promises to become reality:

1. Chinese officials pledge to resolve the issue of market access
2. The agreement is codified into binding laws or regulations
3. The law is strictly implemented by the central government
4. The law is strictly implemented at local and provincial levels
5. The law or regulation becomes standard practice in China<sup>274</sup>

Speaking of China's current progress, then Secretary Locke remarked, "When it comes to indigenous innovation, intellectual property, or a variety of other market-access issues, an enduring frustration is that in too many cases only the earliest steps are taken, but not all five." Recent developments support this claim. While the Chinese government did make promises (step 1) and has begun efforts to reflect those promises in policy decisions (step 2), China continues to struggle to translate policy changes into institutional reform. The central policy repeals, although a political victory for the United States and Europe, will do very little for U.S. and European businesses without strict implementation by the central government and equally firm commitments from local authorities.

#### **China in Search of Western Technology: A Case Study**

While China has refrained since 2001 from explicitly requiring foreign companies operating in China to share technology and trade secrets, the Chinese government still seeks to obtain critical information on cutting-edge technology by other means. One example involves the Chevrolet Volt, a plug-in hybrid that employs three important technologies sought by the Chinese government: electric motors; complex electronic controls; and power storage devices, including batteries and fuel cells.

**China in Search of Western Technology: A Case Study—  
*Continued***

The Chinese government has refused to extend to General Motors (GM) a \$19,300 per car subsidy that is available to Chinese competitors unless GM provides its core technology to a Chinese car company. Thus far, GM has refused, even though the Chinese subsidy is nearly half the sales price of the Volt in the United States, \$41,000.<sup>275</sup> The car has not yet been priced in the Chinese market. Lacking the subsidy, GM would likely find it difficult to sell the Volt against its Chinese competitor, BYD, which manufactures two versions of a plug-in electric car. Complicating GM's dilemma is the fact that the Chinese market for auto sales is now the world's largest and the fastest growing, and GM is the largest foreign manufacturer in China. Said GM Chief Executive Officer Dan Akerson: "There are technology risks, there are relationship risks. I am sure China will do what's best for China. ... But you ignore China at your own peril."<sup>276</sup>

Meanwhile, GM has an eye on its major Detroit rival, the Ford Motor Company, which has announced plans to build four new plants in China and roll out 15 new vehicles there by the end of 2015. That move would double its capacity in China. Ford has not yet decided how much of its technology it would be willing to share in order to qualify for the subsidies.<sup>277</sup> The Chinese government is thus encouraging Ford and GM to compete on the basis of which company will surrender the most technology to Chinese rivals.

**Intellectual Property Infringement in China: The Business Software Case**

All members of the World Trade Organization, including China, are required to provide minimum levels of protection to the intellectual property of fellow WTO members. An agreement within the WTO specifically ensures that copyright protections extend to computer programs, which are protected as literary works under the amended Berne Convention of 1886.<sup>278</sup> The People's Republic of China agreed to enforce these widely recognized rules and regulations when it joined the WTO in 2001.

By nearly all accounts, however, the People's Republic of China is one of the largest sources in the world of counterfeit and pirated goods. China in 2011 remains first on the "priority watch list," a designation shared with 11 other countries, which are among the world's worst enforcers of intellectual property rights, according to the Office of the U.S. Trade Representative.<sup>279</sup> The Chinese government itself estimates that "counterfeits constitute between 15 percent and 20 percent of all products made in China and are equivalent to about 8 percent of China's GDP [gross domestic product]."<sup>280</sup>

China is by far the dominant source of counterfeit and pirated goods that U.S. customs agents seize at ports and airports around the United States. According to U.S. Customs and Border Protection, Chinese-sourced goods accounted for 53 percent of the sei-

zures at U.S. ports of entry in 2010, up from 6 percent in 1995. The second-largest number of seizures originated from Hong Kong.<sup>281</sup> It is likely that many of the illicit goods from Hong Kong actually originated on the mainland; in all, more than three-quarters of the seizures of infringing goods were from mainland China and Hong Kong in 2010.<sup>282</sup>

### **The Importance of Intellectual Property to the U.S. Economy**

Intellectual property plays a key role in creating high-wage jobs and fueling new economic growth. Much of the U.S. economy consists of intellectual assets such as patents, copyrights, and trademarks. These assets compose an estimated 76 percent of the *Fortune 100*'s total market capitalization and approximately 80 percent of the value of the Standard & Poor's 500.<sup>283</sup> Within the United States, intellectual property-intensive companies generated nearly \$7.7 trillion in gross output in 2008, totaling a third of U.S. total gross output.<sup>284</sup>

Intellectual property-intensive industries are particularly critical in the tradable goods\* sector and accounted for 60 percent of all U.S. exports in 2007, a total of \$910 billion.<sup>285</sup> Intellectual property-intensive industries also provide high wages. Between 2000 and 2007, the salary of all workers in intellectual property-intensive industries was on average about 60 percent higher than their counterparts at nonintellectual property-intensive industries.<sup>286</sup>

Major copyright industries—including software—contribute nearly 6.5 percent of the total U.S. gross domestic product (GDP), employ over 5.5 million workers, and generate more than \$125 billion annually in foreign sales and exports.<sup>287</sup> Solely looking at software, in 2010, “the direct, commercial value of stolen software tools for personal computers came to \$59 billion globally ... [and] the indirect costs are even greater. Enterprise software theft undercuts legitimate business activity and imperils job creation in every sector of the economy.”<sup>288</sup>

Business associations also list China as among the largest sources of intellectual property infringement. An estimated 78 percent of the software on personal computers in China is pirated, according to an annual study by the Business Software Alliance. That figure was down from 82 percent in 2006, but the total commercial value of unlicensed software on mainland Chinese computers rose from \$5.4 billion in 2006 to \$7.8 billion in 2010.<sup>289</sup> Hong Kong's piracy rate was considerably lower than on the mainland—45 percent in 2010.<sup>290</sup> Further evidence that China is a large-scale source of piracy: China was the second-largest market for computer hardware in the world—\$64.4 billion in 2009, behind only the United States. But in terms of software sales, China was eighth—behind Canada and Italy, at \$5.4 billion.<sup>291</sup>

The International Intellectual Property Alliance reports that China's lack of enforcement and lack of market access “suggest a con-

\*Tradeable goods are those that can be exported or imported.

scious policy seeking to drive Chinese competitiveness while permitting free access to foreign content through unapproved pirate channels.”<sup>292</sup> Says the Alliance:

*High copyright piracy levels persist in China, from pervasive use of unlicensed software by businesses and pre-installation of unlicensed software (hard disk loading piracy) at the distribution level, to widespread online piracy of music, films, television programming and other copyright materials, and piracy of hard goods. ... China's principal reliance on its woefully under resourced administrative system to deal with IPR [intellectual property rights] infringements rather than through criminal enforcement presents a significant hurdle to effective enforcement.*<sup>293</sup>

Among the remedies suggested by the United States and required by the WTO<sup>294</sup> during negotiations with China is the greater use of criminal penalties rather than administrative fines, which are too often levied at a nominal rate and are absorbed by Chinese counterfeiters as a cost of doing business.

#### **A Case Study: The Rise of Internet Piracy in China**

The increased use of the Internet to market and to sell products and services has also created a new and hard-to-trace pathway for illicit sales of copyrighted software. The case of music piracy offers an illustration of how the Internet eventually could facilitate lawbreaking on a massive scale in other information technology sectors, such as business software. In the case of music, Chinese government statistics indicate that nearly 80 percent of listeners use the Internet to obtain music. And nearly all music downloads are pirated. “Legitimate [music] content is not made available in significant quantities online in China due to the prevalence of piracy, market access restrictions, and other discriminatory measures which effectively keep legitimate content out,” according to Michael Schlesinger of the International Intellectual Property Alliance.

In addition, music piracy in China is facilitated by official tolerance for websites, such as the search engine Baidu, that directs users to infringing content and is supported by advertising. The website has promised to end the practice of providing pirated music but only in the case of music with a Chinese copyright.<sup>295</sup> As a result, the International Intellectual Property Alliance estimates the piracy level for music in China on the web is 99 percent.<sup>296</sup> Many of the same websites and techniques used to distribute pirated music can be employed to distribute pirated business software, including Internet auction sites, peer-to-peer sites, BitTorrent sites, and social networking sites.<sup>297</sup>

China's 457 million Internet users constitute the largest group of computer users in the world, most of them with broadband connections. Two-thirds of them use mobile phones to surf the web for music downloads.

**A Case Study: The Rise of Internet Piracy in China—  
Continued**

The International Intellectual Property Alliance calculates the value of legitimate music sales in 2009 in China at \$94 million. By contrast, in Thailand, with just 5 percent of China's population and the same GDP per capita, sales were \$142 million. Legitimate sales in the United States were \$7.9 billion, about 7,000 times as much as in China.<sup>298</sup>

The trend of Internet piracy established for music downloads is having a spillover effect on business software, noted Commission witness Ken Wasch, president of the Software and Information Industry Association: "What we are finding increasingly is that China is becoming the primary source for illegal intellectual property goods of all kinds being distributed through Chinese servers."<sup>299</sup>

**China's Recent Efforts to Protect Software**

Chinese leaders made significant promises over the past 12 months to improve the level of intellectual property enforcement. At the December 2010 Joint Commission on Commerce and Trade negotiations in Washington and in the joint statement following the summit between President Obama and President Hu in January 2011, China's government committed to buy legitimate software licenses for central government agencies (although not provincial or local government offices.) The central government committed to a pilot program for 30 SOEs to increase the level of software licenses and agreed to audit central government agency budgets to ensure that they appropriated money for legitimate software purchases (although not to audit installed software nor to appoint independent auditors.)<sup>300</sup>

However, China has been making promises in bilateral negotiations to buy only licensed software for government offices since 2004 and during that time, the value of unlicensed software use in China rose from \$3.6 billion in 2004 to \$7.6 billion in 2009, according to Commission witness Mr. Schlesinger.<sup>301</sup>

China also announced in late 2010 that the government would conduct a six-month campaign against intellectual property theft, denoted the "Special Campaign to Strike IPR [intellectual property rights] Infringements and Counterfeit and Shoddy Goods." After complaints that such temporary campaigns in the past had produced a flurry of activity followed by a resumption of counterfeiting and piracy, the campaign was extended for three months until the end of June.

Skeptics noted that the timing coincided with the start of the Joint Commission on Commerce and Trade negotiations in Washington and that such a move might have been made for political reasons. One American businessman operating in China told the Commission during an interview in Hong Kong:

*The problem is that authorities preannounce, for example, six month crackdowns; this allows people to close up shop temporarily and get back in business later. More vagueness would help. Another problem is corruption. Local Party of-*



*officials are sometimes shareholders in counterfeiting companies. Other times, if a factory that produces counterfeit closes in a small city, 30 to 40 percent of the local population might become unemployed, which would reflect poorly upon the local government.*<sup>302</sup>

After Premier Hu's visit and the special campaign ran its original course, Business Software Alliance President and Chief Executive Officer Robert Holleyman told Congress that his member companies "report no significant uptick in sales to the Chinese government, in contrast to what had been expected in light of the commitments" made by China to boost government agencies' purchase of legal software.<sup>303</sup> In May, Mr. Holleyman told the U.S. International Trade Commission that "the towering piracy rate [in China] remains stagnant, the commercial value of it continues to rise, and US software companies are seeing very little in the way of new sales even though China's PC [personal computer] market is surging."<sup>304</sup>

Not all software companies were equally affected, however. One computer executive from a company that aggressively pursues court challenges in China of users of unlicensed operating system software told Commission members during an August trip to China that sales of software had increased by 7 percent in 2010. Still, said the executive, the company's revenue in China is only about 5 percent of the revenue in the United States, despite the fact that China is now the world's largest market for computer sales.<sup>305</sup>

Losses to U.S. software companies from intellectual property theft in China include the loss of royalty and licensing fees that would otherwise be paid to U.S. software firms such as Microsoft, Oracle, and Symantec. In fact, royalties and licensing fees are the most heavily impacted of all U.S. export receipts, since they are derived directly from the protection of intellectual property. The May 2011 U.S. International Trade Commission study notes that software makes up the largest share—nearly a third—of the total of all royalties and licensing fees that Chinese users paid to American companies.

The U.S. International Trade Commission calculated that an improvement in Chinese intellectual property protection would more than double the fees collected by U.S. software firms. Fees paid to U.S. software companies totaled \$737 million in 2009. That amount would increase by \$1 billion if China were to raise its intellectual property protections to the U.S. level.<sup>306</sup>

#### **Reciprocity in Intellectual Property Protection**

In testimony before the Commission on May 4, former U.S. Senator Slade Gorton cited the lack of incentives as the reason for China's failure to enforce intellectual property protections. "As a matter of fact," he said, "all the incentives are in the other direction. There's no real penalty for piracy, and there's a great deal of profit to be made by it." Mr. Gorton noted a troubling new trend—Chinese-produced, counterfeit business software is being exported to the United States and is now being purchased in "significant" numbers by American consumers.



**Reciprocity in Intellectual Property Protection—  
Continued**

The solution, said Mr. Gorton, is to levy a punitive tariff on all imports from China and other countries that fail to safeguard intellectual property. The tariff should exceed the value of trade lost to piracy and counterfeiting. While such a tariff “obviously violates various international trade agreements,” he said, “a country (such as China) with a \$273 billion trade surplus with the United States is never going to win a tit-for-tat exchange of tariffs or trade restrictions with us under those circumstances.”

The goal, said Mr. Gorton, would be to force countries to enforce their intellectual property protection laws so that U.S. companies would gain market access for legitimate products. Once their enforcement improved sufficiently, the tariff could be rescinded.<sup>307</sup>

**Implications for the United States**

China’s indigenous innovation policy is intended to restrict foreign access to the government procurement market or to require the transfer of critical technology to Chinese companies as the price of even limited market access. The result has been job loss in the United States and the transfer of technology to Chinese competitors. Many foreign firms, including those with affiliates in China, will be excluded from a large part of China’s market.

Indigenous innovation needs to be viewed in the larger context of China’s trade policies, which continue to violate the basic principles of the World Trade Organization: national treatment and free and fair market access. The U.S. Chamber of Commerce has said that China’s innovation policy:

*restricts the ability of American companies to access the market and compete in China and around the world by creating advantages for China’s state-owned enterprises and state-influenced champions, [and has] the potential to undermine significantly the innovative capacity of the American economy in key sectors [and] harm the competitiveness and livelihood of American business and the workers that they employ.*<sup>308</sup>

By most accounts, the Chinese government tolerates a very high level of intellectual property theft. In particular, China’s purchases of licensed computer software lag far behind its rapidly rising purchases of computer hardware. Chinese businesses and even government offices typically purchase unlicensed software or fail to obtain licenses for multiple copies of software. The result is a large loss of revenue and jobs in one of America’s most competitive industries.<sup>309</sup>

Longstanding rules of international commerce, including WTO standards, require countries to enforce internationally recognized standards of intellectual property. Nevertheless, the piracy of business software in China continues despite many promises to crack down on violations. This failure in China results from lax enforcement rather than the absence of regulations and laws prohibiting

intellectual property theft. The damage to the U.S. economy is measured in lost sales and lost jobs, not only in the software industry in the United States but also those U.S. domestic industries that use licensed software and compete against Chinese industries.

### Conclusions

- China's indigenous innovation policy is an outgrowth of the government's broad industrial policy and has been openly developed and documented through public plans and pronouncements, particularly the *National Medium- and Long-Term Plan for the Development of Science and Technology (2006-2020)*. The indigenous innovation policy seeks to nurture certain high-wage, high value-added industries designated by the government. Chinese firms are to be favored over foreign firms or China-based foreign affiliates in government procurement contracts. State-owned enterprises and municipal and provincial governments are also to show favoritism to Chinese domestic industries and businesses.
- Chinese officials, including President Hu, have pledged to modify China's indigenous innovation policy in response to protests from U.S. business leaders and top officials. Those promises have not been implemented at the local and provincial levels, however. China has a history of making promises and delivering little, particularly when doing as little as possible benefits the Chinese economy, as has been the case with China's promises to bring its intellectual property protections up to international standards and to cease requiring technology transfers from foreign firms.
- Foreign-invested enterprises seeking to be considered for government procurement contracts or public works projects are expected to file for patents and copyrights within China in order to qualify for preferential treatment in government contracting. Foreign affiliates risk the unintended transfer of their technology to Chinese firms if they do so, because of the nature of the Chinese intellectual property system and the lax enforcement of intellectual property laws and regulations in China.
- Although China agreed in 2001 to stop explicitly requiring foreign companies to surrender their technology to China in return for market access and investment opportunities, the government in Beijing still employs several tactics to coerce foreign firms to share trade secrets with Chinese competitors. China's industrial policy in general and its indigenous innovation policy in particular seek to circumvent accepted intellectual property protections and to extort technology from U.S. companies.
- In addition, the long effort by the central government to foster indigenous innovation is a message that will likely outlive any product catalogues. Restricting market access to domestic firms and requiring technology transfer as a cost for foreigners attempting to do business in China demonstrated the government's view that Chinese companies and governments are better off substituting domestic goods for imports.

## **SECTION 4: CHINA'S 12TH FIVE-YEAR PLAN AND TECHNOLOGY DEVELOPMENT AND TRANSFERS TO CHINA**

### **Introduction**

While China seeks to be considered a market-oriented economy, its government continues to engage in comprehensive economic planning, direction, support, and control. During the 2011 report cycle, the Commission examined various aspects of China's industrial policy and the implications it may have for U.S. companies competing for a share of the Chinese market. This section continues the discussion started in sections 2 and 3 of this Report, with a particular focus on China's newly adopted 12th Five-Year Plan (2011–2015). This section also addresses the policies aimed at helping China move up the manufacturing value-added chain, fostering strategic emerging industries (SEIs), which include new-generation information technology, high-end manufacturing, alternative energy, and biotechnology, and completing its transformation to a global technological powerhouse.

China's rapid industrialization and economic growth during the past 30 years has often been attributed to liberalization policies undertaken as part of its "reform and opening up" era. But that only tells half the story. Chinese economic development during the same period has relied extensively on a government-directed industrial policy to promote certain segments of the economy and support export-led growth. Many such policies are outlined in five-year plans that identify broad development goals. The process then develops regulations, guidelines, and tools to accomplish those objectives. Examples include providing subsidies to companies in select industries and encouraging foreign investment of money and technology in target sectors. Aaron L. Friedberg, professor at Princeton University, noted that "vital though imports have undoubtedly been, it is foreign direct investment that has served as the 'decisive catalyst' propelling China up the high-tech ladder."<sup>310</sup>

### **China's 12th Five-Year Plan**

China began implementing five-year plans in 1953 in order to align the economy with top policy goals and to communicate this directive throughout the government bureaucracy.<sup>311</sup> Five-year plans are designed to be roadmaps for regulators and provincial officials, who are responsible for their implementation and act as "key indicators of the directions and changes in development philosophy" at the highest levels of Chinese leadership, according to Cindy Fan, a professor at the University of California, Los Angeles.<sup>312</sup>

Like previous plans, the 12th Five-Year Plan ratified by the National People's Congress in March 2011 sets out a broad range of goals, policy prescriptions, and reform priorities.\* Unlike earlier plans, however, the 12th Five-Year Plan shifts its emphasis from enumerating hard production targets to describing broader principles, consistent with China's goal of economic rebalancing, and technological and scientific upgrading, especially in industrial production.<sup>313</sup>

The 12th Five-Year Plan attempts to restructure the Chinese economy by encouraging domestic consumption, developing the service sector, shifting to higher value-added manufacturing, conserving energy, and cleaning up the environment. Premier Wen Jiabao's annual address to the National People's Congress on March 5, 2011, the "Report on the Work of the Government," listed the expansion of domestic demand as a key aspect of the government's work in 2011.<sup>314</sup> This section will focus on economic restructuring and industrial upgrading.

### ***Economic Goals and Rebalancing***

Although China has maintained gross domestic product (GDP) growth averaging 10 percent for the past decade, this success was achieved largely due to massive fixed-asset investment† and policies aimed at boosting the export sector. During the past decade, exports and investment that supported export industries were the biggest contributors to China's gross domestic product (GDP) (see Addendum II: Figure 1). Household consumption, by contrast, stagnated (see Addendum II: Figure 1). Moreover, such reliance on investment-led growth resulted in personal disposable income falling as a share of GDP (see Addendum II: Figure 2), causing consumption to lag behind GDP growth.<sup>315</sup>

The Chinese government has long been aware that maintaining growth in an economy so substantially dependent on exports and fixed investment is unsustainable, as articulated by Premier Wen in 2007, when he called the Chinese economy "unstable, unbalanced, uncoordinated and unsustainable."<sup>316</sup> As Chinese economic growth slowed sharply in late 2008 when U.S. and European demand collapsed (together they account for over 40 percent of China's exports), the imperatives of rebalancing became clear.<sup>317</sup>

Fearful of economic instability, however, in the wake of the 2008 crisis, the Chinese government embarked on a massive fiscal and monetary stimulus program, which relied significantly on state-owned bank lending to boost growth. Banks lent out nearly \$1.5 trillion in 2009, leading to a massive investment boom that amounted to nearly 90 percent of GDP growth in the same year.<sup>318</sup> In short, China's dependence on investment and exports grew at a time when global demand for Chinese exports floundered.<sup>319</sup>

\* See Addendum I for a list of 11th and 12th Five-Year Plan key economic indicators.

† Fixed-asset investment includes land improvements (fences, ditches, drains, and so on); plant, machinery, and equipment purchases; and the construction of roads, railways, and the like, including schools, offices, hospitals, private residential dwellings, and commercial and industrial buildings.

### **Key Economic Targets of the 12th Five-Year Plan**

In the “Report on the Work of the Government,” Premier Wen has outlined the key economic targets of the 12th Five-Year Plan:<sup>320</sup>

- Annual GDP growth: 7 percent
- Increase service sector contribution to GDP by 4 percentage points, from 43 percent to 47 percent
- Increase per capita disposable income of urban and per capita net income of rural residents by 7 percent per annum
- Increase spending on research and development (R&D) to 2.2 percent of GDP [from 1.75 percent as of 2010]

**GDP Growth:** The 7 percent GDP growth target is aimed primarily at reining in the Chinese economy, which has been overheating. It is also a signal to provincial and local governments to focus on generating economically and environmentally sustainable growth rather than growth at any cost. China has been trying to accomplish this transition for many years, though with limited success. For example, the 11th Five-Year Plan similarly had a lower GDP growth target (7.5 percent) but achieved rates of nearly 11 percent.<sup>321</sup>

**Service Sector:** The 12th Five-Year Plan places an emphasis on moving away from labor-intensive and low-skilled manufacturing toward more sophisticated and capital-intensive production. As a result, China will need a new source of employment. China’s service sector is underdeveloped: in 2009 it accounted for just 42 percent of total GDP (compared to 54 percent for India and 57 percent for Taiwan).<sup>322</sup> It has the potential, however, to generate new urban jobs and absorb surplus rural labor.<sup>323</sup> According to Trevor Houser, an economist with the Rhodium Group, achieving such structural changes is the best way to meet long-term employment goals: “[I]f I invest a million RMB [renminbi] on services, I create three times more jobs than in the iron and steel sector . . . if you’re resource-constrained and desperate for new jobs [like China is], [being the] world steel mill is a losing strategy in a wide variety of ways.”<sup>324</sup> However, Premier Wen’s work report fails to address the implementation of his goals, that is, how China will actually encourage growth in service industries. (For more on the Chinese government’s concerns over unemployment and social stability, see chap. 1, sec. 5, of this Report.)

**Income:** The government views income inequality and the urban/rural divide as sources of potential social instability (see chap.1, sec. 5, of this Report for more). According to the Chinese government, the 12th Five-Year Plan is intended to help increase income through raises in minimum wages, with a particular focus at the low end of the pay scale.<sup>325</sup> However, boosting income does not guarantee that consumers will reduce precautionary savings. The 12th Five-Year Plan also contains a set of reform priorities, including improving the social safety net and providing low-cost housing, in the hope that this will lead Chinese households to reduce savings rates and increase consumption.<sup>326</sup>

In practice, five-year plans are constantly reviewed and revised over the course of five years.<sup>327</sup> Reversing years of economic policies aimed at growth at all costs will not be easy. Critics doubt the Chinese government's ability to overcome entrenched domestic interests to push through a reform agenda. The 12th Five-Year Plan does not indicate how the economy will become less reliant on capital spending, have more liberalized financial markets, or fundamentally shift China's global trade balance. According to Stephen Green, regional head of research at the Standard Chartered Bank in Shanghai, so far "[t]here's absolutely no sign that the percentage of investment in GDP is slowing. And there are no signs of liberalization of the service sector to allow the private sector to take a bigger share of the economy."<sup>328</sup>

Cornell University economist Eswar Prasad testified before the Commission that one reason that the 12th Five-Year Plan offers few details related to major structural changes, especially a shift to a consumption-driven economy, is the inherent tension between China's short- and long-term objectives. For example, while significantly raising wages would certainly boost domestic consumption, it would also drive up inflation.<sup>329</sup> Moreover, structural change would not be to everyone's benefit. As Dr. Prasad stated, "For the politically well-connected state-owned enterprise bosses, for many of the bank chairmen, this is actually a very good system because it keeps profits flowing into the state enterprises, into the banks."<sup>330</sup> With the leadership change next year, the Communist Party may be reluctant to upset the status quo.

In meetings with the Commissioners, Hong Kong-based journalists have noted that there is a contradiction at the heart of China's 12th Five-Year Plan: It aims to create domestic consumption but an active consumer class will mark a shift in power away from the government and state-owned enterprises (SOEs). Michael Pettis, professor of finance with Peking University's Guanghua School of Management, has pointed out that a key characteristic of China's development model is financial repression. The vast majority of household savings takes the form of bank deposits, while the vast majority of corporate financing takes the form of bank loans. With the lending and deposit rates set very low, household savings are used by the state to heavily subsidize the cost of capital. This amounts to a transfer from the household sector to favored borrowers.<sup>331</sup> Efforts to boost consumption will necessarily cut into household savings thus limiting the amount of the capital available for loans to SOEs and other state-supported entities.

### ***Industrial Upgrading and Strategic Emerging Industries***

For the first time, the 12th Five-Year Plan also makes explicit mention of SEIs. According to Dr. Roach, "the new plan targets a major move up the manufacturing value chain."<sup>332</sup> It focuses on the development and expansion of seven SEIs: New-generation information technology, high-end equipment manufacturing, advanced materials, alternative-fuel cars, energy conservation and environmental protection, alternative energy, and biotechnology. Within these industries, 37 projects have been identified, which are listed in Addendum III of this section. The goal is to take the SEIs



from a current combined share of 3 percent of Chinese GDP to 8 percent by 2015 and 15 percent by 2020.<sup>333</sup>

Willy Shih of the Harvard Business School told the Commission that the 12th Five-Year Plan is a “continuation of a long-term strategy of capability building that has been in place for decades” and is strongly aligned with other guiding policies from the central government, in particular, the National Medium- and Long-Term Plan for the Development of Science and Technology (MLP), issued in 2006. This plan articulated the goal of making China an innovation-oriented society.<sup>334</sup>

The 12th Five-Year Plan calls for funding SEI development and increasing the scale of government and capital-market investment in SEIs and proposes using various subsidization policies to support the SEIs. As with other five-year plan policies, the national five-year plan only provides general guidance, and regional governments are responsible for devising precise subsidies and policies. For example, in May 2011, the Taiyuan City government passed an “opinion” on speeding up the development of SEIs, which calls for various local government measures to enable SEIs to account for 20 percent or more of Taiyuan City GDP and develop locally branded SEIs worth 1 billion RMB (about \$157 million) or more by 2015.<sup>335</sup>

To achieve its SEI goals, the central and local government and private sectors would have to spend between \$600 billion and \$2.1 trillion over the next five years, according to industry experts’ estimates.<sup>336</sup> The central and local governments will likely combine this investment with preferential tax and procurement policies to ensure that Chinese firms emerge as global leaders, or “national champions,” in these industries within the next five years. Similar policies previously have been successful in establishing “national champions” in industries such as telecommunications, steel, and railway, although it is unclear how much of this success can be attributed to China’s domestic innovation and how much to technology transferred or illegally copied from foreign producers. For example, in the railway industry, China went from producing steam engines just over ten years ago to competing internationally, including a joint proposal with General Electric for constructing bullet trains in California.<sup>337</sup>

According to Ministry of Finance Chief of Staff Hu Jinglin, the ministry will actively use finance and taxation policy to support the development of the SEIs, including providing multiple channels for financing. The ministry will encourage its regional offices to develop relevant policies based upon local conditions and will encourage local governments to take a share in SEIs and actively develop investment funds.<sup>338</sup> According to the National Development and Research Commission’s draft, “Major Tasks and Measures for Economic and Social Development in 2011,” released during the Eleventh National People’s Congress on March 5, 2011:

*We will quickly formulate and implement a development plan and supporting policies for strategic emerging industries, set up a special fund for promoting their development, expand the scale of venture capital investment in them, formulate a guiding list for developing them, and work out industry standards for major emerging industries. We will*

*organize the implementation of industrial innovation and development projects, including those on National Broadband Internet Agenda, cloud computing, the Internet of Things, integrated circuits, flat-panel displays, space infrastructure, regional aircraft and industrialization of general aviation aircraft, as well as major application and demonstration, projects on the health of the people and on using information technology to benefit the people. We will advance national pilot programs and demonstrations for IT [information technology] promotion.<sup>339</sup>*

The 12th Five-Year Plan also includes the following, more precise goals for each of the seven SEIs:

<b>Innovation and development of new strategic industries<sup>340</sup></b>
<b>01 Energy conservation and environmental protection industries</b> —Implement major exemplary projects in energy conservation and environmental protection and promote the industrialization of efficient energy conservation, advanced environmental protection and resource recycling.
<b>02 New-generation IT [information technology] industry</b> —Construct new-generation mobile communication networks, the new-generation Internet, and digital broadcast and television networks. Implement exemplary application projects of the Internet of things and special industrialization projects of network products. Construct industrial bases of IC [integrated circuit], panel display, software, and information services.
<b>03 Biological industry</b> —Build databases of gene resources for pharmaceuticals, important plants and animals, and industrial microbial bacteria. Construct R&D [research and development] and industrialization bases for biopharmaceuticals and biomedical engineering products, biological breeding, testing, detection and fine breeding bases, and exemplary biomanufacturing application platforms.
<b>04 High-end equipment manufacturing industry</b> —Construct industrialization platforms for homemade trunk and feeder airplanes, general-purpose airplanes and helicopters, and a spatial infrastructure framework composed of navigation, remote sensing and communication satellites, and develop intelligent control systems, high-class numerically controlled machines, high-speed trains and urban rail traffic equipment, etc.
<b>05 New energy industry</b> —Construct industrial bases for new-generation nuclear power equipment, large wind power generating sets and parts, new assemblies of efficient solar power generation and heat utilization, biomass energy conversion and utilization technologies, and intelligent power grid equipment, and implement exemplary large-scale application projects of marine wind power, solar power, and biomass energy.
<b>06 New material industry</b> —Promote the R&D and industrialization of carbon fibers, semiconductor materials, high-temperature alloy materials, superconductive materials, high-performance rare earth materials and nanometer materials for aviation and spaceflight, energy and resources, traffic and transport, and major equipment.
<b>07 New-energy automobile industry</b> —Conduct R&D and large-scale commercialization demonstration projects for plug-in hybrid electric vehicles and pure electric vehicles, and promote industrialized application.

Four of these industries (biopharmaceuticals, high-end equipment manufacturing, new materials, and next-generation information technology) were previously identified as target industries in the 11th Five-Year Plan. Three of these industries align with sustainable growth (alternative energy, clean energy vehicles, and clean energy technology), and four industries align with moving up the value chain (biotechnology, new materials, next-generation information technology, and high-end manufacturing).<sup>341</sup> There is also overlap between the SEIs and industries the Chinese government previously identified as strategic or heavyweight, including information technology and automobiles. (For more information, see chap. 1, sec. 2, of this Report.)

## **Technology Development and Transfers to China**

### ***Upgrading Manufacturing and Industrial Policy***

Over the past several decades, Chinese exports to the United States have primarily been low-value, labor-intensive products such as toys and games, footwear, textiles, and apparel. However, since China entered the World Trade Organization (WTO) in 2001, an increasing proportion of U.S. imports from China have been more technologically advanced.<sup>342</sup> By far the largest growth sector in Chinese exports to the U.S. market since 2000 has been computer and electronic products, exploding from \$24.7 billion in 2000 to nearly \$132.8 billion in 2010.<sup>343</sup> (See chap.1, sec. 1, of this Report for more on China's exports of advanced technology products.)

But China's evident success in increasing exports of advanced technology does not tell the whole story. To some degree, China has become the assembler of parts produced throughout much of Asia. Assembly operations typically do not pay high wages nor do they represent the majority of the value added to a product along the line from research, design, parts supply, assembly, marketing, advertising, shipping, distribution, financing, retail sales, and servicing. There is a perception in China that opening the country to foreign investment has not led to improvement of domestic capabilities and that foreign technologies continue to dominate, with China "relegated to low value-added labor intensive roles."<sup>344</sup>

The Chinese government desires to become competitive in technology-intensive areas and has adopted a set of policies to achieve this. In October 2005, the Chinese Communist Party Central Committee met and elevated the importance of China's "indigenous innovation to a strategic level equal to Deng Xiaoping's 'reform and opening' policy," according to a comprehensive study of the evolution of the program.<sup>345</sup> The National Medium- and Long-Term Plan for the Development of Science and Technology followed in 2006 with the goal to "increase investments in research and development to 2.5 percent of GDP and reduce reliance on foreign technology by 9 percent by 2020."<sup>346</sup> At the time, China's reliance on foreign technology was estimated at 60 percent.<sup>347</sup>

The term "indigenous innovation" appears in both the 11th and 12th Five-Year Plans. In the 11th Five-Year Plan, strengthening "indigenous innovation" is listed as a "national strategy," and in the 12th Five-Year Plan it is included as a primary objective. According to Jia Qinglin, chairman of the Chinese People's Political

Consultative Conference National Committee, “The success of the 12th FYP [Five-Year Plan] (2011–2015) rests on science and technology and indigenous innovation capacity.”<sup>348</sup> To help promote “indigenous innovation,” the 12th Five-Year Plan has added a new target not present in the 11th Five-Year Plan: patents per 10,000 people. In 2010, there were 1.7 patents per 10,000 people in China; by 2015, the 12th Five-Year Plan anticipates nearly doubling that number to 3.3 patents per 10,000 people. (For more information on patents and indigenous innovation, see chap. 1, sec. 3, of this Report.)

In addition to patents, the 12th Five-Year Plan seeks to improve the international competitiveness of Chinese firms by upgrading and consolidating certain industries (especially high-polluting industries) and promoting mergers and investments in advanced manufacturing equipment and technology.<sup>349</sup> While not mentioned explicitly in the five-year plan, favored companies in China may receive various subsidies, such as inexpensive loans, tax benefits, utility services, and free land.<sup>350</sup> Moreover, even if China’s innovation strategy fails to achieve a broad range of innovation, by heavily investing in certain critical technologies, China could make innovative breakthroughs in those favored technologies.<sup>351</sup> For example, according to Christopher McNally of the East-West Center, state support has enabled hardware and software manufacturers like Huawei and ZTE to innovate.<sup>352</sup> And, according to the consulting firm McKinsey, Chinese innovation has contributed to such fields as pharmaceuticals, genetics, and structural biology.<sup>353</sup>

#### **Global Supply Chains, Innovation, and the Case of Apple Corporation**

A great majority of U.S. technology companies manufacture advanced technology products in China via networks of global (largely Asian) supply chains and then sell them in the United States. Such production often results in lower manufacturing costs, which benefits both U.S. companies and consumers. According to Wayne Morrison of the Congressional Research Service, “U.S. firms that use China as the final point of assembly for their products, or use Chinese-made inputs for production in the United States, are able to lower costs and become more globally competitive.”<sup>354</sup> Becoming more globally competitive allows U.S. companies to increase profits and market share and theoretically should facilitate the hiring of more employees, both in the United States and abroad. Such benefits are not always distributed equally. According to the U.S. Bureau of Economic Analysis, U.S. multilateral corporations cut their work forces in the United States by 2.9 million during the 1999–2009 decade while increasing employment overseas by 2.4 million.<sup>355</sup>

**Global Supply Chains, Innovation, and the Case of Apple Corporation—Continued**

Apple has become a go-to example of such a company. Apple neither manufactures nor assembles any of the components of its famous range of products, including iPods. Instead, components from a variety of suppliers are assembled by Foxconn, a Taiwanese contract manufacturer, at its plant in China. A 2009 study by researchers at the University of California-Irvine, has estimated that the iPod and its components accounted for about 41,000 jobs worldwide in 2006, of which about 27,000 were outside the United States (of which 19,160 were in manufacturing) and 14,000 within the United States (6,101 in engineering and other professional jobs and 7,789 in retail and other nonprofessional jobs).<sup>356</sup>

In the same study, however, the authors concluded that the professional jobs, such as those maintained by Apple in the United States, were “at risk on multiple fronts”:

*Many U.S. high-tech companies are investing in white-collar job creation offshore to tap pools of low-cost talent and gain access to growing markets. The offshore jobs often support high-value jobs in the U.S., but this may not always be the case. Also, when U.S. companies lose their innovation leadership, foreign competitors do not typically employ many engineers or other professionals in the U.S.*<sup>357</sup>

Apple’s success is due in great measure to the company’s emphasis on designing and marketing unique products to a loyal and technologically sophisticated clientele. Business experts typically rank the Apple brand as among the top brands in the world, along with Coca-Cola and IBM. The company has focused its efforts on innovation and in-house research and design far more than most technology companies. For example, according to Gary Pisano and Willy Shih of Harvard Business School, “nearly every U.S. brand of notebook computer, except Apple, is now designed in Asia, and the same is true for most cell phones and many other handheld electronic devices.”<sup>358</sup> Commission witness Ralph Gomory said that an economy based on the Apple model is “both unattainable and undesirable,” because (1) the huge profits generated by Apple are specific to the company and, in any event, “unlikely to last,” and (2) there would be only few high-paying jobs, with the rest in retail.<sup>359</sup>

***Technology Transfers***

The alternative to research-driven innovation is technology transfer. During their 2011 trip to China, the Commissioners heard from representatives of the American Chamber of Commerce in China that the Chinese government mandated technology transfer for some ventures. In the case of joint ventures, in particular, any concession made to the Chinese partner increases the likelihood of the venture being approved.



When joining the WTO, China agreed to the “elimination and cessation of enforcement of trade and foreign exchange balancing requirements, local content and export performance offsets and technology transfer requirements made effective through laws, regulations or other measures.”<sup>360</sup> China has circumvented these WTO obligations through a combination of local-content requirements, mandatory joint ventures, and forced technology transfers. Chinese policies since 2006 “limit investment by foreign companies as well as their access to China’s markets, stipulate a high degree of local content in equipment produced in the country, and force the transfer of proprietary technologies from foreign companies to their joint ventures with China’s state-owned enterprises.”<sup>361</sup>

Thomas Hout and Pankaj Ghemawat wrote in “China vs. the World: Whose Technology Is It?” of the ease with which China has circumvented the WTO rules:

*The WTO’s broad prohibitions on technology transfers and local-content requirements are more complex and easier to subvert than its rules pertaining to international trade in products. Furthermore, China hasn’t yet signed the level playing-field provisions covering government procurement; it claims that its policies don’t violate them, because the WTO allows domestic policy concerns to be accommodated in government purchases. Although the WTO prohibits mandatory technology transfers, the Chinese government maintains that incentivized transfers, whereby companies trade technology for market access, are purely business decisions.*<sup>362</sup>

China’s strategy has been successful because “U.S. industry has feared being locked out of the vast Chinese central, provincial and local government procurement markets.”<sup>363</sup> Dieter Ernst of the East-West Center has argued that foreign firms often must still compromise intellectual property in order to establish a presence in China.<sup>364</sup> Describing Chinese strategy for technological upgrading, Drs. Hout and Ghemawat noted that “Chinese officials have learned to tackle multinational companies, often forcing them to form joint ventures with its national champions and transfer the latest technology in exchange for current and future business opportunities.”<sup>365</sup>

Chinese industrial strategy appears to have become more aggressive since 2006. Drs. Hout and Ghemawat note in their research that:

*[S]ince 2006 the Chinese government has been implementing new policies that seek to appropriate technology from foreign multinationals in several technology-based industries, such as air transportation, power generation, highspeed rail, information technology, and now possibly electric automobiles. These rules limit investment by foreign companies as well as their access to China’s markets, stipulate a high degree of local content in equipment produced in the country, and force the transfer of proprietary technologies from foreign companies to their joint ventures with China’s state-owned enterprises. The new regulations are complex and ever changing. They reverse decades of grant-*



*ing foreign companies increasing access to Chinese markets and put CEOs [chief executive officers] in a terrible bind: They can either comply with the rules and share their technologies with Chinese competitors—or refuse and miss out on the world’s fastest-growing market.*<sup>366</sup>

In a recent example, the Chinese government is refusing to let the Chevy Volt qualify for subsidies totaling up to \$19,300 a car unless General Motors (GM) agrees to transfer the engineering secrets for one of the Volt’s three main technologies to a joint venture with a Chinese automaker.<sup>367</sup> Thus far, GM has refused to transfer the Volt technologies (in a separate case, GM has agreed to develop electric cars in China through a joint venture with a Chinese automaker).<sup>368</sup> The proposed Chinese subsidy rules in question cover new energy vehicles (one of the seven SEIs highlighted in the 12th Five-Year Plan), which China defines as including electric cars, plug-in hybrids, and fuel-cell cars. The three core technologies that China is most interested in acquiring through the subsidy provision are electric motors, complex electronic controls, and power storage devices, whether batteries or a fuel cell. At least one of those systems would need to be included in the technology transfer for a vehicle to qualify for the consumer subsidies. Several trade experts said such a Chinese requirement violates WTO rules.<sup>369</sup> (For more on GM’s negotiations with China on hybrid car technology see chap. 1, sec. 3, of this Report.)

The Chinese government also has sought to encourage multinational companies to invest in R&D in China. According to APCO’s James McGregor, “The government provides incentives for foreign-invested R&D centers, including exemptions of customs duties on imported equipment, as well as business and income tax deductions.”<sup>370</sup> Intellectual property lawyers Jason Cooper and Stephanie Chu of Alston & Bird argue that “innovation centers in China are finding robust funding available for their R&D-related expenses, [which] have already caused significant reverse brain drain from Silicon Valley and are also inducing many foreign corporations without previous ties to China into opening operations there.”<sup>371</sup> Table 1, below, shows R&D expenditures by majority-owned foreign affiliates of U.S. companies in China through 2008 (latest available). There are certain limitations to the data, however, including that the data do not cover R&D expenditures of non-majority-owned affiliates.

**Table 1: R&D Performed in China by Majority-owned Foreign Affiliates of U.S. Parent Companies (2000-2008)**  
(U.S. \$ million)

2000	2001	2002	2003	2004	2005	2006	2007	2008
\$506	*D	\$645	\$565	\$575	\$668	\$759	\$1,173	\$1,517

\* D indicates suppression to avoid disclosure of confidential information.

Source: Bureau of Economic Analysis, *U.S. Direct Investment Abroad (USDIA): Operations of U.S. Parent Companies and Their Foreign Affiliates* (Washington, DC: U.S. Department of Commerce, various BEA issues). <http://www.bea.gov/international/di1usdbal.htm>.

Many incremental design tasks are already delegated to Chinese engineers by multinational corporations, for example, through large, original equipment manufacturers.<sup>372</sup> According to the consulting firm McKinsey, as of January 2011 “foreign-invested com-

panies account[ed] for fully 7 percent of [R&D] spending [by large- and medium-sized enterprises], spread among nearly 1,500 R&D centers established by multinational companies.”<sup>373</sup> This includes major American firms like General Electric (GE) and Caterpillar.<sup>374</sup>

Witnesses at the Commission’s June 15 hearing disagreed about the threat to U.S. technological leadership and competitiveness posed by China’s efforts to move up the value-added chain. Commission witnesses Ralph Gomory and Leo Hindery viewed Chinese efforts with alarm. Philip Levy, another witness, contended that China’s industrial policies are self-harming and will sabotage China’s growth because “state-sponsored attempts to grab technological leadership” stifle the competitive environment, often generating sales but not real innovation.

According to Mr. Hindery, China’s demands that the United States and other developed countries’ advanced technology companies seeking to do business in China make massive transfers of their intellectual property “will, because of their perpetual ripple effects throughout our economy, ultimately ... be an even bigger drain on our economy than the direct offshoring of millions of American jobs over the last 15 years.”<sup>375</sup>

Dr. Levy, on the other hand, concluded that the government-dominated approach to technological development and innovation favored by the Chinese state was “stultifying” and “unlikely to achieve its objective of vaulting [China] to the forefront of global innovation.”<sup>376</sup> He cautioned, however, that while China’s policies do not threaten U.S. technological leadership in the long run, they do have the potential ability to impose substantial costs on U.S. businesses in the short run.

### **Outsourcing of Manufacturing**

China’s 12th Five-Year Plan is the latest example of China’s efforts to upgrade its technological capabilities and encourage production in China. There is considerable debate about whether Chinese industrial policies and outsourcing of manufacturing and R&D to China harm the United States. At the Commission’s June 15, 2011, hearing, the Commissioners heard testimony on China’s efforts move up the value-added chain and their implications for the United States.

According to Dr. Gomory, it is a “dangerous delusion” to maintain that Americans do not need manufacturing jobs and will instead focus on “design and innovation and let other nations do the grunt work.”<sup>377</sup> Dr. Gomory also cautioned that U.S. corporations are increasingly locating their R&D in China, which can have a further detrimental effect on U.S. economic growth. The “interests of our global corporations and the interests of our country have, in fact, diverged,” Dr. Gomory said.

Echoing this argument, Willy Shih wrote in the *Harvard Business Review* with Gary Pisano that:

### **Outsourcing of Manufacturing—Continued**

*[O]utsourcing has not stopped with low value tasks like simple assembly or circuit-board stuffing. Sophisticated engineering and manufacturing capabilities that underpin innovation in a wide range of products have been rapidly leaving, too. As a result, the U.S. has lost or is in the process of losing the knowledge, skilled people, and supplier infrastructure needed to manufacture many of the cutting-edge products it invented.* <sup>378</sup>

Mr. Hindery expressed a similar view, noting that a country as large and complex as the United States needed to maintain high rates of manufacturing employment.<sup>379</sup> He suggested that jobs such as administration and marketing, which are often proposed as alternatives to manufacturing jobs, would not be able to substitute for wealth creation generated by manufacturing.

Dr. Levy, however, urged caution in blaming China for the decline of U.S. manufacturing employment, noting that “we have seen in manufacturing ... a steady decline as a share of employment, dating back to 1979. This long predates China’s emergence ... [and] has probably much more to do with technological change ... [and] a dramatic increase in productivity [in the United States].”<sup>380</sup>

According to the U.S. Bureau of Labor Statistics, the number of U.S. manufacturing jobs fell by a third, from 12.2 million to 8.1 million, during the past decade.<sup>381</sup> The precise number of job losses that can be attributed to outsourcing to China is not known.

### **Implications for the United States**

The policy of indigenous innovation in government procurement, in particular state and local procurement, as well as forced technology transfers, poses a significant challenge to the ability of U.S. companies to export goods and services to China (see chap.1, sec. 3, of this Report for further discussion).

The Chinese government’s emphasis on technology development through technology transfer also poses multiple risks. At the Commission’s June 2011 hearing, witnesses expressed concern over whether U.S. companies’ transferring of technology to Chinese partners in exchange for market access or to be closer to the domestic market ultimately may lead to the growth of Chinese industries and the decline of U.S. equivalents.<sup>382</sup> Even if high-tech manufacturing activity in China has in the past largely been confined to low-value labor and basic engineering to the benefit of U.S. multinational companies, it is unlikely that this will always remain the case. According to Dr. Prasad, “The companies that hand over proprietary technology do so in the hope that they’ll be the ones to get the better end of the bargain. But so far the Chinese have come out ahead in most cases. Hope springs eternal, but it’s a very dangerous bargain to make.”<sup>383</sup>

Transfer of manufacturing and R&D facilities from the United States to China has the potential to damage U.S. competitiveness.

Dr. Shih has testified before the Commission that as a consequence of the long-term implications of outsourcing, as well as the faltering investment in research, the United States “has lost or is on the verge of losing” its collective R&D, engineering, and manufacturing capabilities that sustain innovation. With the loss of these capabilities, according to Dr. Shih, the United States will lose its ability to develop and manufacture many high-tech products.<sup>384</sup> With the transfer of manufacturing to China, vital innovation ecosystems in the United States are lost to Chinese competition.

The handing over of proprietary technology also raises questions about the impact on U.S. national security. For example, a report prepared for the Commission by the RAND Corporation stated that there is “no question . . . that foreign involvement in China’s aviation manufacturing industry is contributing to the development of China’s military aerospace capabilities.”<sup>385</sup> This contribution, the report states, is “increasing China’s ability and possibly its propensity to use force in ways that negatively affect U.S. interests and would increase the costs of resisting attempts to use such force.”<sup>386</sup> Dr. Shih cautioned that the United States “must prepare for the eventuality that we will have to source critical military technology abroad as more of our domestic capabilities wither away.”

A recent case that attracted much interest involves a 50–50 joint venture between GE Aviation and the systems branch of Aviation Industry Corporation of China (AVIC), a Chinese state-owned group corporation which has both civilian and military components. The joint venture will develop and market integrated avionics systems for the global civil aviation industry.<sup>387</sup> Members of Congress raised concerns that AVIC could divert U.S. commercial avionics technology to China’s military systems, as China has done with missile, jet, and satellite know-how.<sup>388</sup> On a voluntary basis GE has sought and received an official ruling from the U.S. government that the joint venture does not involve controlled military technology.\* In press statements and in a meeting with the Commissioners, GE has also noted that the joint venture will have in place several safeguards to prevent diversion of technology to China’s military. Examples of such safeguards include not hiring any AVIC personnel or other Chinese citizens who retain military- or intelligence-related employment or responsibilities, and having separate information technology systems and facility locations. Some U.S. security officials have commented anonymously in the press that such measures, especially relating to employment prohibitions, will be difficult to enforce.<sup>389</sup> (For more information on U.S. involvement with China’s aviation programs in 2011, see chap. 2, sec. 1, of this Report.)

For the U.S. economy more generally, the large-scale outsourcing of high-tech manufacturing activities may lead to a hollowing out of America’s industrial base (a diminishing of skills within the labor pool, supplier base, and infrastructure),<sup>390</sup> the outsourcing of high-wage professional jobs (in addition to assembly jobs),<sup>391</sup> and the inhibition of future U.S.-led innovation.<sup>392</sup>

---

\*The technology in question, the civilian version of the integrated modular avionics (IMA), does not require a license for exports to China.

According to Andy Grove, chief executive officer and later chairman at Intel from 1987 to 2005, as the “scaling process” (the process by which “technology goes from prototype to mass production”) has moved to China, it has taken the potential for future breakthroughs with it. Mr. Grove illustrates the danger of breaking “the chain of experience that is so important in technological evolution” with the example of advanced batteries:

*It has taken years and many false starts, but finally we are about to witness mass-produced electric cars and trucks. They all rely on lithium-ion batteries ... [and] the U.S. share of lithium-ion battery production is tiny ... The U.S. lost its lead in batteries 30 years ago when it stopped making consumer electronic devices. Whoever made batteries then gained the exposure and relationships needed to learn to supply batteries for the more demanding laptop PC [personal computer] market, and after that, for the even more demanding automobile market. U.S. companies did not participate in the first phase and consequently were not in the running for all that followed. I doubt they will ever catch up.*<sup>393</sup>

### Conclusions

- One of the main objectives of the 12th Five-Year Plan is to redirect China’s economy to one more focused on domestic consumption and less on exports and investment. The plan assumes that China’s growth would therefore be more balanced and sustainable. The plan also emphasizes higher value-added production and increased government support for domestic high-tech industries.
- There is cause for skepticism about China’s prospects for carrying out the rebalancing goals of the 12th Five-Year Plan. The Chinese government had similar goals in previous plans, but their implementation was sidelined in favor of pursuing higher export and investment growth.
- Increasing household consumption, a major goal of the 12th Five-Year Plan, and the subsequent emergence of a more assertive consumer class, may be in direct contradiction to the Chinese government’s policy of keeping economic power firmly in the hands of the state and may compromise lending to many vested interests, including SOEs and the export sector.
- The 12th Five-Year Plan also advocates a move up the manufacturing value chain with the explicit mention of seven strategic emerging industries: New-generation information technology, high-end equipment manufacturing, advanced materials, alternative-fuel cars, energy conservation and environmental protection, alternative energy, and biotechnology. These industries, which will receive targeted government support, have the potential to be a source of economic growth and advanced innovation.
- Analysts and foreign business leaders fear that the emphasis on industrial upgrading will lead to the introduction of new govern-

ment subsidies, which in turn will disadvantage foreign competitors.

- As part of its indigenous innovation policy, China incentivizes foreign companies to transfer technology in exchange for market access.
- Chinese government requirements that foreign corporations transfer technology to Chinese joint venture partners in exchange for market access violate written WTO prohibitions on forced technology transfers. The new requirements for technology transfer from foreign partners are often made in implicit rather than explicit terms, which may make challenging them in the WTO dispute procedure more difficult.



**Addendum I: Key Economic Indicators (11th and 12th Five-Year Plans)\***

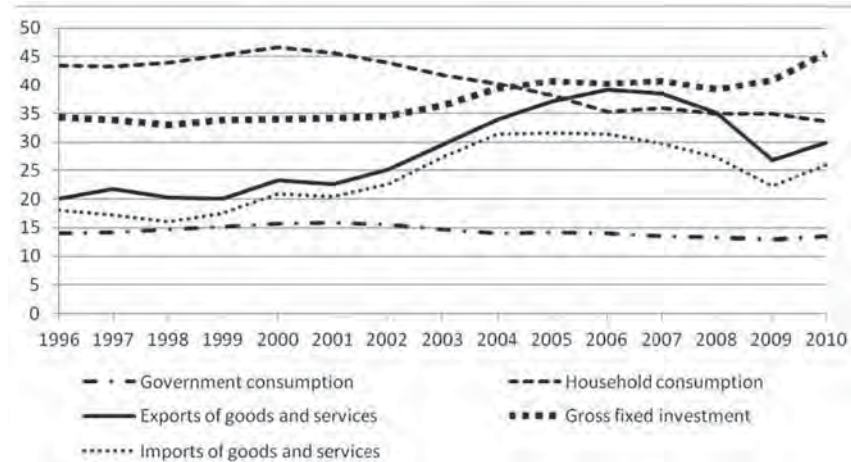
<b>Target</b>	<b>11th FYP (2010 Target)</b>	<b>2010 (Actual)</b>	<b>12th FYP (by 2015)</b>
Average GDP Growth	7.5% (E)	11.2%	7% (E)
Average GDP Growth Per Person	6.6% (E)	10.6%	N/A †
Service Sector as % of GDP	43.3% (E)	43%	47% (E)
Service Sector as % of Total Employment	35.3% (E)	34.8%	N/A
Urbanization (%)	47% (E)	47.5%	51.5% (E)
R&D as % of GDP	2% (E)	1.75%	2.2% (E)
Patents per 10,000 People	N/A	1.7	3.3 (E)
Strategic Industry as a % of GDP ‡	N/A	N/A	+8.0%
Average Educational Attainment	9 Years (E) (+0.5 Years)	9 Years	N/A
Rate of Nine-Year Compulsory Education Enrollment	N/A	89.7%	93% (R)
Rate of High School Enrollment	N/A	82.5%	87% (E)
New Urban Jobs Created (5-year total)	45 million (E)	57.71 million	45 million (E)
Urban Registered Unemployment Rate	5% (E)	4.1%	Under 5%
Urban Annual per Capita Disposable Income (RMB)	13,390 (+5%) (E)	19,109 (+9.7%)	>26,810 (>+7%) (E)
Rural Annual per Capita Income (RMB)	4,150 (+5%) (E)	5,919 (+8.9%)	>8,310 (>+7%) (E) ”

\* In the chart, restricted targets have an (R) next to them, and expected targets an (E).

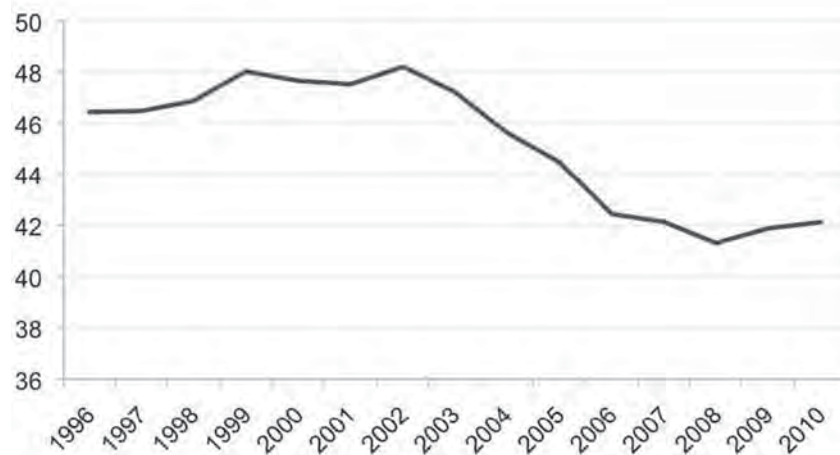
† N/A indicates that this was not a designated key indicator in the relevant Five-Year Plan.

‡ This is not officially included among key indicators in the Five-Year Plan but is instead only stated later in the plan. Therefore, it is neither “restricted” nor “expected.”

105

**Addendum II: Figures 1-2****Figure 1: Composition of China's GDP, 1996-2010**  
(as share of GDP; in percent)

Source: World Bank China data. <http://data.worldbank.org/country/china>. Note: Data for 2010 are Economist Intelligence Unit (EIU) estimates.

**Figure 2: Personal Disposable Income as Share of China's GDP, 1996-2010<sup>394</sup>**  
(in percent)

Source: EIU Country Data. Data for 2009 and 2010 are EIU estimates.

**Addendum III: China's Seven Strategic Emerging Industries and 37 Projects for Subindustries included in the 12th Five-Year Plan**<sup>395</sup>

Energy Saving and Environmental Protection	<ul style="list-style-type: none"> <li>• High-efficiency and energy saving</li> <li>• Advanced environmental protection</li> <li>• Recycling usage</li> <li>• Reusing waste products</li> </ul>
Next-generation IT	<ul style="list-style-type: none"> <li>• Next-generation mobile communications</li> <li>• Next-generation core Internet equipment</li> <li>• Smart devices</li> <li>• Internet of Things</li> <li>• Convergence of telecom / cable TV / Internet networks</li> <li>• Cloud computing</li> <li>• New Displays</li> <li>• Integrated circuits</li> <li>• High-end software</li> <li>• High-end Servers</li> <li>• Digitization of culture and creative industries</li> </ul>
Bio Industries	<ul style="list-style-type: none"> <li>• Bio-pharmaceuticals</li> <li>• Innovative pharmaceuticals</li> <li>• Biomedicine</li> <li>• Bio-agriculture</li> <li>• Bio-manufacturing</li> <li>• Marine biology</li> </ul>
High-end Assembly and Manufacturing Industries	<ul style="list-style-type: none"> <li>• Aerospace and space industries</li> <li>• Rail and transport</li> <li>• Ocean engineering</li> <li>• Smart assembly</li> </ul>
New Energy Sources	<ul style="list-style-type: none"> <li>• Nuclear power</li> <li>• Solar power</li> <li>• Wind power</li> <li>• Biomass power</li> <li>• Smart power grids</li> </ul>
New Materials	<ul style="list-style-type: none"> <li>• New function materials</li> <li>• Advanced structural materials</li> <li>• High performance composites</li> <li>• Generic base materials</li> </ul>
New Energy-Powered Cars	<ul style="list-style-type: none"> <li>• Electric hybrid cars</li> <li>• Pure electric cars</li> <li>• Fuel cell cars</li> </ul>

## SECTION 5: CHINA'S INTERNAL DILEMMAS

### Introduction

The Chinese Communist Party (CCP) and the central government in Beijing face a variety of challenges in maintaining control over a fractious and geographically vast nation. To do so, the party and the government have relied upon two principal strategies: a strict authoritarian rule to discourage challenges from potential political opponents and a record of 30 years of strong economic growth. Opposition parties are banned, senior government leaders are chosen by top Communist Party officials, and only village leaders are elected and even then, only from slates of officially approved candidates. In marked contrast to the social and economic turmoil of the era of Mao Zedong, central party leaders since 1978 have focused their efforts on delivering economic growth at an average 10 percent annual rate. In the process, China has lifted an estimated 400 million people from poverty.<sup>396</sup> Government policies have helped to establish China as the world's largest manufacturer and have fostered a small but growing middle class.

Continued Communist Party rule in China nevertheless remains a challenge for its leaders, who equate the success of the party with the existence of the nation.<sup>397</sup> The central government and the Communist Party face increasing protest from citizens outraged over government corruption, the failure of government regulators to protect the public from unsafe food, and environmental degradation. China's emerging entrepreneurial class has been accompanied by a growing income inequality between the wealthy urbanites and the poorer rural residents and between the coastal region and the interior and western provinces. "Even as the overall level of poverty has dropped, inequality has increased, and remaining poverty has become concentrated in rural and minority areas," notes the World Bank.<sup>398</sup>

Growing inflation particularly threatens lower-income workers, while China's system of residency permits, or *hukou*, creates a disadvantaged migrant worker class. Outbreaks of "mass unrest," which sometimes include violent demonstrations against the government and its policies, have increased from 8,700 incidents in 1998 to over 120,000 incidents in 2008, according to outside estimates.<sup>399</sup> Many such disputes involve illegal land seizures by local authorities, a growing source of income for corrupt local officials. Without recourse to an independent judiciary free of party control, Chinese citizens cannot rely on the courts to intercede on their behalf. In many cases, citizens feel that noisy and sometimes violent demonstrations are their only recourse. The government response to such demonstrations swings between repression and accommodation, seemingly without an overall direction.

On February 25, the Commission held a hearing and a roundtable discussion in Washington on these and other dilemmas faced by the CCP and by the central government. This section examines the origin of the problems faced by the party in maintaining control and describes the reaction of the Chinese citizens to the government's efforts to suppress dissent.

The party has created an extensive police and surveillance network to monitor its citizens and to forestall or react to any potential threat to social stability. However, the party still struggles to respond to the root causes of these protests, such as local corruption and the effects of rising food costs on the rural poor. Other current and potential causes of unrest include the unmet aspirations of the rural poor, the urban middle class, and college and technical school graduates unable to find work. Authorities in China are also concerned that a real estate bubble in the largest cities, particularly along the coast, may be followed by a market crash that could destroy the savings of the urban middle class.

### **Corruption and Abuses of Power**

Government and private sector corruption and abuse of power are prevalent in China, despite growing central government efforts to combat the problem.\* Among those efforts is a relaxation of government press controls on the reporting of cases of local government corruption and the harsh penalties assessed to government officials who take bribes or private businesses that sell adulterated food. Still, the problem persists.

Certainly, the public perceives corruption to be acute. Surveys of Chinese citizens found that 27 percent of respondents had been faced with arbitrary actions by a Chinese official, according to Martin Whyte, a Harvard sociologist who conducted the surveys and presented his findings to the Commission.<sup>400</sup> “[T]his finding suggests that such official mistreatment is a surprisingly common occurrence,” said Dr. Whyte. “We may hazard a generalization that many Chinese feel they now live in a society characterized by distributive justice but fairly widespread procedural injustice.”

In a 2010 ranking of corruption, based on surveys of public perceptions, China ranked 78th worst among 178 nations, sharing this position with Colombia, Greece, Lesotho, Peru, Serbia, and Thailand. According to Transparency International's 2010 Corruption Perception Index, China scored an overall rating of 3.5 on a scale of 0 (highly corrupt) to 10 (highly clean).<sup>401</sup> In comparison, the United States scored a 7.1, tying with Belgium for 22nd place.<sup>402</sup>

Official Chinese statistics, official news accounts, and regulatory efforts also reveal a high incidence of corruption—with over 240,000 official corruption cases investigated from 2003 to 2009, ac-

---

\*Transparency International defines corruption as “the abuse of entrusted power for private gain.” [http://www.transparency.org/news\\_room/faq/corruption\\_faq](http://www.transparency.org/news_room/faq/corruption_faq). The Millenium Challenge Corporation defines a corrupt practice as “the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the actions of a public official ... in the selection process or in contract execution, or the making of any payment to any third party, in connection with or in furtherance of a contract, in violation of the Foreign Corrupt Practices Act, or any other actions taken that otherwise would be in violation of the Act if the Act were applicable, or any applicable law in the (relevant) country.” <http://www.mcc.gov/documents/guidance/mcc-policy-fraudandcorruption.pdf>. Most definitions include fraud and extortion and theft by government officials of public or private funds or assets, including the seizure by government officials of private land without adequate compensation.

according to China's State Council.<sup>403</sup> From January to November 2010, 113,000 officials received some form of punishment related to corruption.<sup>404</sup> In December 2010 alone, Chinese media reported five cases of local officials murdering their mistresses in an attempt to avoid being exposed for corruption or for infidelity.<sup>405</sup>

Accounts in the Chinese news media and on the Internet have focused on the growing numbers of officials who kept mistresses on government salaries padded with misappropriated funds. In July, Xu Maiyong, former vice mayor of Hangzhou, was executed for bribery and embezzlement of more than \$30 million. The media reported that Mr. Xu had kept dozens of mistresses.<sup>406</sup> China's top prosecutor estimated in 2007 that 90 percent of the country's most senior officials implicated in corruption scandals in previous years had kept mistresses.<sup>407</sup> In a December 2010 report, the State Council announced new rules aimed at preventing Chinese officials from funneling misappropriated funds, bribes, and other illegally accrued gains into the bank accounts of family members.<sup>408</sup> This method of embezzlement is the most common method for officials to hide extra income. Another method is simply to leave the country. The People's Bank of China estimates that 16,000 to 18,000 corrupt Chinese officials and executives at state-owned enterprises absconded with \$123 billion from China between the mid-1990s and 2008.<sup>409</sup>

Enforcement efforts often focus on local rather than central government officials and often involve the lack of due process in local regulatory decisions. Dr. Whyte testified that procedural injustice has drawn the most citizen ire:<sup>410</sup>

*In the growing body of research on social protest activity in China in recent years, it seems to me that almost always the sparks that set off popular anger and public protests are abuses of power and other procedural injustice issues, rather than distributive injustice complaints. ... However, by my reading, protest targets tend to be local officials, employers, and other powerful figures, rather than individuals who are simply very rich.*

Senior party officials are more frequently seen as a recourse to corrupt local governments. Chinese officials in the central government have worked to propagate this view among Chinese citizens, notes Dr. Whyte:<sup>411</sup>

*CCP leaders have also proved very adept at taking credit for wise guidance of the economy and the improved living standards of ordinary Chinese citizens, while being perhaps even more obsessed with deflecting blame for procedural abuses onto local officials and bosses rather than on the system itself (and its top leaders). As a result, China displays a 'trust differential' that is common in many authoritarian regimes (although not in Tunisia and Egypt recently). Many citizens get angry at arbitrary and unfair actions of local authorities while having more faith in the central leadership, to whom they direct complaints and appeals in the hope that 'grandpa' Wen Jiabao or other top leaders will intervene and set things right.*



One of the most recent examples did not directly involve a Chinese official, but it quickly came to symbolize the suspicion by ordinary Chinese that the justice system is rigged against them, particularly in disputes between citizens and officialdom. As Li Qiming, 23, was driving recklessly through Hebei University in October 2010, he struck two female pedestrians, killing one 20-year old student and injuring the other. As the drunken Mr. Li tried to flee the scene, he yelled out, “Sue me if you dare, my father is Li Gang.”<sup>412</sup> (Li Gang was a deputy chief of security in the university’s district.) Authorities censored news reports about the incident, but the declaration became a popular rallying cry of Chinese citizens in online posts about Chinese corruption. The son was given a relatively light sentence of six years in prison after the Li family paid \$84,000 in restitution.

Chinese Internet users also highlighted the death of Qian Yunhui, a village leader in Yueqing who had been carrying on a six-year fight with local officials over land seizures. Witnesses reported that four security officers held down Mr. Qian as a truck drove over him. Officials initially described the death as an unfortunate traffic accident.<sup>413</sup> Photos of the scene refuted the official account, showing that Mr. Qian was perpendicular to the truck and that there was no damage to the front of the truck. Even after the truck driver was found guilty and sentenced to three-and-a-half years in prison, Chinese Internet users continue to discuss the incident and remain suspicious of the police and judicial forces involved in the investigation.

The Internet continues to be a useful tool both for the central government and citizens in the fight against local corruption. *China Daily*, a CCP-controlled newspaper with print and Internet editions, will cover instances of crackdowns on abuses of power and corruption and has commented in a positive vein on citizen whistleblowers who target local corruption. The state-owned *Beijing News* revealed that public security officials in Xintai City had been committing to mental institutions residents who protested official corruption or the unfair seizure of their property.<sup>414</sup> In March, *China Daily* published a survey paid for by the Ministry of Industry and Information Technology that was critical of local government websites for lack of information and access to officials. The survey of 450,000 citizens showed that 78 percent were “very unsatisfied” with local web portals.<sup>415</sup> A February article announced an audit of local land use regulators in an effort to stop illegal seizures of rural land.<sup>416</sup> The newspaper also noted that a position reserved for a former city official’s son had been eliminated after Internet protests that local government officials favor hiring the children of senior officials.<sup>417</sup>

The party has attempted to draw a sharp distinction between local officials, who are sometimes portrayed as corrupt, and central party leaders, who are portrayed as trying to end corruption. For example, the central government issued new rules in March on foreign travel by Chinese central government officials to prohibit non-business-related excursions, according to one news report.<sup>418</sup> In contrast to local officials who may line their pockets and fill the municipal coffers with the proceeds of forced sales of land, the government limits the property ownership rights of State Council

members. Commission witness Yukon Huang, from the Carnegie Endowment for International Peace, refers to this official mandate of transparency as the “fishbowl” for top Chinese leaders.<sup>419</sup> The trade-off, said Dr. Huang, is that top officials “be subjected to scrutiny in exchange for assuming power.”<sup>420</sup> He continued:

*When they assume those positions [they] have given up their ability to operate in the economy. They can't earn income; they can't give speeches; they don't own property; they can't even travel without someone signing off on them. When they leave and retire, you don't hear of them anymore. They can't do anything.*<sup>421</sup>

However, this fishbowl does not extend to the families of State Council members, Dr. Huang said. The children and families of Chinese officials regularly own businesses and earn income. Family members are still able to benefit from business and political connections.

Despite such efforts at reform, corruption remains a significant issue even among higher-ranking officials. In one recent example, Liu Zhijun, the former party chief of the Ministry of Railways, was dismissed from his position and placed under investigation for “severe violation of discipline,” a charge frequently used in cases of corruption.<sup>422</sup> The next month, Zhang Shuguang, the Railways Ministry deputy chief engineer, was also dismissed and investigated for corruption. *China Daily* reported that an audit found that at least \$28 million of the Beijing-Shanghai high-speed railway project had been misappropriated through “fake invoices, faulty bidding procedures and mismanagement.”<sup>423</sup> China’s newest rail system drew increased scrutiny after a collision between two bullet trains on July 23 killed 40 people. The state-owned China North Locomotive and Rolling Stock Company admitted that an automatic safety system had malfunctioned.<sup>424</sup> Onlookers were punished for photographing the site, and journalists were prohibited, in some cases, from initially reporting on the accident.

According to Xinhua, the official news agency, 11 ministerial-level officials were sentenced for corruption convictions to life imprisonment or faced other severe punishments in 2010.<sup>425</sup> Even so, officials have an easier time getting their sentences reduced. Xinhua reported that 20–30 percent of prisoners receive a reduced sentence, while convicted officials are given reduced sentences in 70 percent of the cases.<sup>426</sup> A common punishment for high-ranking officials guilty of corruption is a death sentence with a two-year reprieve. While seemingly harsh, this sentence can be legally reduced to life in prison and further commuted to “no less than 12 years for good behavior or contributing to society.” In the first five months of 2011 alone, at least four high-ranking officials were found guilty of corruption charges and sentenced to death with a two-year reprieve. These included former mayor of Shenzhen Xu Zongheng,<sup>427</sup> former Dangchang County Communist Party Chief Wang Xianmin,<sup>428</sup> former Deputy Director of Shanghai’s municipal housing support and building administration bureau Tao Xiaoxing,<sup>429</sup> and former Vice President of the Superior People’s Court of Chongqing Municipality Zhang Tao.<sup>430</sup>

After personal encounters with corrupt officials and institutions, Chinese citizens are becoming increasingly discouraged and aggravated by abuse of power even as the government works to demonstrate competency in reducing corruption at all levels. Given the regime change of the Arab Spring in the Middle East, the Chinese government is keenly aware of the potential that corruption has in serving as a rallying point of discontent under which dissatisfied citizens can gather, Dr. Huang told the Commission:<sup>431</sup>

*Much of this frustration is directed at failings that emanate from corruption and inconsistent application of the rule of law. Corruption in China is a major concern and source of potential internal instability. Even the senior leadership has recognized its seriousness in noting that if unchecked, it could threaten the credibility of the Party.*

### **Inflation**

The CCP faces the difficult challenge of maintaining a balance between growing too fast and overheating the economy, leading to price increases, or slowing growth to a level at which job creation lags behind the number of young adults entering the workforce. The problem for the party and the government is all the more difficult because China's central bank lacks the autonomy and the monetary tools to wage an all-out battle against inflation. Consumer prices increased by 6.1 percent in September, maintaining the fastest pace of inflation since the summer of 2008.<sup>432</sup> Particularly worrisome for Chinese officials was a 13.4 percent increase in food prices.

Food inflation also exacerbates the growing rural/urban wealth inequality divide. Food represents a larger percentage of overall consumption expenditures for rural households in China, 41 percent, than that of urban households, at 37 percent, according to official Chinese statistics.<sup>433</sup> By contrast, food expenditure in Japan averages 14 percent of household income and in the United States just 7 percent, according to UN statistics.<sup>434</sup>

Economic issues have been a large driver of protest in China. Sharp price rises were "perhaps the most pivotal factor" in the early days of the student protests in Tiananmen Square in 1989, Murray Scot Tanner, RAND Corporation senior political scientist, told the Commission. "If growth rates go below about 8 or 10 percent, [Chinese officials] think they're in trouble, but if the economy starts growing too fast and inflation starts taking over, that's been historically another source of unrest[.]"<sup>435</sup>

Nearly 22 years after the 1989 Tiananmen Square massacre, "the most powerful and widespread roots of discontent [are] unaffordable urban real estate followed by inflation—specifically rising commodity and food prices," noted Elizabeth Economy of the Council on Foreign Relations.<sup>436</sup> Several protests have already occurred in China as a result of increasing food and fuel costs. The government has largely relied on price controls to curb discontent, with mixed results. One demonstration against rising costs in April 2011 drew several hundred truck drivers to obstruct access to a Pudong district dock in Shanghai, China's most active port. The

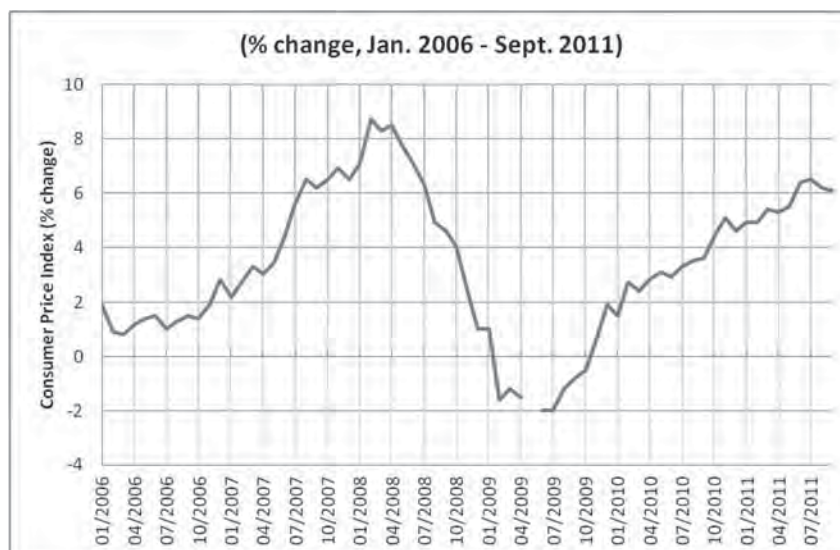
drivers cited increased fuel prices and new fees imposed by warehouse operators as the basis of their anger.<sup>437</sup> In response, the Shanghai Municipal Transport and Port Authority withdrew a fuel surcharge and reduced the cost of other related fees.<sup>438</sup>

While measures such as direct price controls are often effective in the short term in lowering specific costs, their effect is quickly dissipated as secondary or black markets spring up in response to shortages caused by hoarding or production cutbacks. In China, price reductions on energy also reduce the revenue of government-owned or -controlled energy companies, including coal mines. Managers of state-owned companies are expected to meet sales and revenue quotas at the same time that price controls reduce their company income. For example, oil and gasoline distributors suffer when their acquisition costs rise but their retail sales prices remain frozen by government fiat. Consequently, price controls are especially unpopular with government officials and state-owned businesses.

One way that the government has tried to hold down inflation is by pressuring companies to cancel price increases. The government has accused some foreign and domestic companies of “intensifying inflationary expectations among consumers” and “seriously disturbing market order.”<sup>439</sup> One such company, Unilever, was fined \$308,000 by the National Development and Reform Commission (NDRC) in March after announcing it planned to increase product prices by as much as 15 percent.<sup>440</sup> The announcement led to panic buying and hoarding among Chinese consumers and spurred the government to charge Unilever under its pricing law, which limits a company’s ability even to comment about future prices.<sup>441</sup> *China Daily* also reported that the NDRC instructed more than a dozen industry associations to postpone or call off planned price increases.<sup>442</sup>

China has a history of rapid price surges and strong but ultimately ineffective responses. In 2008, China registered a consumer price index that was 8 percent higher in the first quarter than during the same period in the previous year. In response, the government allowed the renminbi (RMB) to appreciate in order to lower the real costs of imports, raised the bank reserve requirement ratio to cut down on bank lending, and rejected requests for price hikes from several companies involved in the food industry.<sup>443</sup> Nevertheless, the consumer price index continued its climb and reached an 11-year high in November 2010, as the government froze the price of gasoline, natural gas, electricity, water heating, and urban public transport fees while setting temporary price controls on staples such as grain, edible oil, meat, milk, eggs, and liquefied petroleum gas.<sup>444</sup>

But the efforts to halt inflation did not keep prices from accelerating throughout 2011. Chinese officials reported that the inflation rate rose from 5.0 percent in the first quarter to a 6.3 percent rate in the third quarter. (See figure 1, below).<sup>445</sup>

**Figure 1: China's Consumer Price Index January 2006–September 2011**

Source: International Monetary Fund, accessed through CEIC Data Manager, *Consumer Price Index: % Change* (Washington, DC: May 31, 2011); *Trading Economics*, "China Inflation Rate at 6.1% in September" (New York, NY: October 14, 2011). <http://www.tradingeconomics.com/china/inflation-cpi>.

Despite the government's dramatic moves, inflation may even be higher than government figures show. China relies on an inflexible consumer price index to measure inflation.\* China's National Bureau of Statistics only updates the basket contents every five years, so it does not accurately capture current trends.<sup>446</sup> Commission witnesses suggested that Chinese methodology also fails to capture the true rate of inflation, perhaps deliberately.<sup>447</sup> While government-reported data may be erroneous, Dr. Economy noted that information on inflation in China is nevertheless available from a variety of nongovernmental sources including consumer-based tracking of foodstuff price increases, and those numbers are considerably higher:

*While the government may try to downplay the challenge of inflation or report specious numbers, postings by concerned citizens ensure that information is available from a number of sources. As one posting on a Chinese website noted, 'As a whole, food prices have risen 10.3 percent since this time last year. The price increases, however, are not uniform across the board. The price of wheat has risen 15.1 percent, the price of meat 10.9 percent, eggs 20.2 percent, water 11.1 percent, vegetables have risen 2 percent and fruits have shot up over 34.8 percent.'*<sup>448</sup>

\*The consumer price index examines trends in prices for a sample, or basket, of goods within an economy to determine inflation. China does not publish the list it uses, but economists believe that food is 30 percent of the index.



In addition to price controls, China has also used monetary policy in an attempt to lower the rate of inflation. Since October 2010, the central bank has boosted interest rates five times. The People's Bank also raised reserve requirements five times in 2011, bringing the cash reserve ratio to a record high of 21 percent.<sup>449</sup> By requiring banks to hold more money in reserve for each loan a bank makes, China hopes to slow lending and therefore economic growth. This may be a false hope, however, as "shadow banking" or unregulated loans to the private sector from hedge funds, insurance companies, and money market funds, among others, continue to undermine China's efforts to control lending.<sup>450</sup> In December 2010, Fitch Ratings released a report warning that "[l]ending has not moderated, it has merely found other channels ... [this] helps explain why inflation and property prices are still stubbornly high, why [third-quarter] GDP [gross domestic product] growth was stronger than expected."<sup>451</sup>

China has limited options for responding to inflation because of its steadfast policy of maintaining an undervalued RMB. This policy actually exacerbates China's inflationary problems by driving investment into manufacturing for exports and interfering with an important market mechanism, the appreciation of the RMB against other currencies, which would make imports cheaper, particularly manufacturing components and energy.

### **Income Inequality and *Hukou***

China faces a large and growing gap in income between its urban and rural populations and between its richest and poorest citizens. In 2010, the average urban citizens' overall income was 3.23 times greater than the average rural income.<sup>452</sup> Urban per-capita disposable income was 5,963 RMB in the first quarter of 2011, while rural residents' per-capita disposable income was less than half that amount, 2,187 RMB.<sup>453</sup> Urban citizens also have access to more jobs, sophisticated health care, better education, and available housing.

Another indicator of China's growing income disparity is its "Gini coefficient." The Gini coefficient is a measure of inequality. A score of 0 indicates total equality, while a score of 1 indicates maximum inequality. China's Gini coefficient rapidly increased from 0.215 20 years ago to 0.447 in 2001 and 0.490 in 2010.<sup>454</sup> China's income inequality is similar to that of the United States, Malaysia, and Singapore, Dr Huang noted to the Commission.<sup>455</sup> (By comparison, the United States also had a high Gini coefficient of 0.469 in 2009.)<sup>456</sup> But China's Gini coefficient may be understated because of China's generally unreliable statistical methods.

While China's official Gini coefficient of 0.490 is not excessively high, it does exceed what some characterize as the "danger" line of 0.4.<sup>457</sup> Dr. Huang characterized China's rate of growth as troubling for government authorities, because it means that China is facing a quickly bifurcating social structure.<sup>458</sup> Even the global recession did not change the trend. The number of "high net worth individuals" in China—defined as a person with \$1.5 million or more—doubled to 585,000 from 2008 to 2011.<sup>459</sup> Additionally, a report by the China Reform Foundation indicated that China's real Gini



score was actually considerably higher than the score quoted in official accounts. According to the *Wall Street Journal*:

*[A] landmark study earlier this year on unreported income ... found that hidden income totaled \$1.5 trillion, with 80 percent in the hands of the richest 20 percent. That would put China's Gini index at over 0.500, on par with many South American countries, and, if trends continue, headed for the income inequality of much of Africa.*<sup>460</sup>

The top income levels may be 3.2 percent wealthier than official data indicate, according to the study by economist and deputy director of the National Research Institute at the PRC's China Reform Foundation, Wang Xiaolu. Corruption may be one answer for the undercounting. Based on a detailed look at spending and income patterns in China in 2008, Dr. Wang estimates China's average urban household income is 90 percent higher than official data. His figures suggest the top 10 percent of Chinese households are 3.2 times richer than public data show, while the second decile income is 2.1 times higher.<sup>461</sup>

Other witnesses, however, were less concerned with the growing inequality, asserting that while the majority of Chinese citizens perceived income disparities as excessive, they did not feel that the gap was unfair. Noted Dr. Whyte:

*If income gaps widen but most people feel that the widened gaps are fair (as appears to be the case in our surveys), then feelings of inequity and injustice will not be generated. Contrary to some public statements in China, there is no Gini coefficient 'danger line' above which further widening of income gaps inevitably produces political turbulence.*<sup>462</sup>

Dr. Whyte did, however, find broad dissatisfaction among both urbanites and rural dwellers with the *hukou* registration system and its intrinsic tendency to produce inequality.<sup>463</sup> Created in its current form in 1960, China's modern *hukou* system was developed after 20 million migrants rushed to China's cities during the Great Leap Forward (1958–1960) in order to fill a perceived labor gap.<sup>464</sup> The *hukou* system was created to manage intracountry migration and requires the registration of all citizens in China at birth and then limits access to government services based on the residency permits issued after registration. Citizens' residency permits fall into one of two categories, urban or rural *hukou*, and entitle a holder access to social services in the town or city to which their *hukou* is registered.

Since *hukou* is hereditary, changing the designation of one's *hukou* is extremely difficult and requires either large amounts of money paid to well-connected officials or a specific exemption, such as admittance to an urban university. Individuals are more easily allowed to migrate downward, from a small city to a village, or horizontally, from small town to small town. This often occurs when a rural bride moves from her hometown to her husband's village.<sup>465</sup>

According to a 2010 Harvard University study:

*The hukou is the core of Chinese citizenship rights allocation, without which the state would not have been able to*

*curb rural-to-urban migration; the hukou is used to maintain the urban unit (danwei) system, to extract agricultural surplus (especially during the high Maoist period), and to enforce rigorous birth control measures (in the reform era), among other policy goals. ... Likewise, China's hukou system has persisted and evolved into an even more complicated matrix of governance during the market transition years.*<sup>466</sup>

Although rural migrants are a key part of the workforce for China's urban-based exporters, these transplanted workers must live as second-class citizens when in urban areas, due in part to their rural *hukou* status. Not only do migrant workers face discrimination and lower wages from employers, but their families also are restricted from access to government services, including education, Dr. Huang testified. In some areas, migrant workers are restricted from purchasing property and registering vehicles and are ineligible for subsidized housing and public health insurance programs.<sup>467</sup>

Migrant workers in urban areas therefore live very basic lifestyles and tend to have high rates of saving. This allows migrant workers to maximize the amount they can send home and to accrue funds to cover healthcare, housing, and education costs.

According to the 2010 national census, more than 260 million Chinese citizens are a part of the "floating population" and do not live in the area designated on their *hukou*.<sup>468</sup> In Beijing alone, one in three residents is a migrant. This is a significant increase when compared with the year 2000's ratio of one in five.<sup>469</sup> Similarly, Shanghai's migrant population accounts for approximately 39 percent of the city's total population, an increase of 159 percent since 2000.<sup>470</sup> For both cities, migrants have been both a burden and an asset. On the one hand, the influx of migrants has taxed local transportation and healthcare facilities. On the other hand, migrants have reduced labor shortages in Shanghai and alleviated Beijing's aging population issue.

This dichotomy has made it difficult for the central government to overcome objections from municipalities to ending the *hukou* system. The Chinese government at the central and local levels has begun to address some of the problems, with mixed results. Healthcare has been expanded in rural areas. However, the level of care provided in rural areas is still below the urban standard, and doctors often will require full payment in advance for more complicated treatments.<sup>471</sup>

Holders of rural and urban *hukou* have joined in protest over the past year against the registration system's unfair policies. One of the most popularly supported issues is education and the inability of rural *hukou* holders to sit for the national university entrance examination in cities despite having lived there for the majority of their lives. Students must take the exam wherever their *hukou* is registered. For children of migrant workers, this means traveling to their parent's hometown and taking tests based on the local curriculum, which may differ from what they have prepared for in the cities.<sup>472</sup>

In May 2011, Beijing authorities revised public middle school admissions policies to give more access to non-Beijing *hukou* holders.

Previously, options for migrant students were scarce and included paying upwards of 30,000 RMB for “sponsorship fees” that would allow non-Beijing *hukou* holders access to Beijing public middle schools.<sup>473</sup> Of 102,000 children who graduated primary school in Beijing this year, 33.4 percent did not possess a Beijing *hukou*.<sup>474</sup> The new policy is expected to equalize entrance requirements for more than 30,000 students without a Beijing *hukou*.

Protests are rarely focused on the *hukou* system alone but rather on specific effects of the system. Farmers, whose residency licenses require them to live in rural areas, can be evicted nevertheless by Chinese officials through land seizures for infrastructure projects or land development. Without their means of livelihood, they are forced to move. Indeed, local governments rely on land sales for as much as 60 percent of their revenues in some cases, according to City University of Hong Kong political scientist Joseph Cheng.<sup>475</sup> This type of activity frequently results in protests.<sup>476</sup> In March, 2,000 Chinese villagers in Suijiang in Yunnan Province launched a five-day protest against unfair prices offered for land in a forced relocation for a hydroelectric dam. Most farmers in the region were offered the equivalent of only \$1,740 per acre, but many without the proper *hukou* were disqualified from any payment. Chinese paramilitary police broke up the demonstration, claiming that a dozen police, but no civilians, had been injured.<sup>477</sup>

One of the most notable calls to action against the *hukou* system occurred in March 2010 when 13 Chinese newspapers initiated a coordinated petition for *hukou* reform. Part of their jointly published editorial read:

*‘China has suffered from the hukou [household registration] system for so long,’ the appeal said. ‘We believe people are born free and should have the right to migrate freely, but citizens are still troubled by bad policies born in the era of the planned economy and [now] unsuitable.’<sup>478</sup>*

Chinese officials are exploring ways to amend the structure without completely abolishing *hukou*. China has launched several programs in rural areas and second-tier cities to improve access to social services, such as basic healthcare. However, Chinese officials still fear they would be faced with a massive influx of migrants into the cities. Local governments argue that the increased demand for public services, such as housing and healthcare, would overwhelm them if the influx were too rapid. In addition, urban residents in major Chinese cities have already protested modest attempts at increasing the rights of migrant workers out of fear that the current residents would face a loss of jobs and increased competition.<sup>479</sup> In both cases, the party and the government consider the potential instability too great a risk. Dr. Huang estimated that China’s rate of urbanization would grow rapidly from the current 40 percent to nearly 70 percent.

### **The “Ant Tribe”**

Chinese attempts to help citizens in rural and second-tier urban settings have also raised expectations and created disappointment. Graduates from second-tier universities in rural areas are unlikely to find employment in urban areas, because they often lack connections. *Hukou* plays a role in exacerbating the situation, since these students are ineligible for subsidized housing and healthcare due to their migratory status. This situation has created a large surplus of underemployed young people living in substandard housing, dubbed “the ant tribe.”<sup>480</sup> This ant tribe consists of over 6 million college graduates who annually flock to major Chinese cities such as Beijing and Shanghai looking for work.<sup>481</sup> Instead of finding jobs in their fields of study, they are forced to take sweatshop jobs or perform other low-skilled work.<sup>482</sup>

In the aftermath of the recent Middle East and North African revolutions, which featured a prominent role for disaffected youth, many academics pondered whether China could undergo a similar experience given its large population of unemployed recent graduates. Many academics agreed that while China shared some similarities to the attacked regimes, it was missing a few critical elements. Compared to Egypt and Tunisia, where youth unemployment is around seven to nine times higher than the national average, China’s unemployed youth, at 2.5 times the average, “is a serious but not explosive social problem,” according to Ho Kwon Ping, chairman of the Singapore Management University. However, quoting Lenin, that “awakened desperation, not idealism makes revolutionaries,” Mr. Ho further notes that:<sup>483</sup>

*Because of hukou ... these jobless graduates are living on the edge of society, almost as disenfranchised as Arab youth. This educated underclass will potentially be more angry and assertive than the floating mass of roughly 100 million to 150 million unskilled migrant workers, simply because their expectations are much higher. Connected by the Internet, they are a potent and potentially organizable force, watching and learning from events in the Arab world with growing interest.*

### **The Middle Class**

During the Commission’s February 25 hearing, witnesses discussed whether the middle class is a force for political change or for stasis. For the present, the growing middle class is considered unlikely to risk its future economic well-being by defying the Communist Party. The party has successfully taken credit for 30 years of economic growth—the very source and foundation of China’s middle class. The party, in turn, comprehends that its control rests, in part, on a middle class that places a high premium on economic stability.

Part of the divergence between these two views of the middle-class role in China’s transformation is due to the nature and size of China’s middle class. Cheng Li, a scholar at The Brookings Institution, notes that there are multiple paths to achieving middle-

class status, making the group heterogeneous and difficult to study. These paths include success in business, party membership, and through an urban social network.<sup>484</sup> This makes blanket conclusions about what the Chinese middle class will do difficult to formulate.<sup>485</sup>

In a book edited by Dr. Li, *China's Emerging Middle Class*, no agreement emerged on a single definition of the term.<sup>486</sup> Some have attempted to define the term based on surveys examining an index of key factors, including education, income, occupation, consumption, and self-identification. One article notes the broad range of estimates that have appeared as a result of varying criteria, stating that “[e]stimates of just how big China’s middle class is range from a low of 157 million (which would be second only to the United States) to more than 800 million.”<sup>487</sup>

Reflecting the importance of the role the middle class is expected to play in China’s future, the government has attempted to study and characterize the group. The Chinese Academy of Social Sciences estimated China’s middle class accounted for 19 percent of the nation’s 2003 population of 1.3 billion, or 247 million. The academy defined the group as having assets between \$18,137 and \$36,275. (This level of wealth would exclude the vast majority of China’s workers. That same year, the per-capita income of China’s 786 million farmers registered only \$317.)<sup>488</sup>

By 2009, China’s urban middle class had reached 230 million, or 37 percent of those living in cities, the academy reported. Based on historical patterns, China’s middle class would make up 40 percent of the population in 2020, the academy predicted. By 2010, 40 percent of Beijing citizens, or 5.4 million, were in the middle class, with an average monthly income of \$885, according to the Academy of Social Sciences.<sup>489</sup>

Precise numbers are debatable and comparisons among the surveys are difficult because some estimates use wealth and others calculate according to annual income. There is more consensus on the existence of two groups: a new and an old middle class. The old middle class is composed of the “self-employed, small merchants and manufacturers” who emerged from the economic reforms of the 1980s, while the new middle class consists of “salaried professionals and technical and administrative employees who work in large corporations” as well as small- and medium-sized enterprise owners.<sup>490</sup> It is, therefore, difficult to categorize the different middle classes as either a force for stability or for change. As Yang Jing, a sociologist at the East Asian Institute notes:

*China’s middle class composes of [sic] not only the majority of white-collar workers and well-educated professionals, but also those at the top of the social hierarchy in terms of wealth. Except for the new middle class who exhibit the most democratic mentality compared with the other two groups, China’s middle class as a whole has yet to hold a distinctive sociopolitical ethos. . . . Their acknowledgement of state authority is similar to that accorded by the rest of the society. As long as the majority of the middle class are able to maintain their current lifestyle despite the social policy reform, the force of democratization is unlikely to become strong.*<sup>491</sup>



Other experts, too, are skeptical that China's middle class will contribute to large-scale unrest or initiate a drive for democracy. George Washington University Professor Bruce Dickson wrote that the party has effectively linked the continued success of China's middle class to the current economic model. Instability or movement away from the current system would endanger that success.<sup>492</sup> Instead, some experts believe that China's urban middle class and elite will remain focused on local issues, especially in preventing construction of polluting or unsafe industry in their areas. Dr. Dickson suggested that China's middle class will be more focused on smaller, "not-in-my backyard" issues rather than with larger social change.

Another Commission witness, sociologist Martin Whyte, agreed.<sup>493</sup> Dr. Whyte's studies have focused on public perceptions of inequalities in China and have found that Chinese citizens are optimistic about their futures, which downplays the chance of significant social unrest. This is a surprising result, he argues, because China has become more unequal as it has developed. Dr. Whyte has written that "forms of wealth and privilege that the revolution set out to destroy have returned with a vengeance—millionaire business tycoons, foreign capitalists exploiting Chinese workers, gated and guarded private mansion compounds, etc."<sup>494</sup>

However, Chinese citizens are willing to accept this growing inequality, because they believe they have a chance to succeed. Dr. Whyte conducted a four-year study, including a questionnaire submitted to Chinese citizens, and found that the Communist Party had effectively convinced most of China's upwardly mobile population that its continued prosperity is inextricably linked to continued stability, while effectively shifting blame for corruption to local-level officials. He argued that China has successfully incorporated China's middle class into the group of winners in the current economic model. They are unlikely to push for systemic change, because their economic well-being remains linked to the control of the party.

Another aspect of China's middle class that pegs it as a force of stability is its size. Even when calculating the magnitude of the middle class at the highest end of the spectrum, the middle class remains a minority. Therefore, in theory, the middle class would be disinclined to bring about a democratic system that would put the majority of voting and political power in the hands of the lower class and the poor. "Those who have prospered from economic reform have no interest in sharing power or the spoils of prosperity with those beneath them," said Li Fan, director of the World and China Institute, a nongovernmental group in Beijing that studies political reform.<sup>495</sup>

Additionally, with the harsh punishments doled out to advocates of democracy such as Nobel Peace Prize winner Liu Xiaobo, the costs of supporting democracy are regarded as prohibitively high. The 2011 activities of Chinese security forces served as a powerful reminder to citizens that supporting the current regime and playing within the system was a far better alternative to near-certain arrest for protest. (For more on this topic, see the following subsection.)



There are some experts, however, who believe that China's middle class is a potential force for instability and that its members will likely challenge the CCP in the coming years. Commission witness Elizabeth Economy observed that China's middle class is now more willing to work to prevent the government from threatening their quality of life:

*In the past few years, the urban middle class has demonstrated a newfound willingness to advance its interests through protest. In addition, the Internet has become a virtual political system with individual complaints able to go viral in a matter of minutes, gaining widespread popular support across gender, age, profession, and provincial boundaries.*<sup>496</sup>

Middle-class protests in recent years have covered a variety of issues, including objections over a garbage incinerator being built in close proximity to middle-class homes, destruction of homes without proper compensation in the lead-up to the World Expo, concern over the environmental impacts of the extension of Maglev lines, and pollution concerns over the construction of a chemical plant. The majority of middle-class protests centered on issues that would adversely impact members' health and/or property value.

According to a survey by China's Academy of Social Sciences, the middle class is also the most likely group in China's social stratum to be critical of the present social and political situation and is the least confident of the government's performance.<sup>497</sup> However, the middle classes' higher levels of criticism and uncertainty about the party's abilities do not necessarily mean that they are the group with the most potential to destabilize the government. Protests among the middle class remain small in frequency and size, and government officials have acted quickly in redressing issues that have attracted significant middle-class anger. As a result, it seems likely that should the CCP continue to sustain healthy economic growth for the country and citizens remain optimistic about the future and see potential for upward mobility, the middle class will continue to be a force for stability for the current regime.

### **China's "Aging" Problem**

Although not as immediate a problem as inflation or mass unrest, China's aging population and stagnant population growth could act as a brake on the economy and an impediment to the growth of a middle class. The Chinese labor force, so crucial to the manufacturing sector, is due to start shrinking in 2016.<sup>498</sup> In addition, as the average age of the population increases, there will be fewer workers supporting more retirees.

Much of the demographic change is due to China's one-child policy, which was instituted in 1980. The policy prevented 400 million births, which would have pegged China's population at 1.73 billion by now, according to the National Population and Family Planning Commission, which administers the program.<sup>499</sup> The population over age 60 is now 13.3 percent of the total, up from 10.3 percent in 2000. Those under age 14 now make up 16.6 percent of the population, down from 23 percent in 2001. One solution is to raise the retirement age, but that would not be popular with those grad-

uating from college and hoping to find a job that might still be occupied.

One problem for China's rulers is the potential for wage inflation as the labor pool declines relative to the demand. However, that problem would be offset by a higher per-capita income.<sup>500</sup>

### **The Party's Response to Growing Unrest**

While the number of protests in China continues to rise, the Communist Party seeks to respond quickly and efficiently either to head off trouble or to quell disturbances before they escalate and serve as a rallying point for further protest. Internal security is one of the top priorities of the Communist Party, which has created a vast apparatus of government control. Monitoring and restraining the population from direct confrontations with the party and the central government are the top priorities. An indication of this is China's 12th Five-Year Plan (2011–2015), which includes a broad range of programs imposing strict controls over the population.<sup>501</sup> The outline, released in March 2011 to the National People's Congress, laid out the party's rapid response system for "emergency incidents." The plan "must be under a comprehensive, unified command, rationally structured, capable of nimble reactions, and it must have guaranteed capability and high-efficiency operations."<sup>502</sup>

The scope of the investment in stability, which includes collaboration among police and paramilitary forces, Internet monitors, and the judiciary, has surpassed China's published military budget.\* China's Finance Ministry budget report showed that in 2010, China's spending on law and order, including police, state security, armed militias, and courts and jails was \$83.5 billion. China's officially reported military expenditure was \$81.2 billion in 2010. The security budget was due to grow faster than military expenditures, by 13.8 percent versus 12.7 percent for the military budget.<sup>503</sup> One example of China's spending on internal security is the effort underway in Chongqing to create the largest police surveillance system in the world, with 500,000 cameras intended to cover a half-million intersections, neighborhoods, and parks over 400 square miles in an area more than 25 percent larger than New York City.<sup>504</sup>

Despite rapid economic growth and increased prosperity, China continues to face growing numbers of public protests, officially referred to as "mass incidents."<sup>505</sup> While official Chinese numbers have not been released since 2005, Dr. Tanner has studied protest statistics, including local Chinese police statistics, and has detected a spike in incidents following the financial crisis in 2008:<sup>506</sup>

*Protest numbers apparently spiked with the onset of the financial crisis soon after the Summer Games, and by the end of 2008, total mass incidents had reportedly risen to 120,000 despite the pre- and post-Olympic security. Nationwide figures for 2009 and 2010 are not yet available, although local data and reports by some prominent Chinese academics indicate protests climbed greatly in 2009 in the wake of economic difficulties.*<sup>507</sup>

\*China's military budget is generally assumed to be larger than officially published figures.

Traditionally, protests were centered in rural areas in response to repressive government actions, especially over abuses by corrupt local officials. While rural protests continue today at record numbers, protests now occur more frequently in urban areas, drawing greater attention. One tactic of suppressing rural riots—blocking foreign media access to remote areas—is not possible within cities. The party has seen a growing number of middle-class and urban residents beginning to protest government actions prior to their enactment. These urban protests were notably different from rural incidents, because they involved middle-class Chinese citizens protesting policies before they were imposed, substituting a demonstration for a petition.<sup>508</sup>

The common theme among all of these issues is China's inability to respond to the underlying factors creating them. This is why protest numbers have continued to increase while China's economy has grown.<sup>509</sup> According to Dr. Economy:

*The roots of protest in China rest in the systemic weakness of the country's governance structure. A lack of transparency, official accountability, and the rule of law make it difficult for public grievances to be effectively addressed and encourage issues such as inflation, forced relocation, environmental pollution, and corruption to transform from otherwise manageable disputes to large-scale protests.*

Dr. Tanner agreed, noting that “[p]arty leaders have repeatedly had to reissue orders calling for an end to these abuses, even while these abuses remain leading causes of unrest.”<sup>510</sup>

### **Censorship and Thought Control**

The CCP and the central government also seek to control the Internet. However, protesters and activists continue to play a cat-and-mouse game with Chinese censors. Chinese microblogs, similar to Twitter, are widely used in China, with over a million posts every hour.<sup>511</sup> China's top two microblogs have over 200 million subscribers.<sup>512</sup> Besides their immense popularity, microblogs are particularly useful for organizing events in China under the nose of Chinese censors, for two reasons. First, 140 characters can convey far more information in Mandarin than in English. Second, the number of homonyms in Mandarin allows users to mask the true meaning of posts from censors.<sup>513</sup> For example, the Mandarin word for harmony sounds like the word for river crab. When Chinese bloggers want to mock the government's “harmonious society” propaganda themes, they reference a river crab with watches lining its arms as a symbol of greedy officials. A “watered weasel ape” sounds like the word for “administrator” and is used to refer to the much-maligned Internet censors. A mythical creature, the grass mud horse, sounds like “... your mother,” where the reference to mother is taken to mean the Communist Party.

China's government has fought the technology. In 2010, the government blocked more than one million websites, including Facebook, Twitter, YouTube, and Evite.<sup>514</sup> Domestic microblogs were required to self-censor postings. In 2011, foreign microblog providers, including Twitter, remained unable to gain market ac-

cess. Most market analysts believed the prohibition on foreign microblogs was driven by concerns among government regulators over the ability to censor those sites.<sup>515</sup>

China began requiring that bars, restaurants, hotels, and bookstores offering access to the Internet install Web-monitoring software to provide the identities to the public security agencies of those logging on. Establishments that resist face a \$2,300 fine and revocation of their business license. Cybercafés offering computers must demand from the customers a state-issued identification before logging on.<sup>516</sup>

China's central government responded forcefully to the possibility that the unrest in the Middle East might spread to China. In January, as protests began in Egypt, Chinese Internet users could not complete keyword searches for terms such as "Egypt" or "Cairo." Official reporting on the protests, such as coverage on the Xinhua website, glossed over the causes of the protests or framed them in a negative light.<sup>517</sup> In a March front-page editorial, *Beijing Daily* had this to say of protests in the Middle East: "Such movements have brought nothing but chaos and misery to their countries' citizens and are engineered by a small number of people using the Internet to organize illegal meetings."<sup>518</sup>

By February, China began to detain human rights and democracy activists<sup>519</sup> and to reimpose restrictions on foreign journalists and to disrupt access to certain websites, including Google's e-mail product, Gmail.<sup>520</sup> Text messages with the words "jasmine" and "revolution" were bounced back. This response was triggered by anonymous Internet postings calling for a Jasmine Revolution in China, the same name given to the December 2010–January 2011 Tunisian revolution in which President Zine El Abidine Ben Ali was ousted after mass civil protests were launched.<sup>521</sup> U.S. ambassador to China Jon Huntsman's name was also blocked from Chinese microblogs in February after he was photographed near an anticipated Jasmine Revolution gathering in Beijing.<sup>522</sup>

On April 3, 2011, Chinese officials detained noted activist Ai Weiwei. Mr. Ai is one of China's most famous artists and an architect who helped design Beijing's "Bird's Nest" building used in Beijing's 2008 Summer Games opening ceremonies. Mr. Ai's wife and employees were also questioned or arrested. Authorities later reported that Mr. Ai was being charged with "economic crimes" including tax evasion. After his release on bail in late June 2011, Mr. Ai eventually returned to posting on the Internet even though he had been ordered not to "be interviewed by journalists, meet with foreigners, use the Internet and interact with human rights advocates for a year from his release."<sup>523</sup> Mr. Ai may have violated the terms of his release when he began posting again on his Twitter account. Mr. Ai revealed that he had undergone "intense psychological pressure" and been interrogated more than 50 times.<sup>524</sup> He also began talking about other prisoners of conscience and abuses by authorities.

Another high-profile case of censorship this year concerned Liu Xiaobo, a human rights activist who was sentenced to 11 years in prison for inciting subversion as one of 303 Chinese activists who called for an expansion of freedoms for Chinese citizens and an end to one-party rule in China in the *Charter 08* manifesto.<sup>525</sup> In Octo-

ber 2010, the Nobel Committee announced that Liu Xiaobo had won the Nobel Peace Prize. In response, China's cybersecurity team blocked all searches of his name and prevented access to foreign news websites such as CNN and the BBC.<sup>526</sup> Mr. Liu's wife was also placed under house arrest, and any gatherings to celebrate the award were quickly dispersed and some attendees jailed.<sup>527, 528</sup> On the day of the actual awards ceremony, CNN and BBC television channels and websites were blocked in mainland China, and text messages containing the words "Liu Xiabo" or "Nobel prize" were blocked as well.<sup>529</sup>

In addition to foreign media being censored online, foreign reporters in China have noticed increased monitoring by authorities and restrictions on their movement. The *New York Times* reported in March that one of its staff had two telephone calls dropped when the call quoted Queen Gertrude from William Shakespeare's *Hamlet*. The line "the lady doth protest too much, methinks" in either English or Mandarin caused both calls to be disconnected due to the use of the word "protest."<sup>530</sup> The Chinese government has also instituted new rules requiring foreign journalists to have government permission when interviewing anyone in a public area.<sup>531</sup>

China has rescinded many of the freedoms that were granted to foreign reporters in the run-up to the Beijing Olympic Games. Reporters are no longer allowed to cover protests or the state response. These restrictions, as well as the arrests of well-known Chinese activists and lawyers, prompted an official complaint from the U.S. embassy in early March, according to a State Department briefing:

*[T]he United States is increasingly concerned by the apparent extralegal detention and enforced disappearance of some of China's most well-known lawyers and activists, many of whom have been missing since mid-February. We note that Teng Biao, Tang Jitian, Jiang Tianyong, and Gu Chuan all disappeared between February 16 and February 19. We have expressed our concern to the Chinese Government over the use of extralegal punishments against these and other human rights activists. We continue to urge China to uphold its internationally recognized obligations of universal human rights, including the freedoms of expression, association, and assembly.*<sup>532</sup>

In response to these protests, a Foreign Ministry spokeswoman said that China would "urge the [UN] mechanism to respect China's judicial sovereignty."<sup>533</sup>

### **Implications for the United States**

China's neighbors, and trading partners, particularly the United States, have an interest in China's peaceful rise and its transition to a modern economic and political system. An evolution of the Chinese government and economy to a multiparty democracy and a free market system would benefit China's citizens as well. Chinese political dissidents, advocates of human and labor rights, and its entrepreneurs all have an incentive and an important role in fostering such a change.



The party and the government in Beijing are determined to pursue at all costs the preservation of single-party rule and the existence of a large, state-owned and -controlled economic sector. In recent years, this has led to violent confrontations and counterstrikes against citizens airing legitimate grievances. These protests are most often aimed at specific instances of local corruption or abuses of power, yet the central government is fearful that such protests could become a political movement.

Internal dilemmas such as the *hukou* system, by definition, are more likely to have an impact on Chinese citizens than the United States. However, issues including governance practices, consumer product safety regulations, and media restrictions may have transnational implications. For example, corruption, abuse of power and suppression of the media may compromise U.S. commercial opportunities just as weak safety supervision may result in tainted food or hazardous products entering the U.S. markets. In addition, tolerance of corruption disadvantages American companies complying with the Foreign Corrupt Practices Act.

The Chinese government continues to manipulate the value of its currency, keeping the RMB at an artificially low value in order to reduce the price of its exports and to increase the price of imports. This policy creates inflation within China's economy and reduces the ability of China's central bank to conduct monetary policy. This policy also reduces U.S. exports to China while it encourages U.S. consumers to purchase Chinese exports. The result has been lost production and jobs in the United States.

### Conclusions

- The primary objective of the CCP is to remain in power. All other goals are intended to serve that end. As a consequence, the party has dedicated enormous resources to repress dissent before it becomes a destabilizing element and threatens the party's control.
- Despite the efforts of the party and the government to minimize dissent, citizen protest has been on the rise. Protests are sometimes brutally suppressed. The government will arrest and detain as a precautionary measure those it considers a threat to its control. The party and the government employ the news media to propagandize and mislead the public.
- The party is well aware of the dangers to its continuing authority posed by public rejection of a government that is unresponsive to the people. The party therefore reacts to citizen ire by attempting appeasement. This may take the form of authorizing the news media to highlight official abuses, particularly those committed by local officials. Still, corruption in all levels of government remains a problem for Beijing.
- Inflation has historically caused problems for the government in China. The rural poor and migrant workers are particularly disadvantaged by higher prices because they are so often reflected disproportionately in food and energy, which consume a larger portion of family expenses in rural areas. The government has responded to rising inflation with price controls and some curbs on bank lending. These tools are inadequate in the long run. Chi-



na's policy of keeping the RMB undervalued in order to gain an export advantage removes a powerful anti-inflation tool from the central bank.

- Income and wealth inequality is a growing problem in China. One cause is the *hukou* system of residential registration, which was intended to limit the migration of the rural poor to the cities. This has created a large migrant population in China, moving from city to city to seek work in factories but unable to access healthcare and education services without the proper *hukou* designation for that area. This situation perpetuates poverty among the disadvantaged. Local officials favor it, because it limits their responsibility toward the migrant workers. A smaller group, known as the "ant tribe," consists of college graduates from second-tier schools in rural areas who also lack the *hukou* to live in urban areas but who nevertheless seek but are unable to find the jobs that they have trained for. This restive and disappointed population is a potential source of unrest.
- China's middle class has been considered by some to be a potential force for political reform. But the opposite is likely. As long as the party can deliver strong economic growth, particularly in urban areas, the middle class is likely to remain a force for stability.
- China's central government has reacted strongly to perceived challenges to its authority. It detains and imprisons dissidents. It censors the news and punishes journalists for infractions of its unwritten and arbitrary rules. China also attempts to control and censor the Internet and has had more success than most other authoritarian regimes in suppressing the flow of information among the public.

## RECOMMENDATIONS

### ***Chinese State-owned Enterprises and U.S.-China Bilateral Investment***

The Commission recommends that:

- Congress urge the administration to employ all necessary remedies authorized by WTO rules to counter the anticompetitive and trade-distorting effects of the Chinese government's extensive subsidies for Chinese companies operating in China and abroad.
- Congress assess the extent to which existing laws provide for effective remedies against the anticompetitive actions of Chinese state-owned or state-invested enterprises operating in the U.S. market. Appropriate remedies, if they are not readily available, should also be considered.
- Congress urge the administration to include in any bilateral investment treaty with China the principles of nondiscrimination and competitive neutrality between SOEs and other state-invested or -supported entities and private enterprises.
- Congress assess China's new national security review process for foreign investment to determine whether it is being used as a trade barrier.
- Congress direct the U.S. Department of Commerce to report annually on Chinese investment in the United States including, among other things, data on investment in the United States by Chinese SOEs and other state-affiliated entities.
- Congress direct the U.S. Securities and Exchange Commission to revise its protocols for reviewing filings by foreign entities listed on or seeking to be listed on the U.S. stock exchanges. The Securities and Exchange Commission should develop country-specific data to address unique country risks to assure that U.S. investors have sufficient information to make investment decisions. The commission should focus, in particular, on state-owned and -affiliated companies, and subsidies and pricing mechanisms that may have material bearing on the investment.
- Congress urge the administration to review federally subsidized contracts provided under the American Recovery and Reinvestment Act of 2009 and report on the extent to which Chinese-produced goods and services were procured using such funds.
- Congress urge the administration to direct the USTR to move aggressively to bring more WTO cases against China for violating its obligations under the WTO Subsidies Agreement.

- Congress urge the administration to direct the USTR to strengthen its mandated annual review of China's compliance with its WTO obligations by adding conclusions and recommendations to its annual report to Congress.

### ***Indigenous Innovation and Intellectual Property Rights***

The Commission recommends that:

- Congress request the administration to report on whether procurement catalogues are actionable under WTO obligations.
- Congress instruct the administration to insist that all procurement catalogues at all levels of government be explicitly recalled in order to comply with assurances by President Hu Jintao to separate government procurement from the catalogues.
- Congress urge the administration to raise with China in the Strategic and Economic Dialogue and the Joint Commission on Commerce and Trade and in other appropriate bilateral and multilateral venues the need for China to table a serious offer to join the Government Procurement Agreement that provides reciprocal opportunities for access to the estimated \$1 trillion in procurement controlled by central, provincial, and local governments as well as state-affiliated entities. If China fails to engage in serious negotiations, the U.S. government should restrict access to Chinese suppliers to government procurement opportunities and should coordinate policies with the states to limit procurement contracts with China.
- Congress instruct the administration to make a top priority within the Joint Commission on Commerce and Trade and the Strategic and Economic Dialogue negotiations an agreement to lower the threshold for criminal prosecution of cases of piracy and counterfeiting of business and entertainment software.
- Congress recommend the administration adopt a more reciprocal trading relationship in critical areas, such as intellectual property protection. The United States should demand the same level of treatment from its major trading partners that it provides to those other nations. The administration should identify those sectors that China has failed to open up to trade in goods and services and identify the practices that act to nullify and impair anticipated economic benefits for U.S. producers and service providers. The administration should seek the elimination of such practices in a timely manner and, if unable to gain sufficient market access, should evaluate what reciprocal actions may be appropriate.
- Congress urge the administration to insist that China audit the use of licensed software on government computers rather than just audit the budget for software procurement. The audit should be performed by the World Bank.
- Congress assess the reauthorization of Super 301 to assist in the identification of the policies and practices that China pursues that create the greatest impediment to U.S. exports entering the Chinese market and the most important policies or practices that

unfairly or unjustifiably harm U.S. producers and workers in the U.S. market. Priority should be given to addressing such practices by the United States Trade Representative under such legislation.

- The President should direct USTR to move aggressively to bring cases to the WTO to enforce intellectual property rights.

***China's 12th Five-Year Plan and Technology Development and Transfers to China***

The Commission recommends that:

- Congress hold hearings to assess the success of the Strategic and Economic Dialogue and the Joint Committee on Commerce and Trade in addressing Chinese actions to implement its WTO commitments, including with regard to the issue of technology transfers. In preparation for such hearings, Congress should request that the Government Accountability Office prepare an inventory of specific measures agreed to as part of these bilateral discussions and the implementation efforts of the Chinese.
- Congress direct the Government Accountability Office to undertake an evaluation of investments and operations of U.S. firms in the Chinese market and identify what federally supported R&D is being utilized in such facilities and the extent to which, and on what terms, such R&D has been shared with Chinese actors in the last ten years.

***China's Internal Dilemmas***

The Commission recommends that:

- The administration work with the Chinese leaders in the Strategic and Economic Dialogue and the Joint Commission on Commerce and Trade talks to identify specific commodities and products in the case where supply does not adequately meet demand in China and where enhanced access for U.S. goods might help alleviate inflationary pressures. Specific attention should be given to agricultural commodities and Chinese barriers that may limit access to the Chinese market for American goods and products.
- Congress direct the Government Accountability Office to conduct a review of efforts by the Chinese government to censor content on the Internet and identify the extent to which any foreign technology providers may be assisting the government in its efforts.

## ENDNOTES FOR CHAPTER 1

1. World Bank, "Southwest Poverty Reduction Project" (Washington, DC: October 2011) <http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/EASTASIA/PACIFICEXT/CHINAEXTN/0,,contentMDK:20680094~pagePK:141137~piPK:141127~theSitePK:318950,00.html>.
2. Carl F. Minzner, "China's Turn against the Law," *American Journal of Comparative Law* (forthcoming 2011). [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1767455](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1767455).
3. There was a substantial jump in U.S. exports to China in 2009. Top export categories that year included electrical machinery (\$22.4 billion); agricultural products (\$17.5 billion); machinery (\$11.2 billion); miscellaneous grains (\$11 billion); and aircraft (\$ 5.8 billion). Office of the United States Trade Representative, "China" (Washington, DC: Office of China Affairs, 2010). <http://www.ustr.gov/countries-regions/china>.
4. U.S. Census Bureau, "Balance by Partner Country—China," (Washington, DC: U.S. Department of Commerce, 2011). <http://www.census.gov/foreign-trade/balance/c5700.html#2011>; Ministry of Commerce of the People's Republic of China, "Brief Statistics on China's Import & Export in August 2011" (Beijing, China: 2011). <http://english.mofcom.gov.cn/article/statistic/BriefStatistics/201110/20111007785417.html>.
5. Peter Robertson, "In China's Wake: Has Asia Gained From China's Growth?" (Perth, Australia: The University of Western Australia, Discussion Paper 10.15, June 2010); David Greenaway, "Has China Displaced Other Asian Countries' Exports?" (Nottingham, United Kingdom: University of Nottingham Leverhulme Centre for Research in Globalisation and Economic Policy, July 2006).
6. U.S. Census Bureau, "Advanced Technology Product Data—Imports and Exports—Country by ATP [advanced technology product] Group" (Washington, DC: U.S. Department of Commerce, 2011). <http://www.census.gov/foreign-trade/statistics/product/atp/select-ctryatp.html#2011>.
7. U.S. Bureau of the Census, *U.S. Trade in Goods and Services* (Washington, DC: U.S. Department of Commerce, August 15, 2011).
8. Office of the United States Trade Representative, "2010 National Trade Estimate Report on Foreign Trade Barriers" (Washington, DC: 2009). [http://www.ustr.gov/webfm\\_send/2694](http://www.ustr.gov/webfm_send/2694).
9. The American Chamber of Commerce in the People's Republic of China, "China Business Climate Survey" (Beijing, China: 2011), p. 16.
10. European Chamber of Commerce in China, "Public Procurement in China: European Business Experiences Competing for Public Contracts in China" (Shanghai, China: September, 2010) [http://www.europeanchamber.com.cn/images/documents/marketing\\_department/beijing/publications/2011/PP%20Study%20EN%20Final.pdf](http://www.europeanchamber.com.cn/images/documents/marketing_department/beijing/publications/2011/PP%20Study%20EN%20Final.pdf).
11. US-China Business Council, "Provincial and Local Indigenous Innovation Product Catalogues" (Washington, DC: July 2011). [https://www.uschina.org/public/documents/2011/07/local\\_ii\\_catalogues.pdf](https://www.uschina.org/public/documents/2011/07/local_ii_catalogues.pdf).
12. Alicia Herrero, "China's 5-year financial sector and the new 5-year plans," *Asian Banking and Finance* (June 1, 2011). <http://asianbankingandfinance.net/blogs-opinion/commentary/chinas-5-year-financial-sector-and-new-5-year-plans>.
13. DBS Group Research, "China: CNY capital account liberalization—recent developments & implications" (Singapore, China: February 8, 2011). [https://www.dbsresearch.com/research/DBS/research.nsf/\(vwAllDocs\)/FA53A532665277C34825783100094D61/\\$FILE/cn\\_110208.pdf](https://www.dbsresearch.com/research/DBS/research.nsf/(vwAllDocs)/FA53A532665277C34825783100094D61/$FILE/cn_110208.pdf).
14. Jack Barnes, "China's Money Printing Addiction Could Spell Disaster," *Business Insider*, January 11, 2011. <http://www.businessinsider.com/china-worlds-fastest-printing-press-2011-1>.
15. Jeffrey Frankel, "On the Renminbi," *CESifo Forum* 6:3 (Autumn 2005):16–21. <http://www.hks.harvard.edu/fs/jfrankel/ChinaYuanpub05CES-Ifo.pdf>.
16. Ding Lu, "China's capability to control its exchange rate," *China Economic Review* 15:3 (2004):343–347. <http://www.sciencedirect.com/science/article/pii/S1043951X04000355>.
17. Yi Zhang, "Digging Out of the Foreign Exchange Reserves," *China Daily*, August 2, 2011. [http://usa.chinadaily.com.cn/us/2011-08/02/content\\_13032759.htm](http://usa.chinadaily.com.cn/us/2011-08/02/content_13032759.htm); Chinese State Administration of Foreign Exchange, "Monthly Foreign Exchange Reserves, 2010" (Beijing, China: July 2010). [http://www.safe.gov.cn/model\\_safe\\_en/tjsj\\_en/tjsj\\_detail\\_en.jsp?ID=3030300000000000,19&id=4](http://www.safe.gov.cn/model_safe_en/tjsj_en/tjsj_detail_en.jsp?ID=3030300000000000,19&id=4).
18. U.S. Department of the Treasury, "Major Foreign Holders of Treasury Securities" (Washington, DC: September 16, 2011). <http://www.treasury.gov/resource-center/data-chart-center/tic/Documents/mfh.txt>.

19. Keith Richburg, "China, with much to lose, largely silent on debt talks" *Washington Post*, July 23, 2011. [http://www.washingtonpost.com/world/asia-pacific/china-with-much-to-lose-largely-silent-on-debt-talks/2011/07/23/gIQArawHWI\\_\\_print.html](http://www.washingtonpost.com/world/asia-pacific/china-with-much-to-lose-largely-silent-on-debt-talks/2011/07/23/gIQArawHWI__print.html).
20. Reuters, "U.S. debt still safest place for China reserves: top banker," August 16, 2011. <http://ca.reuters.com/article/businessNews/idCATRE77F1GR20110816>.
21. Chris Oliver, "China lending, money supply growth cools," *MarketWatch*, June 13, 2011. <http://www.marketwatch.com/story/china-lending-money-supply-growth-cools-2011-06-13>; Bloomberg, "China New Loans, Money Supply Growth Rebound Even after Cooling Measures," July 12, 2011. <http://www.bloomberg.com/news/2011-07-12/china-new-loans-money-supply-growth-rebound-even-after-cooling-measures.html>.
22. Xinyuan Wang, "Money supply may trigger inflation," *People's Daily Online*, October 19, 2010. <http://english.peopledaily.com.cn/90001/90778/90862/7169746.html>.
23. Cullen Roche, "On the Myth of Exploding U.S. Money Supply," *Seeking Alpha*, March 8, 2011. <http://seekingalpha.com/article/256913-on-the-myth-of-exploding-u-s-money-supply>; U.S. Department of the Treasury, *U.S. Currency and Coin Outstanding and in Circulation* (Washington, DC: March 2011). [http://www.fms.treas.gov/bulletin/b2011\\_2uscc.doc](http://www.fms.treas.gov/bulletin/b2011_2uscc.doc).
24. U.S.-China Economic and Security Review Commission staff, e-mail exchange with Derek Scissors, October 9, 2011.
25. *Business Insider*, "People's Bank of China Raises Reserve Requirement Ratio By 50bp [basis points]," March 12, 2011. <http://www.businessinsider.com/people8217s-bank-of-china-raises-reserve-requirement-ratio-by-50bp-2011-5>.
26. Simon Rabinovitch, "China Moves to Curb Off-Balance Sheet Lending," *Financial Times*, August 29, 2011. <http://www.ft.com/intl/cms/s/0/376b6504-d21c-11e0-9137-00144feab49a.html?ftcamp=rss#axzz1XKmbeigz>.
27. Wen Jiabao, "How China Plans to Reinforce the Global Recovery," *Financial Times*, June 23, 2011. <http://www.ft.com/cms/s/0/e3fe038a-9dc9-11e0-b30c-00144feabdc0.html>.
28. Francis Xiong, "China's Inflation Eases Slightly, Pressure Remains Though," *Xinhua*, October 17, 2011, [http://news.xinhuanet.com/english/2010/china/2011-10/17/c\\_131194974.htm](http://news.xinhuanet.com/english/2010/china/2011-10/17/c_131194974.htm).
29. Shai Oster, "China's Rising Wages Propel U.S. Prices," *Wall Street Journal*, May 9, 2011. <http://online.wsj.com/article/SB10001424052748703849204576302972415758878.html>.
30. Elizabeth Economy, "China's Growing Water Crisis," *World Politics Review*, August 9, 2011. <http://www.worldpoliticsreview.com/articles/9684/chinas-growing-water-crisis>.
31. Sheng Wen, "China hardens rein on home bubble, prices to come down," *People's Daily Online*, August 19, 2011. <http://english.peopledaily.com.cn/90778/7574020.html>.
32. Esther Fung, "Shanghai Slumps Amid Real-Estate Slowdown," *Wall Street Journal*, August 19, 2011. <http://online.wsj.com/article/SB10001424053111903596904576515314278100504.html>.
33. Google Finance, "Claymore/AlphaShares China Real Est [estate] ETF [exchange traded fund]." <http://www.google.com/finance?q=TAO>.
34. Nigel Chalk, "Whack-A-Mole in China's Bubbly Housing Market," *iMFdirect*, August 9, 2011. <http://blog-imfdirect.imf.org/2011/08/09/whack-a-mole-in-china%E2%80%99s-bubbly-housing-market/>.
35. Deepanshu Bagchee, "China Risks Inflation Getting Out of Hand: Expert," *CNBC*, June 9, 2011. <http://www.cnn.com/id/43335366>.
36. Nouriel Roubini, "China's Bad Growth Bet," *Project Syndicate*, April 14, 2011. <http://www.project-syndicate.org/commentary/roubini37/English>.
37. Tom Orlik, "Whack-a-Mole: IMF [International Monetary Fund] Not Impressed With China Bubble Management," *Wall Street Journal*, August 19, 2011. [http://blogs.wsj.com/economics/2011/08/19/whack-a-mole-imf-not-impressed-with-china-bubble-management/?mod=google\\_news\\_blog](http://blogs.wsj.com/economics/2011/08/19/whack-a-mole-imf-not-impressed-with-china-bubble-management/?mod=google_news_blog).
38. Jean Yung, "China Yuan Up Late On PBOC (People's Bank of China) Guidance; Likely Rangebound In Near Term," *Wall Street Journal*, October 17, 2011. <http://online.wsj.com/article/SB10001424053111903918104576503764019812054.html>.
39. U.S. Department of the Treasury, "Report to Congress on International Economic and Exchange Rate Policies" (Washington, DC: February 11, 2011).
40. Xiaoyin Wang, Chunjie Qi, and Yuhong Li, "A Study on the Impact of RMB Fluctuation in Exchange on Chinese Citrus Export," *Advances in Information Sciences and Service Sciences* 3:3 (April 2011). <http://www.aicit.org/aiss/ppl/Binder1-6.pdf>.



41. *Wall Street Journal*, “China Paper: Time Is Ripe To Widen Yuan Trading Band Vs. Dollar,” August 15, 2011. <http://online.wsj.com/article/BT-CO-20110815-716163.html>.
42. Josh Noble, “Did the RMB Just Go Global?” *Financial Times*, August 20, 2011. <http://blogs.ft.com/beyond-brics/2010/08/20/did-the-rmb-just-go-global/#axzz1Vc7H5er5>.
43. James Anderlini, “McPanda bonds still just a McGesture,” *Financial Times*, August 20, 2010. <http://blogs.ft.com/beyond-brics/2010/08/20/mcpanda-bonds-still-just-a-mcgesture/#axzz1Vc7H5er5>.
44. Fiona Law, “Caterpillar Yuan Bond Issue Draws Strong Demand,” *Wall Street Journal*, November 24, 2010. <http://online.wsj.com/article/SB10001424052748703572404575634532182318468.html>.
45. Fiona Law, “Caterpillar Yuan Bond Issue Draws Strong Demand,” *Wall Street Journal*, November 24, 2010. <http://online.wsj.com/article/SB10001424052748703572404575634532182318468.html>.
46. Esteban Duarte, “Morgan Stanley Said to Market Yuan Bonds at 1.625 percent—1.7 percent Yield,” Bloomberg, May 25, 2011. <http://www.bloomberg.com/news/2011-05-26/morgan-stanley-said-to-market-yuan-bonds-at-1-625-1-7-yield.html>.
47. Guanqun Wang, “China issues 20 bln RMB treasury bonds in Hong Kong,” *Xinhua*, August 17, 2011. [http://news.xinhuanet.com/english/2010/china/2011-08/17/c\\_131055155.htm](http://news.xinhuanet.com/english/2010/china/2011-08/17/c_131055155.htm).
48. James Anderlini, “McPanda bonds still just a McGesture,” *Financial Times*, August 20, 2010. <http://blogs.ft.com/beyond-brics/2010/08/20/mcpanda-bonds-still-just-a-mcgesture/#axzz1Vc7H5er5>.
49. Josh Noble, “Renminbi bonds: dim sum for dull palates,” *Financial Times*, March 29, 2011. <http://blogs.ft.com/beyond-brics/2011/03/29/renminbi-bonds-dim-sum-for-dull-palates/>.
50. Daniel Hui, “Guest Post: RMB internationalization—too big to ignore,” *Financial Times*, June 8, 2011. <http://blogs.ft.com/beyond-brics/2011/06/08/rmb-internationalisation-too-big-to-ignore/#axzz1Vc7H5er5>.
51. Securities Industry and Financial Markets Association, “Statistics and data pertaining to financial markets and the economy” (New York, NY). <http://www.sifma.org/research/statistics.aspx>.
52. Tian Li, “RMB Internationalization Well Underway,” *People’s Daily Online*, July 18, 2011. <http://english.peopledaily.com.cn/90001/90780/91344/7443776.html>.
53. Reuters, “The RMB’s Internationalization Continues Apace,” *Asia Money*, July 29, 2011. <http://www.asiamoney.com/Article/2875840/The-RMBs-internationalization-continues-apace.html>.
54. Jialong Tan, “RMB Trade Settlement Puts Upward Pressure on Forex [foreign exchange] Reserves,” *People’s Daily Online*, July 29, 2011. <http://english.peopledaily.com.cn/90778/7454911.html>.
55. Jialong Tan, “RMB Trade Settlement Puts Upward Pressure on Forex [foreign exchange] Reserves,” *People’s Daily Online*, July 29, 2011. <http://english.peopledaily.com.cn/90778/7454911.html>.
56. Fiona Law, “Hong Kong Expects Yuan FDI Framework This Year,” *Wall Street Journal*, August 22, 2011. <http://online.wsj.com/article/SB10001424053111903327904576523631444547752.html>.
57. Jialong Tan, “RMB Trade Settlement Puts Upward Pressure on Forex [foreign exchange] Reserves,” *People’s Daily Online*, July 29, 2011. <http://english.peopledaily.com.cn/90778/7454911.html>.
58. Agence France-Presse, “US seeks WTO action on China, India subsidies,” October 6, 2011.
59. World Trade Organization, *Report of the Working Party on the Accession of China*, para. 104, WTO Doc. WT/MIN(01)/3 (Geneva, Switzerland: November 10, 2001).
60. World Trade Organization, *Accession of the People’s Republic of China*, art. 18.4, WT/L/432, WTO Doc. 01–5996 (Geneva, Switzerland: November 23, 2001); Julia Qin, “WTO-Plus’ Obligations and Their Implications for the World Trade Organization Legal System—An Appraisal of the China Accession Protocol,” *Journal of World Trade* 37:3 (2003): 483–522. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=939329](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=939329).
61. World Trade Organization, “Trade Policy Reviews.” [http://www.wto.org/english/tratop\\_e/tpr\\_e/tpr\\_e.htm](http://www.wto.org/english/tratop_e/tpr_e/tpr_e.htm).
62. William Steinberg, “Monitor With No Teeth: An Analysis of the WTO China Trade Review Mechanism,” *U.C. Davis Business Law Journal* 6 (2005): 2–23.
63. U.S.-China Security and Economic Review Commission, “China’s Compliance with World Trade Organization Obligations: A Review of China’s 1st Two Years of Membership” (Washington, DC: 2004).

64. *Inside U.S.-China Trade*, "WTO quietly approves China's first compliance review without recommendation," December 11, 2002.
65. U.S.-China Security and Economic Review Commission, "China's Compliance with World Trade Organization Obligations: A Review of China's 1st Two Years of Membership" (Washington, DC: 2004).
66. Henry Gao, "Aggressive Legalism: the East Asian Experience and Lessons for China," in *China's Participation in the WTO* (London, United Kingdom: Cameron May Publishers, November 2005), p. 315. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=897140](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=897140).
67. These cases are U.S. Anti-Dumping, E.U. Steel Fasteners, U.S. Tyres, and E.U. Footwear. Henry Gao, "Elephant in the Room: Challenges of Integrating China Into the WTO System," *Asian Journal of WTO & International Health Law and Policy* 6:1 (March 2011):137–168. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1822946](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1822946).
68. Henry Gao, "Elephant in the Room: Challenges of Integrating China Into the WTO System," *Asian Journal of WTO & International Health Law and Policy* 6:1 (March 2011):137–168. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1822946](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1822946).
69. This is done to ascertain an appropriate price for the inputs being considered in such cases by referencing the price of similar inputs in market economies with similar levels of economic development. As a nonmarket economy, China's prices are viewed as not reflecting market forces and, accordingly, proxy rates from third countries are appropriate and legal under WTO codes and jurisprudence. World Trade Organization, "Protocols of Accession of the People's Republic of China," Section 15(a) (Geneva, Switzerland: November 10, 2001).
70. World Trade Organization, "Protocols of Accession of the People's Republic of China," Section 15(b) (Geneva, Switzerland: November 10, 2001).
71. World Trade Organization, "Protocols of Accession of the People's Republic of China," Section 15(d) (Geneva, Switzerland: November 10, 2001). In addition to this, the China-specific Product Safeguard provisions are set to expire in 2013. See Protocols of Accession, Section 16(9).
72. World Trade Organization, *Report of the Working Party on the Accession of China*, Accession Protocol, paras 5.1 and 5.2; WT/MIN(01)/3 (Geneva, Switzerland: November 10, 2001).
73. State Council of China, State Council Order No. 594 (19 March 2011) arts. 41, 43; State Council Order No. 595 (19 March 2011) art. 27.
74. Julia Qin, "Agora: Ten Years of China's Participation in the WTO," *Chinese Journal of International Law* 10 (June 2011): 271.
75. Julia Qin, "Agora: Ten Years of China's Participation in the WTO," *Chinese Journal of International Law* 10 (June 2011): 319.
76. Human Rights in China, *State Secrets: China's Legal Labyrinth* (New York, NY: 2007).
77. Julia Qin, "Agora: Ten Years of China's Participation in the WTO," *Chinese Journal of International Law* 10 (June 2011): 271.
78. Robert Scott, "Unfair China Trade Costs Local Jobs" (Washington, DC: Economic Policy Institute, March 23, 2010). <http://www.epi.org/publication/bp260/>.
79. House Committee on Ways and Means, *Testimony of C. Fred Bergsten*, "Correcting the Chinese Exchange Rate: An Action Plan," 111th Cong., 2nd sess., March 24, 2010; Robert E. Scott, "Unfair China Trade Costs Local Jobs" (Washington, DC: Economic Policy Institute, March 23, 2010).
80. *Economist*, "Climbing the Greenback Mountain," September, 24, 2011.
81. U.S.-China Economic and Security Review Commission, *2004 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, June 2004), p. 62.
82. *China Daily*, "Deputy Raps SOEs' Imparity on Taxes and Jobs," March 10, 2010. [http://www.chinadaily.com.cn/china/2010-03/10/content\\_9567711.htm](http://www.chinadaily.com.cn/china/2010-03/10/content_9567711.htm).
83. Patrick Chovanec, "Guo Jin, Min Tui—The State Advances, The Private Sector Retreats," *Seeking Alpha blog*, August 31, 2010. <http://seekingalpha.com/article/223160-guo-jin-min-tui-the-state-advances-the-private-sector-retreats>.
84. WTO, *Trade Policy Review of China, Report of the Secretariat*, WT/TPR/S/230 (Geneva, Switzerland: April 26, 2010), p. 54. [http://www.wto.org/english/tratop\\_e/tptr\\_e/tp330\\_e.htm](http://www.wto.org/english/tratop_e/tptr_e/tp330_e.htm).
85. World Bank, *China Quarterly Update* (Beijing, China: June 2010), p. 3. [http://siteresources.worldbank.org/CHINAEXTN/Resources/318949-1268688634523/Quarterly\\_June\\_2010.pdf](http://siteresources.worldbank.org/CHINAEXTN/Resources/318949-1268688634523/Quarterly_June_2010.pdf).
86. Michael Wines, "China Fortifies State Business to Fuel Growth," *New York Times*, August 29, 2010.
87. World Bank, *China Quarterly Update* (Beijing, China: June 2010), p. 3. [http://siteresources.worldbank.org/CHINAEXTN/Resources/318949-1268688634523/Quarterly\\_June\\_2010.pdf](http://siteresources.worldbank.org/CHINAEXTN/Resources/318949-1268688634523/Quarterly_June_2010.pdf).

88. Michael Wines, "China Fortifies State Business to Fuel Growth," *New York Times*, August 29, 2010.
89. Barry Naughton, *The Chinese Economy: Transitions and Growth* (Cambridge, MA: MIT Press, 2007), pp. 301–304.
90. Barry Naughton, *The Chinese Economy: Transitions and Growth* (Cambridge, MA: MIT Press, 2007), p. 308.
91. Gao Xu, "State-Owned Enterprises in China: How Big Are They?" East Asia and Pacific on the Rise (*World Bank Blog*). <http://blogs.worldbank.org/eastasiapacific/state-owned-enterprises-in-china-how-big-are-they>.
92. WTO, *Trade Policy Review of China, Report of the Secretariat*, WT/TPR/S/230 (Geneva, Switzerland: April 26, 2010), pp. 54–55. [http://www.wto.org/english/tratop\\_e/tp\\_e/tp330\\_e.htm](http://www.wto.org/english/tratop_e/tp_e/tp330_e.htm).
93. There is a discrepancy in the number of SOEs listed on the State-Owned Assets Supervision and Administration Commission's website in Chinese (121) and in English (125). <http://www.sasac.gov.cn/n1180/n1226/n2425/index.html>.
94. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Derek Scissors, March 30, 2011.
95. Cheng Li, "China's Midterm Jockeying: Gearing Up for 2012 (Part 4: Top Leaders of Major State-Owned Enterprises)," *China Leadership Monitor* 34 (February 2011): 3.
96. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Derek Scissors, March 30, 2011.
97. U.S.-China Economic and Security Review Commission, "An Analysis of State-Owned Enterprises and State Capitalism in China" (Washington, DC: Capital Trade, Incorporated, October 2011), p. 11.
98. Junyeop Lee, "State Owned Enterprises in China: Reviewing the Evidence," *OECD Working Group on Privatization and Corporate Governance of State Assets Occasional Paper* (Paris, France: January 26, 2009), p. 5. <http://www.oecd.org/dataoecd/14/30/42095493.pdf>.
99. Junyeop Lee, "State Owned Enterprises in China: Reviewing the Evidence," *OECD Working Group on Privatization and Corporate Governance of State Assets Occasional Paper* (Paris, France: January 26, 2009), p. 6. <http://www.oecd.org/dataoecd/14/30/42095493.pdf>.
100. World Trade Organization, *Trade Policy Review: China (Revised)*, WT/TPR/S/230 (Geneva, Switzerland: May 31 and June 2, 2010), p. 54 (fn. 84). [http://www.wto.org/english/tratop\\_e/tp\\_e/tp330\\_e.htm](http://www.wto.org/english/tratop_e/tp_e/tp330_e.htm).
101. Junyeop Lee, "State Owned Enterprises in China: Reviewing the Evidence," *OECD Working Group on Privatization and Corporate Governance of State Assets Occasional Paper* (Paris, France: January 26, 2009). <http://www.oecd.org/dataoecd/14/30/42095493.pdf>.
102. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Derek Scissors, March 30, 2011.
103. U.S.-China Economic and Security Review Commission, "An Analysis of State-Owned Enterprises and State Capitalism in China" (Washington, DC: Capital Trade, Incorporated, October 2011), p. 25.
104. Cheng Li, "China's Midterm Jockeying: Gearing Up for 2012 (Part 4: Top Leaders of Major State-Owned Enterprises)," *China Leadership Monitor* 34 (February 2011): 4.
105. For a list of institutions under the administration of CSRC, see China Banking Regulatory Commission, "Domestic Financial Institutions." [http://www.cbrc.gov.cn/english/info/yjhj/index\\_links.jsp?s=dbi](http://www.cbrc.gov.cn/english/info/yjhj/index_links.jsp?s=dbi).
106. For a list of institutions under the administration of CIRC, see China Insurance Regulatory Commission, "A–Z Index of China's Insurance Companies." [http://www.gov.cn/misc/2006-01/05/content\\_148059.htm](http://www.gov.cn/misc/2006-01/05/content_148059.htm).
107. Cheng Li, "China's Midterm Jockeying: Gearing Up for 2012 (Part 4: Top Leaders of Major State-Owned Enterprises)," *China Leadership Monitor* 34 (February 2011): 3.
108. Cheng Li, "China's Midterm Jockeying: Gearing Up for 2012 (Part 4: Top Leaders of Major State-Owned Enterprises)," *China Leadership Monitor* 34 (February 2011): 4.
109. *Fortune*, Fortune Global 500, July 26, 2010. [http://money.cnn.com/magazines/fortune/global500/2010/full\\_list/](http://money.cnn.com/magazines/fortune/global500/2010/full_list/).
110. *Fortune*, Fortune Global 500, July 26, 2010. [http://money.cnn.com/magazines/fortune/global500/2010/full\\_list/](http://money.cnn.com/magazines/fortune/global500/2010/full_list/).
111. *Economist*, "The Long Arm of the State," June 23, 2011.

112. Scott Otteman, "New China Procurement Plan Shows Improvement, but No Sub-Central Coverage," *Inside U.S.-China Trade*, July 14, 2010.

113. Loretta Chao, "The Big Deal with Procurement," *Wall Street Journal China Real Time Report blog*, July 21, 2010. <http://blogs.wsj.com/chinarealtime/2010/07/21/the-big-deal-with-procurement/>; WTO, *Trade Policy Review of China, Report of the Secretariat*, WT/TPR/S/230 (Geneva, Switzerland: April 26, 2010), p. 40. <http://www.wto.org/english/tratop-e/tptr-e/tp330-e.htm>; Demetrios Marantis, "The WTO Government Procurement Agreement: A Tremendous Opportunity for China" (Shenyang, China: Consulate General of the United States, August 11, 2010). <http://shenyang.usembassy-china.org.cn/wto-gpa.html>.

114. European Chamber of Commerce in China, *Public Procurement in China: European Business Experiences Competing for Public Contracts in China* (Beijing, China: April 2011), p. 15. [http://www.europeanchamber.com.cn/images/documents/marketing\\_department/beijing/publications/2011/PP%20Study%20EN%20Final\\_0421.pdf](http://www.europeanchamber.com.cn/images/documents/marketing_department/beijing/publications/2011/PP%20Study%20EN%20Final_0421.pdf).

115. Gilbert Van Kerckhove, "Are Discussions around GPA Missing the Real Issue?" August 28, 2010. <http://blog.strategy4china.com/wp-content/uploads/100828GPAcomments.pdf>.

116. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Derek Scissors, March 30, 2011.

117. *Economist*, "The Long Arm of the State," June 23, 2011.

118. Wang Jing, "Unirule: SOEs Register Negative Real Profits," *Caixin*, March 3, 2011.

119. U.S.-China Economic and Security Review Commission, "An Assessment of China's Subsidies to Strategic and Heavyweight Industries" (Washington, DC: Capital Trade, Incorporated, March 2009).

120. Barry Naughton, *The Chinese Economy: Transitions and Growth* (Cambridge, MA: MIT Press, 2007), p. 308; *Economist*, "Let a Million Flowers Bloom," May 10, 2011; Kellee S. Tsai, *Capitalism Without Democracy: The Private Sector in Contemporary China* (Ithaca, NY: Cornell University Press, 2007), p. 192.

121. Jonathan G.S. Koppell, "Political Control for China's State-Owned Enterprises," *Governance: An International Journal of Policy, Administration, and Institutions* 20:2 (April 2007): 261–273.

122. Kellee S. Tsai, *Capitalism Without Democracy: The Private Sector in Contemporary China* (Ithaca, NY: Cornell University Press, 2007), p. 191.

123. Kellee S. Tsai, *Capitalism Without Democracy: The Private Sector in Contemporary China* (Ithaca, NY: Cornell University Press, 2007), pp. 191–192.

124. Some local governments are claimed to have pressured burgeoning private businesses to merge or cooperate with struggling SOEs in exchange for land or capital. Kellee S. Tsai, *Capitalism Without Democracy: The Private Sector in Contemporary China* (Ithaca, NY: Cornell University Press, 2007), p. 192.

125. Barry Naughton, *The Chinese Economy: Transitions and Growth* (Cambridge, MA: MIT Press, 2007), p. 324.

126. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Derek Scissors, March 30, 2011.

127. U.S.-China Economic and Security Review Commission, "An Analysis of State-Owned Enterprises and State Capitalism in China" (Washington, DC: Capital Trade, Incorporated, October 2011).

128. *Economist*, "Capitalism Confined," September 3, 2011.

129. U.S.-China Economic and Security Review Commission, "An Analysis of State-Owned Enterprises and State Capitalism in China" (Washington, DC: Capital Trade, Incorporated, October 2011), pp. 8, 22.

130. China Europe International Business School, "CEIBS Releases 8th Annual 'China's Top 100 Private Listed Companies'," September 6, 2011. <http://www.ceibs.edu/media/archive/65776.shtml>.

131. U.S.-China Economic and Security Review Commission, "An Analysis of State-Owned Enterprises and State Capitalism in China" (Washington, DC: Capital Trade, Incorporated, October 2011), pp. 22–25.

132. Dinny McMahon, "Who are the Big Players in China's Private Sector?" *Wall Street Journal*, September 8, 2011.

133. Zhao Huanxin, "China names key industries for absolute state control," *China Daily*, December 19, 2006. [http://www.chinadaily.com.cn/china/2006-12/19/content\\_762056.htm](http://www.chinadaily.com.cn/china/2006-12/19/content_762056.htm).

134. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Derek Scissors, March 30, 2011.



135. Michael Sainsbury, "China Rules Out Political Reform," *Australian* (Sydney), March 14, 2011. <http://www.theaustralian.com.au/news/world/china-rules-out-political-reform/story-e6frg6so-1226020720813>.
136. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Derek Scissors, March 30, 2011.
137. Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: HarperCollins 2010), p. 44.
138. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Derek Scissors, March 30, 2011.
139. Michael Wines, "China Fortifies State Businesses to Fuel Growth," *New York Times*, August 29, 2010.
140. Zhiwu Chen, "Economic Consequences of State Capitalism" (The Brookings Institution event on *China's New Breed of State Capitalism*, Washington, DC, March 1, 2011). [http://www.brookings.edu/events/2011/0301\\_china\\_capitalism.aspx](http://www.brookings.edu/events/2011/0301_china_capitalism.aspx).
141. Michael Wines, "China Fortifies State Businesses to Fuel Growth," *New York Times*, August 29, 2010.
142. Cheng Li, "China's Midterm Jockeying: Gearing Up for 2012 (Part 4: Top Leaders of Major State-Owned Enterprises)," *China Leadership Monitor* 34 (February 2011): 24–25.
143. Leslie Hook, "Sinopec Chief Tapped for Political Post," *Financial Times*, March 22, 2011. <http://www.ft.com/cms/s/0/29e13b50-5465-11e0-979a-00144feab49a, dup uuid=9c33700c-4c86-11da-89df-0000779e2340.html#axzz1lw47BEra>.
144. Cheng Li, "China's Midterm Jockeying: Gearing Up for 2012 (Part 4: Top Leaders of Major State-Owned Enterprises)," *China Leadership Monitor* 34 (February 2011): 1.
145. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, written testimony of K.C. Fung, March 30, 2011.
146. Yuqing Xing, "Facts About and Impacts of FDI on China and the World Economy," *China: An International Journal* 8:2 (September 2010): 309.
147. Yuqing Xing, "Facts About and Impacts of FDI on China and the World Economy," *China: An International Journal* 8:2 (September 2010): 310.
148. Yuqing Xing, "Facts About and Impacts of FDI on China and the World Economy," *China: An International Journal* 8:2 (September 2010): 309.
149. Ministry of Commerce (MOFCOM), "Statistics of China's Absorption of FDI from January to December 2010" (Beijing, China: January 27, 2011). <http://www.mofcom.gov.cn/aarticle/tongjiziliao/v/201101/20110107370784.html>.
150. For a detailed discussion on round-tripping, see Nargiza Salidjanova, "Going Out: Overview of China's Outward Foreign Direct Investment" (Washington, DC: USCC Staff Research Report, March 30, 2011). <http://www.uscc.gov/researchpapers/2011/GoingOut.pdf>.
151. Office of the U.S. Trade Representative (USTR), "China" (Washington, DC). <http://www.ustr.gov/countries-regions/china>.
152. Bureau of Economic Analysis, U.S. *Direct Investment Abroad: Financial and Operating Data for U.S. Multinational Companies* (Washington, DC: U.S. Department of Commerce). <http://www.bea.gov/international/di1usdop.htm>.
153. Andrew Halkyard and Ren Linghui, [Excerpts from] "China's Tax Incentive Regimes for Foreign Direct Investment: An Eassonian Analysis," in *Globalization and Its Tax Discontents: Tax Policy and International Investments*, ed. Art Cockfield (Toronto, Ontario: University of Toronto Press, August 2010), pp. 35–59.
154. Luosha Du, Ann Harrison, and Gary Jefferson, "Do Institutions Matter for FDI Spillovers? The Implications of China's 'Special Characteristics'" (Cambridge, MA: National Bureau of Economic Research, Working Paper 16767, February 2011), p. 4. <http://www.nber.org/tmp/47998-w16767.pdf>.
155. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, written testimony of Robert Scott, March 30, 2011.
156. Andrew Halkyard and Ren Linghui, [Excerpts from] "China's Tax Incentive Regimes for Foreign Direct Investment: An Eassonian Analysis," in *Globalization and Its Tax Discontents: Tax Policy and International Investments*, ed. Art Cockfield (Toronto, Ontario: University of Toronto Press, August 2010), pp. 35–59.
157. U.S. Trade Representative, *2010 Report to Congress on China's WTO Compliance* (Washington, DC: December 2010), pp. 42–43.
158. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, written testimony of Robert Scott, March 30, 2011.

159. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of K.C. Fung, March 30, 2011.

160. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of K.C. Fung, March 30, 2011.

161. American Chamber of Commerce in China, “2011 Business Climate Survey”(Beijing, China: March 2011), p. 16.

162. Tom Barkley, “U.S. Warns China is Closing Up Again,” *Wall Street Journal*, May 5, 2011.

163. Tom Barkley, “U.S. Warns China is Closing Up Again,” *Wall Street Journal*, May 5, 2011.

164. For more information, see NDRC [National Development and Reform Commission], “Catalogue for the Guidance of Foreign Investment Industries” (in Chinese), April 2, 2011. [http://www.ndrc.gov.cn/yjq/t20110402\\_4799.htm](http://www.ndrc.gov.cn/yjq/t20110402_4799.htm). Also see Baker & McKenzie, “Draft Revisions to the Catalogue for Guiding Foreign Investment in Industry 2011,” *Client Alert*, April 2011. <http://www.bakermckenzie.com/ALChinaDraftRevisionsForeignInvestmentApr11/>.

165. Baker & McKenzie, “Draft Revisions to the Catalogue for Guiding Foreign Investment in Industry 2011,” *Client Alert*, April 2011. <http://www.bakermckenzie.com/ALChinaDraftRevisionsForeignInvestmentApr11/>.

166. *Inside U.S.-China Trade*, “Draft Catalogue Said to Show Little New Openness to Foreign Investment,” April 27, 2011.

167. *Inside U.S.-China Trade*, “Chamber, AmCham Call on Beijing to Stop Guiding Foreign Investment,” May 3, 2011.

168. The national security review was first mentioned in Article 31 of China’s Anti-Monopoly Law. For more information, see Jones Day, “New Chinese Anti-Monopoly Law,” Jones Day Publications, October 2007. <http://www.jonesday.com/newsknowledge/publicationdetail.aspx?publication=4662>.

169. *Inside U.S.-China Trade*, “Chamber Urges Major Changes in China’s Investment Security Review,” April 13, 2011.

170. *Inside U.S.-China Trade*, “Chamber Urges Major Changes in China’s Investment Security Review,” April 13, 2011.

171. *Covington E-Alert*, “China Issues Final Implementation Provisions for National Security Review Rules,” August 31, 2011. <http://www.cov.com/publications/?pubtype=7&archiveyear=2011>. See also *Covington E-Alert*, “China Issues National Security Review Rules for Foreign Investment,” February 18, 2011.

172. Wayne M. Morrison, “China-U.S. Trade Issues” (Washington, DC: Congressional Research Service, June 2, 2011), p. 19.

173. U.S.-China Economic and Security Review Commission, “Evaluating a Potential U.S.-China Bilateral Investment Treaty” (Washington, DC: Economist Intelligence Unit, March 30, 2010). [http://www.uscc.gov/researchpapers/2010/EIU\\_Report\\_on\\_US-China\\_BIT-FINAL\\_14\\_April\\_2010.pdf](http://www.uscc.gov/researchpapers/2010/EIU_Report_on_US-China_BIT-FINAL_14_April_2010.pdf).

174. Daniel Rosen and Thilo Hanemann’s research found that one third of Chinese FDI in the United States was in services and two thirds in industry and manufacturing. See Daniel H. Rosen and Thilo Hanemann, *An American Open Door? Maximizing the Benefits of Chinese Foreign Direct Investment* (New York, NY: Asia Society Special Report, May 2011), pp. 29–30, 90.

175. Norihiko Shirouzu, “Geely’s Volvo Plans Take Shape,” *Wall Street Journal*, August 27, 2010.

176. Reuters, “BAIC [Beijing Automotive Industry Holding Co.] Paid \$197 mln for Saab Assets—Paper,” December 14, 2009. <http://www.reuters.com/article/2009/12/14/saab-idUSLDE5BD2E920091214>.

177. Joann S. Lublin and Shayndi Raice, “Security Fears Kill Chinese Bid in U.S.,” *Wall Street Journal*, November 5, 2010. <http://online.wsj.com/article/SB10001424052748704353504575596611547810220.html>.

178. Edward M. Graham and David M. Marchick, *U.S. National Security and Foreign Direct Investment* (Washington, DC: Peterson Institute for International Economics, May 2006), p. 100.

179. Ding Qingfen, “Crisis Creating ODI [outward direct investment] Opportunities,” *China Daily*, September 7, 2011.

180. For more information on China’s global outward direct investment position, see Nargiza Salidjanova, “Going Out: Overview of China’s Outward Foreign Direct Investment” (Washington, DC: USCC Staff Research Report, March 30, 2011). <http://www.uscc.gov/researchpapers/2011/GoingOut.pdf>.

181. U.S. Department of the Treasury, “Major Foreign Holders of Treasury Securities” (Washington, DC: September 16, 2011). <http://www.treasury.gov/resource-center/data-chart-center/tic/Documents/mfh.txt>.



182. Thilo Hanemann, “It’s Official: Chinese FDI in the U.S. is Soaring,” *China Investment Monitor* (New York, NY: The Rhodium Group, LLC: August 25, 2011). <http://rhgroup.net/china-investment-monitor/>.

183. Thilo Hanemann, “It’s Official: Chinese FDI in the U.S. is Soaring,” *China Investment Monitor* (New York, NY: The Rhodium Group, LLC: August 25, 2011). <http://rhgroup.net/china-investment-monitor/>.

184. U.S. Department of the Treasury, “Major Foreign Holders of Treasury Securities” (Washington, DC: September 16, 2011). <http://www.treasury.gov/resource-center/data-chart-center/tic/Documents/mfh.txt>.

185. For more information about CIC, its creation and mission, see U.S.-China Economic and Security Review Commission, “China’s Capital Investment Vehicles and Implications for the U.S. Economy and National Security,” *2008 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2008), pp. 43–68.

186. Lingling Wei, Bob Davis, and Dinny McMahon, “China Fund Confident of Getting More Cash,” *Wall Street Journal*, May 13, 2011.

187. U.S. Department of the Treasury, *Report on Foreign Portfolio Holdings of U.S. Securities as of June 30, 2010* (Washington, DC: April 2011). <http://www.treasury.gov/resource-center/data-chart-center/tic/Documents/shla2010r.pdf>.

188. Kevin Davies, “Outward [Chinese] FDI and its Policy Context” (New York: Vale Columbia Center, 2010), pp. 259–262.

189. Kevin Davies, “Outward [Chinese] FDI and its Policy Context” (New York: Vale Columbia Center, 2010), p. 259.

190. Derek Scissors (research fellow, The Heritage Foundation), e-mail interview with Commission staff, March 2, 2011.

191. Derek Scissors (research fellow, The Heritage Foundation), e-mail interview with Commission staff, March 2, 2011.

192. Ministry of Commerce of the People’s Republic of China, *2009 Statistical Bulletin of China’s Outward Foreign Direct Investment* (Beijing, China: 2010), p. 12. <http://hzs.mofcom.gov.cn/accessory/201009/1284339524515.pdf>. The \$38.2 billion figure is attributed to *zhongyang qiye*, or “central enterprise,” which refers specifically to SOEs under the direct control of the central government, as opposed to the more generic *guoyou qiye*, which simply means “state-owned enterprise.”

193. For more information on China’s investment patterns, see Nargiza Salidjanova, “Going Out: Overview of China’s Outward Foreign Direct Investment” (Washington, DC: USCC Staff Research Report, March 30, 2011). <http://www.uscc.gov/researchpapers/2011/GoingOut.pdf>.

194. Daniel H. Rosen and Thilo Hanemann, *An American Open Door? Maximizing the Benefits of Chinese Foreign Direct Investment* (New York, NY: Asia Society Special Report, May 2011), p. 33.

195. The authors conclude that the high share of deal value attributable to SOEs is mostly due to three large-scale acquisitions and one big greenfield project by state-owned firms: CIC’s stake in AES (\$2.5 billion), the Tianjin Pipe steel plant (\$1 billion), CNOOC’s stake in the Ford Eagle Shale project (\$1 billion), and Pacific Century’s acquisition of Nexteer Automotive (\$450 million). See Daniel H. Rosen and Thilo Hanemann, *An American Open Door? Maximizing the Benefits of Chinese Foreign Direct Investment* (New York, NY: Asia Society Special Report, May 2011), p. 33.

196. Paritosh Bansal, Soyoung Kim, and Benjamin Lim, “Special Report: The U.S. and China Start an M&A [mergers and acquisitions] Cold War,” Reuters, April 12, 2011.

197. Edward M. Graham and David M. Marchick, *U.S. National Security and Foreign Direct Investment* (Washington, DC: Peterson Institute for International Economics, May 2006), p. 105.

198. Edward M. Graham and David M. Marchick, *U.S. National Security and Foreign Direct Investment* (Washington, DC: Peterson Institute for International Economics, May 2006), p. 107.

199. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Daniel Rosen, March 30, 2011.

200. John Burke, “The United States Welcomes Chinese Foreign Direct Investment—The Handful of Deals Blocked by CFIUS are Aberrant,” *China-U.S.-Trade Law blog*, February 7, 2011. <http://www.chinaustradelawblog.com/2011/02/articles/investment/the-united-states-welcomes-chinese-foreign-direct-investment-the-handful-of-deals-blocked-by-cfius-are-aberrant/>.

201. Clint Shields, “Pipeline to the World,” *Texas Rising* (March/April 2009). <http://www.texasahead.org/texasrising/tr0903/>.

202. Felicity Carus, "Suntech Chief Praises China's Policy Incentives, Builds Plant in Arizona," *AOL Energy*, May 17, 2011.

203. Paritosh Bansal, Soyoung Kim, and Benjamin Lim, "Special Report: The U.S. and China Start an M&A [mergers and acquisitions] Cold War," Reuters, April 12, 2011.

204. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Daniel Rosen, March 30, 2011. Also see Daniel H. Rosen and Thilo Hanemann, *An American Open Door? Maximizing the Benefits of Chinese Foreign Direct Investment* (New York, NY: Asia Society Special Report, May 2011), pp. 66–67.

205. Michael Wines, "China Fortifies State Businesses to Fuel Growth," *New York Times*, August 29, 2010.

206. Wen Jiabao, *2010 Report on the Work of the Government* (Beijing, China: March 5, 2010).

207. Office of the U.S. Trade Representative, "United States Details China and India Subsidy Programs in Submission to WTO" (Washington, DC: October 6, 2011). <http://www.ustr.gov/about-us/press-office/press-releases/2011/october/united-states-details-china-and-india-subsidy-prog>.

208. U.S.-China Economic and Security Review Commission, "An Assessment of China's Subsidies to Strategic and Heavyweight Industries" (Washington, DC: Capital Trade, Incorporated, March 2009), pp. ix-x.

209. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Derek Scissors, March 30, 2011.

210. U.S.-China Business Council [USCBC], *USCBC 2010 Member Priorities Survey Results* (Washington, DC: November 17, 2010), pp. 1, 9. [http://www.uschina.org/public/documents/2010/membership\\_survey.pdf](http://www.uschina.org/public/documents/2010/membership_survey.pdf).

211. U.S. Department of the Treasury, "The 2011 U.S.-China Strategic and Economic Dialogue U.S. Fact Sheet—Economic Track" (Washington, DC: May 10, 2011). <http://www.treasury.gov/press-center/press-releases/Pages/TG1172.aspx>.

212. According to the Bureau of Economic Analysis, Chinese majority-owned nonbank affiliates in the United States employed 4,300 U.S. workers in 2009 (most recent data available).

213. Woodrow Wilson Center for International Scholars, "Chinese Foreign Direct Investment: Is It a Threat to the United States, Domestically or Globally?" (Washington, DC: June 21, 2011). [http://www.wilsoncenter.org/index.cfm?topic\\_id=514556&fuseaction=topics.event\\_summary&event\\_id=700288](http://www.wilsoncenter.org/index.cfm?topic_id=514556&fuseaction=topics.event_summary&event_id=700288).

214. Scott Otteman, "Chamber Seeks U.S. Effort to Pry China Open to More Foreign Investment," *Inside U.S.-China Trade*, July 13, 2011.

215. Wayne M. Morrison, "China-U.S. Trade Issues" (Washington, DC: Congressional Research Service, June 2, 2011), pp. 16–17.

216. Cheng Li, "China's Midterm Jockeying: Gearing Up for 2012 (Part 4: Top Leaders of Major State-Owned Enterprises)," *China Leadership Monitor* 34 (2011):5–8.

217. European Union Chamber of Commerce in China, *Public Procurement in China: European Business Experiences Competing for Public Contracts in China* (Beijing, China: April 2011), p. 15. This figure includes public works projects such as water, transportation, telecommunications, and energy as well as government procurement. [http://www.europeanchamber.com.cn/images/documents/marketing\\_department/beijing/publications/2011/PP%20Study%20EN%20Final\\_0421.pdf](http://www.europeanchamber.com.cn/images/documents/marketing_department/beijing/publications/2011/PP%20Study%20EN%20Final_0421.pdf).

218. U.S. International Trade Commission, "China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy" (Washington, DC: May 2011).

219. Jiang Zemin, "The Government Procurement Law of the People's Republic of China (order of the President No. 68)," *Chinese Government's Official Web Portal*, June 29, 2002. [http://www.gov.cn/english/laws/2005-10/08/content\\_75023.htm](http://www.gov.cn/english/laws/2005-10/08/content_75023.htm).

220. *Chinese Government's Official Web Portal*, "China issues S&T [scientific and technology] development guidelines," February 2006; State Council of the People's Republic of China, *Outline of the National Medium- and Long-Term Program on Scientific and Technological Development (2006–2020)* (Beijing, China: February 9, 2006). [http://www.gov.cn/english/2006-02/09/content\\_183426.htm](http://www.gov.cn/english/2006-02/09/content_183426.htm).

221. *Chinese Government's Official Web Portal*, "China issues S&T [scientific and technology] development guidelines," February 2006; State Council of the People's Republic of China, *Outline of the National Medium- and Long-Term Program on Scientific and Technological Development (2006–2020)* (Beijing, China: February 9, 2006). [http://www.gov.cn/english/2006-02/09/content\\_183426.htm](http://www.gov.cn/english/2006-02/09/content_183426.htm).

222. U.S.-China Economic and Security Review Commission, *Hearing on China's Intellectual Property Rights and Indigenous Innovation Policy*, written testimony of

Alan Wm. Wolff, May 4, 2011. Also see [http://english.gov.cn/2006-07/26/content\\_34673.htm](http://english.gov.cn/2006-07/26/content_34673.htm).

223. European Union Chamber of Commerce in China, *Public Procurement in China: European Business Experiences Competing for Public Contracts in China* (Beijing, China: April 2011), p. 15.

224. European Union Chamber of Commerce in China, *Public Procurement in China: European Business Experiences Competing for Public Contracts in China* (Beijing, China: April 2011), p. 15. [http://www.europeanchamber.com.cn/images/documents/marketing\\_department/beijing/publications/2011/PP%20Study%20EN%20Final\\_0421.pdf](http://www.europeanchamber.com.cn/images/documents/marketing_department/beijing/publications/2011/PP%20Study%20EN%20Final_0421.pdf).

225. United States Trade Representative, *2010 Report to Congress on China's WTO Compliance* (Washington, DC: December 2010), p. 64. [http://www.ustr.gov/webfm\\_send/2596](http://www.ustr.gov/webfm_send/2596).

226. *The World Factbook*, "China: Economy" (Langley, VA: Central Intelligence Agency, 2010 nominal gross national product figure). <https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html>.

227. James McGregor, *China's Drive for 'Indigenous Innovation': A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, July 28, 2010), p. 15. <http://www.uschamber.com/reports/chinas-drive-indigenous-innovation-web-industrial-policies>.

228. State Council of the People's Republic of China, *Medium- and Long-Term National Plan for Science and Technology Development (2006–20)* (Beijing, China: February 2006), as quoted in James McGregor, *China's Drive for 'Indigenous Innovation': A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, July 28, 2010), p. 4. <http://www.uschamber.com/reports/chinas-drive-indigenous-innovation-web-industrial-policies>.

229. U.S.-China Business Council, *Issues Brief: China's Domestic Innovation and Government Procurement Policies* (Washington, DC: March 2011), p. 9q.

230. U.S.-China Economic and Security Review Commission, *Hearing on China's Five Year Plan, Indigenous Innovation and Technology Transfers and Outsourcing*, testimony of John Neuffer, June 15, 2011.

231. U.S. International Trade Commission, "Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the U.S. Economy" (Washington, DC: November 2010), p. 4–2.

232. U.S. International Trade Commission, "Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the U.S. Economy" (Washington, DC: November 2010), p. 4–2.

233. James McGregor, *China's Drive for 'Indigenous Innovation': A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, July 28, 2010), p. 20. <http://www.uschamber.com/reports/chinas-drive-indigenous-innovation-web-industrial-policies>.

234. Letter to Chinese Officials, December 10, 2009. [http://www.tiaonline.org/gov\\_affairs/issues/intl\\_advocacy/documents/12-10-09IntlBusinessLetterNIIPAccreditation.pdf](http://www.tiaonline.org/gov_affairs/issues/intl_advocacy/documents/12-10-09IntlBusinessLetterNIIPAccreditation.pdf).

235. James McGregor, *China's Drive for 'Indigenous Innovation': A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, July 28, 2010), p. 20. <http://www.uschamber.com/reports/chinas-drive-indigenous-innovation-web-industrial-policies>.

236. U.S.-China Business Council, "Intellectual Property and Import Substitution References in China's Provincial and Local-Level Accreditation Criteria for Indigenous Innovation Products" (Washington, DC: July 2011), pp. 1, 11.

237. Kenneth G. Lieberthal, "Managing the China Challenge; How to achieve Corporate Success in the People's Republic" (Washington, DC: The Brookings Institution, 2011), p. 55.

238. *Sohu Finance*, "The Catalogue for the Government Procurement of Indigenous Innovation Products has yet to be issued," July 6, 2011. [http://www.ccgp.gov.cn/lisj/cgxx/201107/t20110706\\_1680731.shtml](http://www.ccgp.gov.cn/lisj/cgxx/201107/t20110706_1680731.shtml).

239. U.S.-China Business Council, "Provincial and Local Indigenous Innovation Product Catalogues" (Washington, DC: July 2011), p. 1. [https://www.uschina.org/public/documents/2011/07/local\\_ii\\_catalogues.pdf](https://www.uschina.org/public/documents/2011/07/local_ii_catalogues.pdf).

240. U.S.-China Business Council, "Provincial and Local Indigenous Innovation Product Catalogues" (Washington, DC: July 2011), p. 1. [https://www.uschina.org/public/documents/2011/07/local\\_ii\\_catalogues.pdf](https://www.uschina.org/public/documents/2011/07/local_ii_catalogues.pdf).

241. U.S.-China Business Council, "Provincial and Local Indigenous Innovation Product Catalogues" (Washington, DC: July 2011), p. 1. [https://www.uschina.org/public/documents/2011/07/local\\_ii\\_catalogues.pdf](https://www.uschina.org/public/documents/2011/07/local_ii_catalogues.pdf).

242. AmCham-China, *2011 White Paper on American Business in China* (Beijing, China: April 2011), p. 56. <http://web.resource.amchamchina.org/cmsfile/2011/04/25/3669adf22687ab754895c0b30da144b3.pdf>.

243. James McGregor, *China's Drive for 'Indigenous Innovation': A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, July 28, 2010), p. 19. <http://www.uschamber.com/reports/chinas-drive-indigenous-innovation-web-industrial-policies>.

244. National People's Congress of the People's Republic of China, *Enterprise Income Tax Law of the People's Republic of China* (trans. Lehman, Lee & Xu, LLX Translation Department) (March 16, 2007). [http://www.lehmanlaw.com/fileadmin/lehmanlaw\\_com/laws\\_regulations/Enterprise\\_Income\\_Tax\\_Law\\_of\\_the\\_PRC\\_LLX\\_03162007\\_.pdf](http://www.lehmanlaw.com/fileadmin/lehmanlaw_com/laws_regulations/Enterprise_Income_Tax_Law_of_the_PRC_LLX_03162007_.pdf).

245. Price Waterhouse Coopers, "Overview of PRC [People's Republic of China] Taxation System" (Hong Kong, SAR [Special Administrative Region]: September 5, 2011). [http://www.pwchk.com/home/eng/prctax\\_corp\\_overview\\_taxation.html](http://www.pwchk.com/home/eng/prctax_corp_overview_taxation.html).

246. U.S.-China Economic and Security Review Commission, *Hearing on China's Intellectual Property Rights and Indigenous Innovation Policy*, written testimony of Thea Lee, May 4, 2011.

247. U.S.-China Economic and Security Review Commission, *Hearing on China's Intellectual Property Rights and Indigenous Innovation Policy*, testimony of Thea Lee, May 4, 2011.

248. Jason Cooper and Stephanie Chu, "Surge in Chinese Innovation and the IP [intellectual property] Implications" (Washington, DC: Intellectual Property Owners Association, January 2011). [www.ipo.org/articles](http://www.ipo.org/articles).

249. James McGregor, *China's Drive for 'Indigenous Innovation': A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, July 28, 2010), p. 26. <http://www.uschamber.com/reports/chinas-drive-indigenous-innovation-web-industrial-policies>.

250. Jason Cooper and Stephanie Chu, "Surge in Chinese Innovation and the IP [intellectual property] Implications" (Washington, DC: Intellectual Property Owners Association, January 2011). [www.ipo.org/articles](http://www.ipo.org/articles).

251. Dieter Ernst, *Briefing to the U.S.-China Economic and Security Review Commission* (East-West Center, Honolulu, HI, May 17, 2011).

252. U.S.-China Economic and Security Review Commission, *Hearing on China's Intellectual Property Rights and Indigenous Innovation Policy*, testimony of Alan Wm. Wolff, May 4, 2011.

253. U.S. House of Representatives, Committee on Foreign Affairs, Subcommittee on Terrorism, Nonproliferation, and Trade, *testimony of Karen Laney*, 112th Cong., 1st sess., March 9, 2011. <http://foreignaffairs.house.gov/112/lan030911.pdf>.

254. U.S. House of Representatives, Committee on Foreign Affairs, Subcommittee on Terrorism, Nonproliferation, and Trade, *testimony of Karen Laney*, 112th Cong., 1st sess., March 9, 2011. <http://foreignaffairs.house.gov/112/lan030911.pdf>.

255. U.S. Department of Commerce, "21st U.S.-China Joint Commission on Commerce and Trade Fact Sheet" (Washington, DC: December 2010). <http://www.commerce.gov/node/12467>.

256. United States Trade Representative, "U.S.-China Joint Commission on Commerce and Trade 2010: China Agrees to Significant IP [intellectual property] Rights Enforcement, Market Opening, and Revisions to Indigenous Innovation Policies That Will Help Boost U.S. Exports" (Washington, DC: December 2010). <http://www.ustr.gov/about-us/press-office/press-releases/2010/december/us-china-joint-commission-commerce-and-trade-2010>.

257. The White House, Office of the Press Secretary, "U.S.-China Joint Statement" (Washington, DC: January 19, 2011). <http://www.whitehouse.gov/the-press-office/2011/01/19/us-china-joint-statement>

258. Barack Obama, Press Conference with President Obama and President Hu of the People's Republic of China (Washington, DC: January 19, 2011). <http://www.whitehouse.gov/the-press-office/2011/01/19/press-conference-president-obama-and-president-hu-peoples-republic-china>.

259. U.S. Department of the Treasury, "Third Meeting of the U.S.-China Strategic and Economic Dialogue Joint U.S.-China Economic Track Fact Sheet" (Washington, DC: May 10, 2011). <http://www.treasury.gov/press-center/press-releases/Pages/tg1170.aspx>.

260. *Inside U.S.-China Trade*, "Telecom Groups Urge China Directive to Clarify Innovation-Procurement Delink," October 5, 2011, p. 4.

261. Chinese Ministry of Finance, *Evaluation Measures on Indigenous Innovation Products for Government Procurement* (Beijing, China: April 3, 2007); and Chinese Ministry of Finance, *Administrative Measures on Government Procurement Contracts for Indigenous Innovation Products* (Beijing, China: April 3, 2007).



262. Chinese Ministry of Finance, Ministry of Science and Technology, and National Development and Reform Commission, Notice Concerning the Repeal of *Trial Measures for the Administration for the Accreditation of National Indigenous Innovation Products* (Beijing, China: July 4, 2011).

263. U.S.-China Business Council, *Issues Brief: China's Domestic Innovation and Government Procurement Policies* (Washington DC: March 2011), p. 8.

264. U.S.-China Business Council, "USCBC Statement on China's Innovation and Procurement Regulatory Changes" (Washington, DC: June 29, 2011). <https://www.uschina.org/public/documents/2011/06/statement-on-regulatory-changes.html>.

265. European Union Chamber of Commerce in China, "European Chamber Welcomes the Ministry of Finance's Announcement on Abolishing Indigenous Innovation-Related Policies" (Beijing, China: July 1, 2011). <http://www.europeanchamber.com.cn/view/media/printview?cid=8939&print=1>.

266. Jiangsu Province Government Procurement Office, Provincial government ministries and agencies convened for a conference on the government procurement policy for indigenous innovation products, Vice Minister Song Yiwu attended and spoke, Jiangsu Government Procurement website, July 19, 2011. [http://www.ccgj-jiangsu.gov.cn/pub/jszfcg/xwdt/xw/201107/t20110719\\_50444.html](http://www.ccgj-jiangsu.gov.cn/pub/jszfcg/xwdt/xw/201107/t20110719_50444.html).

267. Jiangsu Province Government Procurement Office, Provincial government ministries and agencies convened for a conference on the government procurement policy for indigenous innovation products, Vice Minister Song Yiwu attended and spoke, Jiangsu Government Procurement website, July 19, 2011. [http://www.ccgj-jiangsu.gov.cn/pub/jszfcg/xwdt/xw/201107/t20110719\\_50444.html](http://www.ccgj-jiangsu.gov.cn/pub/jszfcg/xwdt/xw/201107/t20110719_50444.html).

268. Shanghai Municipality Finance Bureau, Notice Regarding the Repeal of *Shanghai Municipality Operating Procedures on the Government Procurement of Indigenous Innovation Products* (Shanghai, China: June 30, 2011). [http://www.czj.sh.gov.cn/zcfj/gfxwj/zfcg/201107/t20110708\\_128212.html](http://www.czj.sh.gov.cn/zcfj/gfxwj/zfcg/201107/t20110708_128212.html).

269. Dustin Ensinger, "Locke Chides China on Indigenous Innovation," *Economy in Crisis; America's Economic Report*, February 3, 2011. <http://economyincrisis.org/content/locke-chides-china-indigenous-innovation>.

270. Gary Locke, "Remarks to Asia Society on Chinese Foreign Direct Investment in America," *An American Open Door? Maximizing the Benefits of Chinese Foreign Direct Investment* (Keynote Address: Asia Society, Kissinger Institute on China and the United States, Washington, DC, May 4, 2011). <http://asiasociety.org/policy/center-us-china-relations/complete-text-us-commerce-secretary-gary-lockes-asia-society-speech>.

271. U.S.-China Economic and Security Review Commission, *Hearing on Chinese State-Owned Enterprises and U.S.-China Bilateral Investment*, testimony of Theodore H. Moran, March 30, 2011.

272. U.S.-China Economic and Security Review Commission, *Hearing on China's Five-Year Plan, Indigenous Innovation and Technology Transfers and Outsourcing*, written testimony of Dieter Ernst, June 15, 2011.

273. *Sohu Finance*, "The catalogue for the government procurement of indigenous innovation products has not yet been issued," July 6, 2011. [http://www.ccgj.gov.cn/ljsj/cgxx/201107/t20110706\\_1680731.shtml](http://www.ccgj.gov.cn/ljsj/cgxx/201107/t20110706_1680731.shtml).

274. Gary Locke, "Keynote Address, U.S.-China Business Council Luncheon" (U.S.-China Business Council, Washington DC, January 13, 2011). <http://www.commerce.gov/news/secretary-speeches/2011/01/13/remarks-us-china-business-council-luncheon>.

275. Colin Beere, "Hybrid in a Trade Squeeze," *New York Times*, September 5, 2011.

276. Sharon Terlep, "Road Gets Bumpy for GM in China," *Wall Street Journal*, September 16, 2011.

277. Sharon Terlep, "Road Gets Bumpy for GM in China," *Wall Street Journal*, September 16, 2011.

278. World Trade Organization, "Intellectual Property: Protection and Enforcement" (Geneva, Switzerland). [http://www.wto.org/english/thewto\\_e/whatis\\_e/tif\\_e/agrm7\\_e.htm](http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm).

279. Office of the United States Trade Representative, *2011 Special 301 Report* (Washington, DC: 2011).

280. Wayne M. Morrison, "China-U.S. Trade Issues" (Washington, DC: Congressional Research Service, August 10, 2011).

281. U.S. Customs and Border Protection, "Department of Homeland Security IPR [intellectual property rights] Seizures" (Washington DC: Intellectual Property Rights National Targeting and Analysis Group, March 16, 2011).

282. U.S. International Trade Commission, "China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy" (Washington, DC: May 2011), pp. 2-3.

283. Paul Goldstein, *Intellectual Property: The Tough New Realities That Could Make or Break Your Business* (New York: Portfolio, 2007), p. 2.
284. Nam Pham, "The Impact of Innovation and the Role of Intellectual Property Rights on U.S. Productivity, Competitiveness, Jobs, Wages and Exports" (Washington, DC: NDP Consulting, April 2010).
285. Nam Pham, "The Impact of Innovation and the Role of Intellectual Property Rights on U.S. Productivity, Competitiveness, Jobs, Wages and Exports" (Washington, DC: NDP Consulting, April 2010).
286. Nam Pham, "The Impact of Innovation and the Role of Intellectual Property Rights on U.S. Productivity, Competitiveness, Jobs, Wages and Exports" (Washington, DC: NDP Consulting, 2010).
287. U.S.-China Economic and Security Review Commission, *Hearing on "China's Intellectual Property Rights and Indigenous Innovation Policy"*, testimony of Michael Schlesinger, May 4, 2011.
288. Robert Holleyman, "How Chinese companies steal a critical business advantage," *Hill (Washington, DC)*, May 11, 2011.
289. Business Software Alliance, "Eighth Annual BSA Global Software 2010 Piracy Study" (Washington, DC: May 2011).
290. Business Software Alliance, "Eighth Annual BSA Global Software 2010 Piracy Study" (Washington, DC: May 2011).
291. David Leonhardt, "Software Piracy in China," *New York Times*, January 19, 2011.
292. International Intellectual Property Alliance, *2011 Special 301 Report on Copyright Protection and Enforcement, People's Republic of China* (Washington, DC: February 15, 2011). <http://www.iipa.com/rbc/2011/2011SPEC301PRC.pdf>.
293. International Intellectual Property Alliance, *2011 Special 301 Report on Copyright Protection and Enforcement, People's Republic of China* (Washington, DC: February 15, 2011). <http://www.iipa.com/rbc/2011/2011SPEC301PRC.pdf>.
294. John H. Jackson, William J. Davey, and Alan O. Sykes, Jr., *Legal Problems of International Economic Relations, Documents Supplement, Trade Related Aspects of Intellectual Property Rights* (St. Paul, MN: Thomson-West, 2008), p. 360.
295. TechNode, "Baidu Promises to Put An End to its Music Piracy," June 14, 2011. <http://technode.com/2011/06/14/baidu-promises-to-put-an-end-to-its-music-piracy/>; Office of the U.S. Trade Representative, *2011 Special 301 Report* (Washington, DC: April 2011), p. 21.
296. U.S.-China Economic and Security Review Commission, *Hearing on China's Intellectual Property Rights and Indigenous Innovation Policy*, testimony of Michael Schlesinger, May 4, 2011.
297. Business Software Alliance, "Internet Software Piracy: A Multifaceted Challenge" (Washington, DC). <http://internet.bsa.org/overview/home.aspx>.
298. U.S.-China Economic and Security Review Commission, *Hearing on China's Intellectual Property Rights and Indigenous Innovation Policy*, testimony of Michael Schlesinger, May 4, 2011.
299. U.S.-China Economic and Security Review Commission, *Hearing on China's Intellectual Property Rights and Indigenous Innovation Policy*, testimony of Ken Wasch, May 4, 2011.
300. International Intellectual Property Alliance, *2011 Special 301 Report on Copyright Protection and Enforcement, People's Republic of China* (Washington, DC: February 15, 2011). <http://www.iipa.com/rbc/2011/2011SPEC301PRC.pdf>.
301. U.S.-China Economic and Security Review Commission, *Hearing on China's Intellectual Property Rights and Indigenous Innovation Policy*, testimony of Michael Schlesinger, May 4, 2011.
302. Interview with local American business representatives, U.S.-China Economic and Security Review Commission in Hong Kong, August 2011.
303. U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing and Trade, *Hearing on Made in America: Increasing Jobs through Exports and Trade*, testimony of Robert W. Holleyman II, 107th Cong., 1st sess., March 16, 2001.
304. Business Software Alliance, "ITC [U.S. International Trade Commission] Report Highlights Severe Economic Consequences of Intellectual Property Theft in China" (Washington DC: May 18, 2011). <http://www.bsa.org/country/News%20and%20Events/News%20Archives/en/2011/en-05182011-itc.aspx>.
305. *Forbes*, "China Tops U.S. As the World's Largest PC [personal computer] Market," August 23, 2011. <http://www.forbes.com/sites/ericavitz/2011/08/23/china-tops-u-s-as-the-worlds-largest-pc-market/>.
306. U.S. International Trade Commission, "China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy" (Washington, DC: May 2011), pp. 3–15.



307. U.S.-China Economic and Security Review Commission, *Hearing on China's Intellectual Property Rights and Indigenous Innovation Policy*, testimony of Slade Gorton, May 4, 2011.

308. U.S. International Trade Commission, *Hearing on China: Intellectual Property Infringement, Indigenous Innovation Policies and Frameworks for Measuring the Effects on the U.S. Economy* (Washington, DC: testimony of Jeremie Waterman, June 15, 2010).

309. Business Software Alliance, *Piracy Impact Study: The Economic Benefits of Reducing Software Piracy* (Washington, DC: 2010). <http://portal.bsa.org/piracyimpact2010/studies/piracyimpactstudy2010.pdf>.

310. Aaron L. Friedberg, *A Contest for Supremacy* (New York, NY: W.W. Norton, 2011), p. 236.

311. For more on the formulation of the five-year plans, including the institutional processes involved in the 12th Five-Year Plan, see Joseph Casey and Katherine Koleski, "Backgrounder: China's 12th Five-Year Plan" (Washington, DC: USCC Staff Research Report, June 24, 2011). [www.uscc.gov/researchpapers/research\\_archive.php](http://www.uscc.gov/researchpapers/research_archive.php).

312. C. Cindy Fan, "China's Eleventh Five-Year Plan (2006–2010): From 'Getting Rich First' to 'Common Prosperity,'" *Eurasian Geography and Economics* 47:6 (2006): 708. <http://www.sscnet.ucla.edu/geog/downloads/597/300.pdf>.

313. For the full text of the 12th Five-Year Plan, see "Guomin jingji he shehui fazhan dishier ge wunian guihua gangyao" (People's Economy and Social Development 12th Five-Year Plan Outline), *Zhonghua Renmin Gongheguo Zhongyang Renmin Zhengfu* (Central People's Government). [http://www.gov.cn/2011lh/content\\_1825838.htm](http://www.gov.cn/2011lh/content_1825838.htm).

314. Open Source Center, "China: NPC [National People's Congress] Reconfirms China's Development Strategies, Sets Goals for 2011 and Next Five Years," March 11, 2011. OSC ID: CPF20110311786003, p. 2. <http://www.opensource.gov>.

315. U.S.-China Economic and Security Review Commission, *Hearing on China's Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Eswar Prasad, June 15, 2011.

316. Xinhua, "Premier: China Confident in Maintaining Economic Growth," March 16, 2007.

317. Stephen S. Roach, "China's 12th Five-Year Plan: Strategy vs. Tactics," Morgan Stanley, March 21, 2011. <http://www.scribd.com/doc/51554032/Chinas-Twelve-Five-Year-Plan-032111>.

318. U.S.-China Economic and Security Review Commission, *Hearing on China's Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Eswar Prasad, June 15, 2011.

319. For a detailed discussion of China's response to the financial crisis, see U.S.-China Economic and Security Review Commission, "China's Role in the Origins of the Global Financial Crisis and China's Response," in U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), pp. 38–55.

320. Wen Jiabao, "Report on the Work of the Government," March 5, 2011. <http://online.wsj.com/public/resources/documents/2011NPCWorkReportEng.pdf>.

321. APCO Worldwide, "China's 12th Five-Year Plan: How it actually works and what's in store for the next five years" (Washington, DC: December 10, 2010), p. 3. [http://www.apcoworldwide.com/content/pdfs/chinas\\_12th\\_five-year\\_plan.pdf](http://www.apcoworldwide.com/content/pdfs/chinas_12th_five-year_plan.pdf).

322. Qing Wang, Seven Zhang, and Ernest Ho, "The China Files: Chinese Economy Through 2020," Morgan Stanley Blue Paper, November 8, 2010, pp. 29–30. [http://www.morganstanley.com/views/perspectives/China\\_Economy\\_2020.pdf](http://www.morganstanley.com/views/perspectives/China_Economy_2020.pdf).

323. Stephen S. Roach, "China's 12th Five-Year Plan: Strategy vs. Tactics," Morgan Stanley, March 21, 2011. <http://www.scribd.com/doc/51554032/Chinas-Twelve-Five-Year-Plan-032111>.

324. Trevor Houser, "China's Low-Carbon Development" (event at The Brookings Institution, Washington, DC, May 31, 2011). [http://www.brookings.edu/~media/Files/events/2011/0531\\_china\\_carbon/20110531\\_china\\_carbon.pdf](http://www.brookings.edu/~media/Files/events/2011/0531_china_carbon/20110531_china_carbon.pdf).

325. Stephen S. Roach, "China's 12th Five-Year Plan: Strategy vs. Tactics," Morgan Stanley, March 21, 2011. <http://www.scribd.com/doc/51554032/Chinas-Twelve-Five-Year-Plan-032111>.

326. See Wen Jiabao, "Report on the Work of the Government," March 5, 2011, p. 14. <http://online.wsj.com/public/resources/documents/2011NPCWorkReportEng.pdf>.

327. APCO Worldwide, "China's 12th Five-Year Plan: How it actually works and what's in store for the next five years" (Washington, DC: December 10, 2010), p. 1. [http://www.apcoworldwide.com/content/pdfs/chinas\\_12th\\_five-year\\_plan.pdf](http://www.apcoworldwide.com/content/pdfs/chinas_12th_five-year_plan.pdf). For an example of a longer-term goal, the State Council announced targets on November 26, 2009, for energy reduction, carbon reduction, and nonfossil fuel energy by 2020.

The 2015 targets laid out in the 12th Five-Year Plan are only an intermediate step in achieving these goals. For details on these 2020 targets, *see* Xinhua, “China announces targets on carbon emission cuts,” November 26, 2009.

328. Alan Wheatley, “Why the world should heed China’s five-year plan,” Reuters, March 7, 2011.

329. U.S.-China Economic and Security Review Commission, *Hearing on China’s Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Eswar Prasad, June 15, 2011.

330. U.S.-China Economic and Security Review Commission, *Hearing on China’s Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Eswar Prasad, June 15, 2011.

331. Michael Pettis, “Post-Crisis China and the Changing Global Economic Order” (Carnegie Endowment for International Peace event, Brussels, Belgium, September 8, 2010); Michael Pettis, “China Faces a Difficult Economic Transition” (Washington, DC: Carnegie Endowment for International Peace, *Carnegie Commentary*, August 25, 2010).

332. Stephen S. Roach, “China’s 12th Five-Year Plan: Strategy vs. Tactics,” Morgan Stanley, March 21, 2011. <http://www.scribd.com/doc/51554032/Chinas-Twelve-Five-Year-Plan-032111>.

333. Stephen S. Roach, “China’s 12th Five-Year Plan: Strategy vs. Tactics,” Morgan Stanley, March 21, 2011. <http://www.scribd.com/doc/51554032/Chinas-Twelve-Five-Year-Plan-032111>.

334. U.S.-China Economic and Security Review Commission, *Hearing on China’s Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Willy C. Shih, June 15, 2011.

335. Taiyuan Xinwen Wang, “Woshi Chutai <Yijian>: Jiakuai peiyu he fazhan zhanluexing xingxinchanye” (Our City Promulgates the Opinion: Speed up the development of SEIs), May 25, 2011.

336. APCO Worldwide, “China’s 2011 National People’s Congress (NPC): Fine-tuning the economy with an eye on social stability” (Washington, DC: March 2011). [http://www.apcoworldwide.com/content/PDFs/npc\\_briefing\\_2011.pdf](http://www.apcoworldwide.com/content/PDFs/npc_briefing_2011.pdf).

337. Patrick Chovanec, “China’s Been Working on the Railroad,” *Business Insider*, May 25, 2011. <http://www.businessinsider.com/chinas-been-working-on-the-railroad-2011-5>. On claims of technology theft in the railway industry, see Thomas M. Hout and Pankaj Ghemawat, “China vs. the World: Whose Technology Is It?” *Harvard Business Review* (December 2010); Robert Samuelson, “China’s new world order demands stronger U.S. response,” *Washington Post*, January 24, 2011.

338. *Zhongguo Zhengjuan Bao* (China). “Guli Jinrong Jigou Rongzi Zhichi Zhanluexing Xinxing Chanye” (Encourage Finance Institutions to Support SEIs), December 1, 2010.

339. National Development and Reform Commission, “Report on the Implementation of the 2010 Plan for National Economic and Social Development and on the 2011 Draft Plan for National Economic and Social Development,” Eleventh National People’s Congress, March 5, 2011, <http://online.wsj.com/public/resources/documents/2011NDRReportEng.pdf>.

340. Confederation of British Industries, Full English Translation of 12th Five-Year Plan. <http://www.cbichina.org.cn/cbichina/upload/fckeditor/Full%20Translation%20of%20the%2012th%20Five-Year%20Plan.pdf>.

341. KPMG, “China’s 12th Five-Year Plan: Overview,” March 2011, p. 2. <http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Publicationseries/5-years-plan/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf>.

342. “According to the U.S. Census Bureau, U.S. imports of advanced technology products (ATP) from China in 2009 totaled \$89.7 billion. ATP products accounted for 30.3 percent of total U.S. imports from China, compared to 19.2 percent (\$29.3 billion) in 2003. In addition, China in 2009 accounted for 29.8 percent of total U.S. ATP imports, compared to 14.1 percent in 2003.” Wayne Morrison, *China-U.S. Trade Issues* (Washington, DC: Congressional Research Service, January 2011), p. 7.

343. TradeStats Express, <http://tse.export.gov>.

344. U.S.-China Economic and Security Review Commission, *Hearing on China’s Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Willy C. Shih, June 15, 2011.

345. James McGregor, “China’s Drive for ‘Indigenous Innovation’: A Web of Industrial Policies” (Washington, DC: APCO Worldwide, July 28, 2010), p. 13.

346. Jason Cooper and Stephanie Chu, “Surge in Chinese Innovation and the IP [intellectual property] Implications” (Washington, DC: Intellectual Property Owners Association, January 2011). [www.ipo.org/articles](http://www.ipo.org/articles).

347. James McGregor, “China’s Drive for ‘Indigenous Innovation’: A Web of Industrial Policies” (Washington, DC: APCO Worldwide, July 28, 2010), p. 15.

348. Xinhua, "China's top political stresses indigenous innovation," April 19, 2011.
349. APCO Worldwide, "China's 12th Five Year Plan—Prepared for Public Affairs Council" (Washington, DC: April 2011), slide 15. [http://pac.org/files/Presentation\\_China's%20Five%20Year%20Plan.pdf](http://pac.org/files/Presentation_China's%20Five%20Year%20Plan.pdf).
350. Nick Carey and James Kelleher, "Special report: Does corporate America kowtow to China?" Reuters, April 27, 2011. <http://www.reuters.com/article/2011/04/27/us-special-report-china-idUSTRE73Q10X20110427>.
351. Dieter Ernst, *Briefing to the U.S.-China Economic and Security Review Commission*, East-West Center, Honolulu, HI, May 17, 2011.
352. Christopher McNally, *Briefing to the U.S.-China Economic and Security Review Commission*, East-West Center, Honolulu, HI, May 17, 2011.
353. Gordon Orr, "Unleashing innovation in China," McKinsey & Company, January 2011.
354. Wayne Morrison, *China-U.S. Trade Issues* (Washington, DC: Congressional Research Service, May 6, 2011), Summary.
355. Bureau of Economic Analysis, "Summary Estimates for Multinational Companies: Employment, Sales and Capital Expenditures for 2009" (Washington, DC: U.S. Department of Commerce, *News Release BEA 11-16*, April 18, 2011). <http://www.bea.gov/newsreleases/international/mnc/2011/pdf/mnc2009.pdf>.
356. Greg Linden, Jason Dedrick, and Kenneth Kraemer, "Innovation and Job Creation in a Global Economy: The Case of Apple's iPod" (Irvine, CA: University of California-Irvine, Personal Computing Industry Center, January 2009), p. 2.
357. Greg Linden, Jason Dedrick, and Kenneth Kraemer, "Innovation and Job Creation in a Global Economy: The Case of Apple's iPod" (Irvine, CA: University of California-Irvine, Personal Computing Industry Center, January 2009), p. 9.
358. Gary P. Pisano and Willy C. Shih, "Restoring American Competitiveness," *Harvard Business Review* (July-August 2009).
359. U.S.-China Economic and Security Review Commission, *Hearing on China's Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Ralph E. Gomory, June 15, 2011.
360. World Trade Organization, *Accession of the People's Republic of China, Decision of 10 November 2001*, WT/L/432, IV.8(a) (Geneva, Switzerland), p. 16. <http://docsonline.wto.org/imrd/directdoc.asp?DDFDdocuments/t/WT/L/432.doc>. See also The White House, Office of Public Liaison, "Summary of U.S.-China Bilateral WTO Agreement," Briefing on the Clinton Administration Agenda for the World Trade Organization Material (Washington, DC: November 17, 1999). <http://www.uschina.org/public/991115a.html>.
361. Thomas Hout and Pankaj Ghemawat, "China vs. the World: Whose Technology Is It?" *Harvard Business Review* (2010): 3, 5.
362. Thomas Hout and Pankaj Ghemawat, "China vs. the World: Whose Technology Is It?" *Harvard Business Review* (2010): 5.
363. Doug Palmer, "Analysis: Hu addresses U.S. stress over China high-tech drive," *International Business Times*, January 21, 2011. <http://www.ibtimes.com/articles/103394/20110121/analysis-hu-addressess-stress-over-china-high-tech-drive.htm>.
364. Dieter Ernst, *Briefing to the U.S.-China Economic and Security Review Commission*, East-West Center, Honolulu, HI, May 17, 2011.
365. Thomas Hout and Pankaj Ghemawat, "China vs. the World: Whose Technology Is It?" *Harvard Business Review* (2010): 4–5.
366. Thomas Hout and Pankaj Ghemawat, "China vs the World: Whose Technology Is It?" *Harvard Business Review* (2010): 3.
367. Keith Bradsher, "G.M. Aims the Volt at China, but Chinese Want Its Secrets," *New York Times*, September 5, 2011.
368. Keith Bradsher, "G.M. Plans to Develop Electric Cars with China," *New York Times*, September 20, 2011. <http://www.nytimes.com/2011/09/21/business/global/gm-plans-to-develop-electric-cars-with-chinese-automaker.html>.
369. Keith Bradsher, "G.M. Aims the Volt at China, but Chinese Want Its Secrets," *New York Times*, September 5, 2011.
370. James McGregor, "China's Drive for 'Indigenous Innovation': A Web of Industrial Policies" (Washington, DC: APCO Worldwide, July 28, 2010), p. 32.
371. Jason Cooper and Stephanie Chu, "Surge in Chinese Innovation and the IP [intellectual property] Implications" (Washington, DC: Intellectual Property Owners Association, January 2011). [www.ipo.org/articles](http://www.ipo.org/articles).
372. Edward Steinfeld, "Why China's Rise is Not a Threat to the West" (Event at the School for Advanced International Studies, Washington, DC, March 9, 2011).
373. Gordon Orr, "Unleashing Innovation in China," McKinsey & Company, January 2011.

374. Nick Carey and James Kelleher, “Special report: Does corporate America kowtow to China?” Reuters, April 27, 2011. <http://www.reuters.com/article/2011/04/27/us-special-report-china-idUSTRE73Q10X20110427>.

375. U.S.-China Economic and Security Review Commission, *Hearing on China’s Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Leo Hindery, June 15, 2011.

376. U.S.-China Economic and Security Review Commission, *Hearing on China’s Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Philip I. Levy, June 15, 2011.

377. U.S.-China Economic and Security Review Commission, *Hearing on China’s Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Ralph E. Gomory, June 15, 2011.

378. Gary P. Pisano and Willy C. Shih, “Restoring American Competitiveness,” *Harvard Business Review* (July-August 2009).

379. U.S.-China Economic and Security Review Commission, *Hearing on China’s Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Leo Hindery, June 15, 2011.

380. U.S.-China Economic and Security Review Commission, *Hearing on China’s Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Philip I. Levy, June 15, 2011.

381. Nick Carey and James B. Kelleher, “Special Report: Does Corporate America Kowtow to China?” Reuters, April 27, 2011. <http://www.reuters.com/article/2011/04/27/us-special-report-china-idUSTRE73Q10X20110427>.

382. U.S.-China Economic and Security Review Commission, *Hearing on China’s Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Willy C. Shih, June 15, 2011.

383. Nick Carey and James Kelleher, “Special report: Does corporate America kowtow to China?” Reuters, April 27, 2011. <http://www.reuters.com/article/2011/04/27/us-special-report-china-idUSTRE73Q10X20110427>.

384. U.S.-China Economic and Security Review Commission, *Hearing on The Impact of Trade with China on New York State and Opportunities for Economic Growth*, testimony of Willy C. Shih, July 23, 2009.

385. Roger Cliff, Chad J. R. Ohlandt, and David Yang, *Ready for Takeoff: China’s Advancing Aerospace Industry* (report prepared by the RAND Corporation for the U.S.-China Economic and Security Review Commission, 2011), p. 37. [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf).

386. Roger Cliff, Chad J. R. Ohlandt, and David Yang, *Ready for Takeoff: China’s Advancing Aerospace Industry* (report prepared by the RAND Corporation for the U.S.-China Economic and Security Review Commission, 2011), p. 115. [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf).

387. General Electric Aviation, “GE and AVIC Sign Agreement for Integrated Avionics Joint Venture,” Press Release, January 21, 2011. [http://www.geae.com/aboutgeae/presscenter/systems/systems\\_20110121.html](http://www.geae.com/aboutgeae/presscenter/systems/systems_20110121.html).

388. Bill Gertz, “GE–China Venture Probed,” *Washington Times*, August 31, 2011. For more information on the close integration of China’s commercial and military aviation sectors, see U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), pp. 92–105.

389. Bill Gertz, “GE–China Venture Probed,” *Washington Times*, August 31, 2011.

390. Gary P. Pisano and Willy C. Shih, “Restoring American Competitiveness,” *Harvard Business Review* (July-August 2009). See also *Economist*, “Multinational Manufacturers Moving back to America,” May 14, 2011; Greg Linden, Jason Dedrick, and Kenneth Kraemer, “Innovation and Job Creation in a Global Economy: The Case of Apple’s iPod” (Irvine, CA: University of California-Irvine, Personal Computing Industry Center, January 2009), p. 4; Clyde Prestowitz, “Clyde Prestowitz: The Betrayal of American Prosperity (Excerpt),” May 11, 2010. <http://www.progressivereader.com/?p=58997>.

391. Greg Linden, Jason Dedrick, and Kenneth Kraemer, “Innovation and Job Creation in a Global Economy: The Case of Apple’s iPod” (Irvine, CA: University of California-Irvine, Personal Computing Industry Center, January 2009), pp. 5, 9.

392. “In reality, there are relatively few high-tech industries where the manufacturing process is not a factor in developing new—especially, radically new—products.” Gary P. Pisano and Willy C. Shih, “Restoring American Competitiveness,” *Harvard Business Review* (July-August 2009).

393. Andy Grove, “How America Can Create Jobs,” *Bloomberg BusinessWeek*, July 1, 2010.



394 U.S.-China Economic and Security Review Commission, *Hearing on China's Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Eswar Prasad, June 15, 2011.

395. U.S.-China Economic and Security Review Commission, *Hearing on China's Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing*, testimony of Willy C. Shih, June 15, 2011.

396. World Bank, "Southwest Poverty Reduction Project" (Washington, DC) <http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/EASTASIAPACIFICEXT/CHINAEXTN/0,,contentMDK:20680094~pagePK:141137~piPK:141127~theSitePK:318950,00.html>.

397. Drew Thompson (then director of China Studies, Nixon Center, Washington, DC), interview with Commission staff, December 28, 2010.

398. The World Bank, "Results Profile: China Poverty Reduction" (Washington, DC: March 19, 2010). <http://www.worldbank.org/en/news/2010/03/19/results-profile-china-poverty-reduction>.

399. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Murray Scot Tanner, February 25, 2011.

400. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, written testimony of Martin Whyte, February 25, 2011.

401. Transparency International, "Corruption Perceptions Index 2010" (Berlin, Germany: October 2010). [http://www.transparency.org/policy\\_research/surveys\\_indices/cpi/2010](http://www.transparency.org/policy_research/surveys_indices/cpi/2010).

402. The 2010 Corruption Perceptions Index draws on different assessments and business opinion surveys carried out by independent and reputable institutions. It captures information about the administrative and political aspects of corruption. Broadly speaking, the surveys and assessments used to compile the index include questions relating to bribery of public officials, kickbacks in public procurement, embezzlement of public funds, and questions that probe the strength and effectiveness of public sector anticorruption efforts. [http://www.transparency.org/policy\\_research/surveys\\_indices/cpi/2010/in\\_detail#2](http://www.transparency.org/policy_research/surveys_indices/cpi/2010/in_detail#2).

403. Mike Forsythe, "China Investigated 240,000 Official Corruption Cases Over Seven Years," Bloomberg News, December 29, 2010.

404. Keith Richburg, "Chinese Scandals Raise Public Ire," *Washington Post*, January 1, 2011.

405. Keith Richburg, "Chinese Scandals Raise Public Ire," *Washington Post*, January 1, 2011.

406. Dan Levin, "China's New Wealth Spurs a Market for Mistresses," *New York Times*, August 9, 2011. <http://www.nytimes.com/2011/08/10/world/asia/10mistress.html>.

407. Dan Levin, "China's New Wealth Spurs a Market for Mistresses," *New York Times*, August 9, 2011. <http://www.nytimes.com/2011/08/10/world/asia/10mistress.html>.

408. Agence France-Presse, "Corruption 'still very serious,' government reports," December 29, 2010.

409. Associated Press, "Report Reveals Huge Scale of Corruption among Chinese Government Officials," *Guardian (United Kingdom)*, June 17, 2011. <http://www.guardian.co.uk/world/2011/jun/17/report-corruption-Chinese-government-officials>.

410. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, written testimony of Martin Whyte, February 25, 2011.

411. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, written testimony of Martin Whyte, February 25, 2011.

412. David Barboza, "Chinese Man Who Bragged of Privilege Gets Six Years," *New York Times*, January 30, 2011. <http://www.nytimes.com/2011/01/31/world/asia/31china.html>. Keith Richburg, "Chinese Scandals Raise Public Ire," *Washington Post*, January 1, 2011.

413. Xiyun Yang and Edward Wong, "Suspicious Death Ignites Fury in China," *New York Times*, December 28, 2010.

414. Andrew Jacobs, "Chinese paper says whistleblowers are sent to mental wards," *New York Times*, November 8, 2008. <http://www.nytimes.com/2008/12/08/world/asia/08iht-china.1.18483551.html>.

415. Cui Jia, "Survey reveals Web of frustration," *China Daily*, March 4–6, 2011.

416. Wang Qian, "Ministries To Crack Down on Land Abuse," *China Daily*, February 18–20, 2011.

417. Wang Huazhong, "Former Official's Son Denied Govt Post," *China Daily*, December 27, 2010.

418. Edward Wong, "China: Cutting Frills From Junkets," *New York Times*, March 25, 2011.

419. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Yukon Huang, February 25, 2011.
420. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Yukon Huang, February 25, 2011.
421. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Yukon Huang, February 25, 2011.
422. Lu Hui, "China's railway minister under investigation over 'disciplinary violation'," *Xinhua*, February 12, 2011.
423. Yan Jie, "\$28 m misused in railway project," *China Daily*, March 24, 2011.
424. Simon Rabinovitch, "China applies brakes to high speed rail," *Financial Times*, August 10, 2011 <http://www.ft.com/intl/cms/s/0/ef91c278-c31b-11e0-9109-00144feabdc0.html#axzz1UdV3AHRb>.
425. Yan Jie, "Graft remains top public concern prior to annual parliamentary session: survey," *Xinhua*, February 24, 2011.
426. Wang Jingqiong, "Public irked over officials using get-out-of-jail cards," *China Daily*, May 17, 2011.
427. Yang Lina, "Former Shenzhen mayor given suspended death penalty for bribery," *Xinhua*, May 9, 2011.
428. Yan Jie, "Former China county boss receives suspended death sentence for bribery," *Xinhua*, April 7, 2011.
429. Wu Yiyao, "Land official does not object to charges," *China Daily*, February 2, 2011.
430. Bi Mingxin, "Former southwest China court chief sentenced on graft, gang crime charges," *Xinhua*, January 26, 2011.
431. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Yukon Huang, February 25, 2011.
432. Annalyn Censky, "Pork Prices Drive Chinese Inflation," *CNNMoney*, July 11, 2011. [http://money.cnn.com/2011/07/08/news/international/china\\_inflation\\_cpi/index.htm](http://money.cnn.com/2011/07/08/news/international/china_inflation_cpi/index.htm). *Trading Economics*, "China Inflation Rate." <http://www.tradingeconomics.com/china/inflation-cpi>.
433. Compiled by National Bureau of Statistics of China, *China Statistical Yearbook 2010*, "Table 10-5 Basic Conditions of Urban Households" (Beijing, China: China Statistics Press, October 2010). <http://www.stats.gov.cn/tjsj/ndsj/2010/html/J1005e.htm>.
434. United Nations Statistics Division Database, *Household Consumption Expenditure on Food*. [http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/EN/Content/Statistics/Internationales/InternationalStatistics/Topic/Tables/BasicData\\_HouseholdExpFood,templateId=renderPrint.psml](http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/EN/Content/Statistics/Internationales/InternationalStatistics/Topic/Tables/BasicData_HouseholdExpFood,templateId=renderPrint.psml).
435. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Murray Scot Tanner, February 25, 2011.
436. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Elizabeth Economy, February 25, 2011.
437. Joe McDonald, "Angry truckers in China protest rising costs," *Associated Press*, April 21, 2011.
438. Ronald Gribben, "China strikers win concessions, as ugly protests underline inflation fears," *Telegraph (United Kingdom)*, April 24, 2011.
439. Zhou Xin and Simon Rabinovitch, "China fines Unilever for talking about price rises," *Reuters*, May 6, 2011.
440. Li Woke, "P&G: Price hike 'last option,'" *China Daily*, May 11, 2011.
441. Paul Sonne and Laurie Burkitt, "China Fines Unilever for Price Comments," *Wall Street Journal*, May 7, 2011.
442. Li Woke, "P&G: Price hike 'last option,'" *China Daily*, May 11, 2011.
443. Jodi Xu, "China's Rising Food Prices Cause Pain," *TIME*, April 17, 2008.
444. Sun Yunlong, "China announces continuation of measures to ease inflation," *Xinhua*, January 25, 2008.
445. David Barboza, "Inflation Pressures Grow in China as Consumer Prices Increase 4.9%," *New York Times*, March 11, 2011.
446. Diana Choyleva, "The Real Picture of Chinese Inflation," *Wall Street Journal*, January 24, 2011.
447. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Yukon Huang and Steven Dunaway, February 25, 2011.
448. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, written testimony of Elizabeth Economy, February 25, 2011.
449. Nerys Aver, Sophie Leung, and Zheng Lifei, "China 'Over-Tightening' Concern to Limit Rate Moves as Reserve Ratio Rises," *Bloomberg*, May 13, 2011; Dexter Roberts, "Preparing for the (Possible) China Crash," *Bloomberg BusinessWeek*, July 18, 2011.



450. *Economist*, "China's Shadow-Banking System: Trust Belt," February 10, 2011.
451. Dinny McMahon, "Shadow Lending Hampers Beijing," *Wall Street Journal*, December 2, 2010.
452. Chen Jia, "Difference in incomes to resume widening trend," *China Daily*, April 20, 2011.
453. Sheng Laiyun, "National Economy Maintained Steady and Fast Growth in the First Quarter of 2011" (Beijing, China: National Bureau of Statistics of China, April 15, 2011).
454. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, Testimony of Yukon Huang, February 25, 2011.
455. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, Testimony of Yukon Huang, February 25, 2011.
456. Danielle Kurtzleben, "7 Ways the U.S. Population Is Changing," *U.S. News & World Report*, May 13, 2011.
457. Chen Jia, "Country's wealth divide past warning level," *China Daily*, May 12, 2010.
458. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Yukon Huang, February 25, 2011.
459. Bain & Company and China Merchants Bank, "Number of Chinese high net worth individuals nearly doubles since onset of global recession, according to far-reaching '2011 China Private Wealth Study' " (Boston, MA, and New York, NY: April 19, 2011). <http://www.bain.com/about/press/press-releases/number-of-chinese-high-net-worth-individuals.aspx>.
460. Didi Kirsten Tatlow, "Cost of Living Increasingly a Struggle for China's Poor," *New York Times*, December 9, 2010.
461. Andrew Peaple, "Shades of Gray in China's Income Levels," *Wall Street Journal*, August 11, 2010. <http://online.wsj.com/article/SB10001424052748704901104575422841352859712.html>.
462. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Martin Whyte, February 25, 2011.
463. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Martin Whyte, February 25, 2011.
464. Martin Whyte, "The Paradoxes of Rural-Urban Inequality in Contemporary China," in *One Country, Two Societies* (Cambridge, MA: Harvard University Press, 2010), p. 6.
465. Martin Whyte, "The Paradoxes of Rural-Urban Inequality in Contemporary China," in *One Country, Two Societies* (Cambridge, MA: Harvard University Press, 2010), p. 11.
466. Wu Jieh-min, "Rural Migrant Workers and China's Differential Citizenship: A Comparative Institutional Analysis," in Martin Whyte, *One Country, Two Societies* (Cambridge, MA: Harvard University Press, March 1, 2010), p. 56.
467. John Liu, "Beijing to Reduce Student Residence Permits," *Beijing Times Says*, Bloomberg News, May 17, 2011.
468. Shan Juan, "Census: Population hits 1.37b," *China Daily*, April 29, 2011.
469. Shan Juan, "One in three Beijingers a migrant worker," *China Daily*, May 6, 2011.
470. Wang Hongyi, "Migrants restore population base," *China Daily*, May 5, 2011.
471. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Elizabeth Economy, February 25, 2011.
472. Pang Qi, "Residence status influences students sitting national exams in Beijing," *Global Times (China)*, May 23, 2011.
473. Wang Wei, "School policy a boon for migrants' kids," *China Daily*, May 9, 2011.
474. Wang Wei, "School policy a boon for migrants' kids," *China Daily*, May 9, 2011.
475. Dester Roberts, "Preparing for the (Possible) China Crash," *Bloomberg BusinessWeek*, July 18, 2011.
476. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Yukon Huang, February 25, 2011.
477. Brian Spegele, "Chinese Police Quash Protest Over Land Rights," *Wall Street Journal*, March 31, 2011.
478. Tania Branigan, "Chinese newspapers in joint call to end curb on migrant workers," *Guardian (United Kingdom)*, March 1, 2010.
479. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Elizabeth Economy, February 25, 2011.
480. Sue Feng and Ian Johnson, "China Job Squeeze Sends 'Ants' to Fringes," *Wall Street Journal*, May 3, 2010.

481. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Martin Whyte, February 25, 2011; Andrew Jacobs, "China's Army of Graduates Struggles for Jobs," *New York Times*, December 11, 2010.
482. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Martin Whyte, February 25, 2011.
483. Ho Kwon Ping, "China's 'ant tribe' may sow seeds of unrest," *Straits Times (Singapore)*, March 16, 2011.
484. Cheng Li, "The Rise of the Middle Class in the Middle Kingdom," in *China's Emerging Middle Class* (Washington DC: The Brookings Institution, 2010), p. 18.
485. Cheng Li, "The Rise of the Middle Class in the Middle Kingdom," in *China's Emerging Middle Class* (Washington, DC: The Brookings Institution, 2010), p. 20.
486. Cheng Li, "The Rise of the Middle Class in the Middle Kingdom," in *China's Emerging Middle Class* (Washington, DC: The Brookings Institution, 2010), pp. 14–16.
487. Christa Case Bryant, "Surging middle classes eclipsing global poverty," *Christian Science Monitor*, May 17, 2011.
488. Xin Zhigang, "Dissecting China's Middle Class," *China Daily*, October 27, 2004. [http://chinadaily.com.cn/english/doc/2004-1027/content\\_386060.htm](http://chinadaily.com.cn/english/doc/2004-1027/content_386060.htm).
489. Li Shuang, "40 Percent of Beijingers Middle Class," *Global Times (China)*, August 11, 2011. <http://beijing.globaltimes.cn/society/2011-04/553384.html>
490. Yang Jing, "Stumbling on the Rocky Road: Understanding China's Middle Class," *International Journal of China Studies* 1: 2 (October 2010): 437.
491. Yang Jing, "Stumbling on the Rocky Road: Understanding China's Middle Class," *International Journal of China Studies* 1: 2 (October 2010): 437.
492. Bruce Dickson, "China's Cooperative Capitalists," in *China's Emerging Middle Class* (Washington, DC: The Brookings Institution, 2010), p. 292.
493. Martin Whyte (Harvard University sociologist), telephone interview with Commission staff, January 2011.
494. Martin Whyte and Guo Maocan, "How Angry Are Chinese Citizens about Current Inequalities? Evidence from A National Survey," in *Social Stratification in Chinese Societies* (Boston, MA: Brill Publishers, 2009), p. 17.
495. Andrew Jacobs, "Where 'Jasmine' Means Tea, Not a Revolt," *New York Times*, April 2, 2011.
496. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, written testimony of Elizabeth Economy, February 25, 2011.
497. Kenneth Lieberthal, "China's Emerging Middle Class: Beyond Economic Transformation" (Washington, DC: The Brookings Institution, December 14, 2010).
498. Laurie Burkitt and Jeremy Page, "China's Population is Aging Rapidly," *Wall Street Journal*, April 29, 2011. <http://www.online.wsj.com/article/SB10001424052748704187604576290031070463712.html>.
499. Laurie Burkitt and Jeremy Page, "China's Population is Aging Rapidly," *Wall Street Journal*, April 29, 2011. <http://www.online.wsj.com/article/SB10001424052748704187604576290031070463712.html>.
500. *Economist*, "Getting On: The Consequences of an Ageing Population," June 23, 2011. <http://www.economist.com/node/18832070>.
501. Willy Lam, "Beijing's 'Wei-Wen' Imperative Steals Thunder at NPC [National People's Congress]," *China Brief* (Washington, DC: The Jamestown Foundation, March 10, 2011).
502. Willy Lam, "Beijing's Blueprint for Tackling Mass Incidents and Social Management," (Washington, DC: The Jamestown Foundation, *China Brief*, March 25, 2011).
503. Jeremy Page, "Internal Security Tops Military in China Spending," *Wall Street Journal's China Real Time Report*, March 5, 2011.
504. Loretta Chao and Don Clark, "Cisco Poised to Help China Keep an Eye on Its Citizens," *Wall Street Journal*, July 5, 2011. <http://online.wsj.com/article/SB10001424052702304778304576377141077267316.html>.
505. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Murray Scot Tanner, February 25, 2011.
506. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Murray Scot Tanner, February 25, 2011.
507. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Murray Scot Tanner, February 25, 2011.
508. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Elizabeth Economy, February 25, 2011.
509. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, written testimony of Elizabeth Economy, February 25, 2011.

510. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, written testimony of Murray Scot Tanner, February 25, 2011.
511. Keith Richburg, "In China, Microblogging sites become free-speech platform," *Washington Post*, March 27, 2011.
512. Charles Chao, "Chinese microblogs growing faster than Twitter," *WantChina Times.com*, May 20, 2011.
513. U.S.-China Economic and Security Review Commission, *Hearing on China's Internal Dilemmas*, testimony of Murray Scot Tanner, February 25, 2011.
514. Andrew Jacobs, "As China steps Up Web Monitoring, Many Wi-Fi Users Stay Away," *New York Times*, July 26, 2011.
515. David Barboza, "Despite Restrictions, Twitterish Microblogs Are Booming in China," *New York Times*, May 16, 2011.
516. Andrew Jacobs, "As China steps Up Web Monitoring, Many Wi-Fi Users Stay Away," *New York Times*, July 26, 2011.
517. Agence France-Presse, "PRC's Plan to Send Chartered Jets to Cairo Bring Home 500 Stranded Chinese," January 31, 2011.
518. Christopher Bodeen, "Chinese newspaper attacks Middle East uprisings," *Associated Press*, March 6, 2011.
519. Tania Brannigan, "Crackdown in China spreads terror among dissidents," *Guardian (United Kingdom)*, March 31, 2011.
520. Andrew Quinn, "U.S. urges China to halt detention of activists," *Reuters*, March 8, 2011.
521. Keith Richburg, "In China, Microblogging sites become free-speech platform," *Washington Post*, March 27, 2011.
522. Sui-Lee Wee, Huang Yan, and Jonathan Standing, "U.S. envoy's name blocked in latest run-in with China," *Reuters*, February 25, 2011.
523. Sui-Lee Wee, "Ai Weiwei endured 'immense pressure' in detention: source," *Reuters*, August 10, 2011. [www.reuters.com/article/2011/08/10/us-china-artist-idUSTRE7793E620110810](http://www.reuters.com/article/2011/08/10/us-china-artist-idUSTRE7793E620110810).
524. Tania Branigan, "Ai Weiwei interrogated by Chinese police 'more than 50 times,'" *Guardian (United Kingdom)*, August 10, 2011. [www.guardian.co.uk/artanddesign/2011/aug/10/ai-weiwei-chinese-police](http://www.guardian.co.uk/artanddesign/2011/aug/10/ai-weiwei-chinese-police).
525. *Foreign Policy*, "Charter 08" (October 8, 2010).
526. Isaac Stone Fish and Duncan Hewitt, "All Eyes on the Prize," *Newsweek*, October 8, 2010.
527. Andrew Jacobs, "China, Angered by Peace Prize, Blocks Celebration," *New York Times*, October 9, 2010.
528. Brian Walker and Steven Jiang, "Chinese Nobel prize winner's wife detained," *CNN*, October 11, 2010.
529. Debbi Wilgoren, Keith B. Richburg, and Chris Richards, "Liu Xiaobo, jailed in China, honored in absentia by Nobel committee," *Washington Post*, December 10, 2010.
530. Sharon LaFraniere and David Barboza, "China Tightens Censorship of Electronic Communications," *New York Times*, March 21, 2011.
531. Keith B. Richburg, "Amid fears of unrest, China imposes new restrictions on foreign journalists," *Washington Post*, March 8, 2011.
532. U.S. State Department Daily Press Briefing, comments by Spokesman P.J. Crowley (Washington, DC: March 8, 2011).
533. Edward Wong, "China: Government Tells U.N. Agency Not To Interfere," *New York Times*, March 29, 2011.

## CHAPTER 2

### CHINA'S ACTIVITIES DIRECTLY AFFECTING U.S. SECURITY INTERESTS

#### SECTION 1: MILITARY AND SECURITY YEAR IN REVIEW

##### **Introduction**

This section provides an overview of the most relevant Chinese military and security developments since the Commission's *2010 Annual Report to Congress*. It is divided into three subsections: military developments, China's recent foreign policy activities, and updates on China's cyber activities. This year's military developments section describes progress in China's military modernization efforts, official statements from Beijing concerning its security interests, recent People's Liberation Army (PLA) activities, and the U.S.-China military-to-military relationship. China's foreign policy subsection focuses on China's assertive behavior in the South China Sea over the past year. The final subsection describes China's recent cyber activities, both at home and abroad.

##### **Military Developments in 2011**

Over the past year, several notable developments involving China's military have occurred. China's military modernization continued to progress, as evidenced by a series of firsts: China conducted test flights of its first stealth fighter, conducted a sea trial of its first aircraft carrier, and may have deployed the world's first ballistic missile capable of hitting moving ships at sea. China also conducted a major noncombatant evacuation of its citizens from Libya, the first involving the PLA. The past year also saw the resumption of military-to-military engagement between the United States and China, with three consecutive meetings between senior U.S. and Chinese military officials. The following subsection describes these events.

##### **Military Modernization**

###### ***J-20 stealth fighter***

In January 2011, China conducted the inaugural test flight of its next-generation fighter aircraft, the J-20. Although the flight attracted considerable attention in and outside of China, few details emerged about the fighter. Developed at the Chengdu Aircraft Design Institute, the plane appears to have a sufficient combat radius

to operate beyond China's borders and will likely have midair refueling capabilities.\* The fighter's other features, such as the speed and altitude at which it can travel, and its thrust capabilities and maneuverability, could not be determined by foreign observers of the test. Each of these capabilities depends on the J-20's engine, a component that the manufacturer may not yet have finally selected.<sup>1</sup> As described in the Commission's 2010 Report, turbofan engine development remains a persistent weakness in China's aviation industry,<sup>2</sup> which raises questions about the J-20's performance potential if it relies on domestic technology. The use of a Russian engine is one possibility to overcome any problems with an indigenous Chinese engine.† The U.S. Department of Defense (DoD) does not anticipate the J-20 to be operational prior to 2018.<sup>3</sup>

The J-20's design has led to considerable speculation about its stealth capability, or ability to evade radar detection. This capability consists primarily of the plane's configuration and design, as well as the materials and coatings it incorporates.‡ Aspects of the J-20's design, such as the forewings ("canards"), engine cover ("cowling"), jet and pelvic fin, and engine nozzles raise questions about whether it would successfully evade advanced radars.<sup>4</sup> In addition to design, the use of certain materials and coatings absorb radar signals, which can increase stealth. Pictures and video of the J-20 do not provide enough information to determine whether China's defense industries have mastered this aspect of advanced aircraft design. However, in late January 2011, Croatia's former military chief of staff stated that China had possibly received the stealth technology for the J-20 from parts of a U.S. F-117 stealth bomber shot down over Serbia in 1999.§

#### **U.S. Corporate Participation in China's Aviation Programs in 2011**

Several western aviation firms established or deepened ties to Chinese state-owned aviation firms in 2011. For example, General Electric (GE) Aviation and the state-owned Aviation Industry Corporation of China announced in January a joint venture

\*"Combat radius" refers to the distance a plane can travel to a mission area, execute a mission, and have adequate fuel to return to its base. Combat radius estimates for the J-20 range from 1,000 to 1,500 nautical miles. Carlo Kopp, "An Initial Assessment of China's J-20 Stealth Fighter," *China Brief* 11:8 (May 6, 2011): 9. [http://www.jamestown.org/uploads/media/cb\\_11\\_8\\_04.pdf](http://www.jamestown.org/uploads/media/cb_11_8_04.pdf).

†Two J-20 demonstrators may exist: one with a Chinese WS-10A engine and one with a Russian-made AL-F1FN engine. Notably, China has been unable to place the WS-10 series engine into serial production even several years after its development plans had been completed. As recently as last year, China requested advanced 117S engines from Russia. Tai Ming Cheung, "What the J-20 Says About China's Defense Sector," *Wall Street Journal*, January 13, 2011. <http://blogs.wsj.com/chinarealtime/2011/01/13/what-the-j-20-says-about-chinas-defense-sector/?mod=rss> WSJBlog&mod=chinablog.

‡This discussion includes passive design features but not active measures, such as electronic warfare, that might be used to evade radar detection.

§China's state-run newspaper, *Global Times*, referred to this claim as a "smear." BBC, "China stealth fighter 'copied parts from downed US jet'," January 24, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-12266973>; BBC, "China newspaper rejects J-20 stealth jet claim," January 25, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-12274807>. China also reportedly gained access to U.S. stealth materials from Pakistan following the downing of a U.S. stealth helicopter used for the raid on Osama Bin Laden's compound in May 2011, although the event took place after the J-20's maiden voyage. Reuters, "Pakistan let China see crashed U.S. 'stealth' copter," August 14, 2011. <http://www.reuters.com/article/2011/08/14/us-pakistan-china-usa-idUSTRE77D2BT20110814>.



**U.S. Corporate Participation in China's Aviation Programs in 2011—*Continued***

for integrated avionics, which, according to a GE press release, will transfer ownership of GE's existing civilian avionics operations to the joint venture and be "the single route-to-market for integrated avionics systems for both GE and AVIC [Aviation Industry Corporation of China]." The press release further describes the deal, stating that "the new AVIC [Aviation Industry Corporation of China] and GE joint venture company will develop and market integrated, open architecture avionics systems to the global commercial aerospace industry for new aircraft platforms. This system will be the central information system and backbone of the airplane's networks and electronics and will host the airplane's avionics, maintenance, and utility functions."<sup>5</sup> Notably, GE characterized the joint venture's work in China as research and development "to come up with breakthrough technologies and create 'new IP [intellectual property] and new technology'." In describing the Aviation Industry Corporation of China, the press release also noted that "[t]he company has also developed strong capabilities to supply avionics products to various models of aircrafts, both for military and civil use."<sup>6</sup> Of import, because GE is also providing the engines for the C919, through a joint venture with the French firm Snecma (Safran Group),<sup>7</sup> improving the C919's avionics will make it more marketable, which will in turn allow GE to sell more engines. It is worth noting that as a Commission-sponsored report details, both engine development and avionics are areas where China's aviation industry continues to have problems and currently must rely on foreign imports.<sup>8</sup>

Boeing also undertook several new projects with the Aviation Industry Corporation of China in 2011. In June, the firms announced the creation of a new Manufacturing Innovation Center in Xi'an, which would, among other things, "support AVIC's [Aviation Industry Corporation of China] goals of improving its manufacturing and technological capabilities and the competitiveness of its affiliated factories to achieve global Tier-1 supplier status."<sup>9</sup> In addition, Boeing announced in April that it planned to double the capacity of a joint venture with the Aviation Industry Corporation of China, called Boeing Tianjin, which produces composites.<sup>10</sup> One of the joint venture's customers is the Xi'an Aviation Industry Corporation,<sup>11</sup> which manufactures components for civil aircraft and produces military aircraft, such as the JH-7A fighter bomber and the H-6 bomber, for the PLA.<sup>12</sup>

***Aircraft carrier program***

In July 2011, China officially revealed its long-suspected aircraft carrier program when it publicly announced that it was developing an aircraft carrier.<sup>13</sup> A month later, China conducted a sea trial of its first aircraft carrier off the port of Dalian.<sup>14</sup> Not an indigenously developed vessel, China's aircraft carrier is a renovated Soviet *Kuznetsov*-class carrier (the *Varyag*) purchased from Ukraine in 1998. At the time of its purchase, a Hong Kong company, with al-



leged ties to the Chinese government and the PLA, purchased the carrier without engines, rudders, or weapons, ostensibly for use as a floating casino off the island of Macau.<sup>15</sup> After several years of setbacks, in 2002 the *Varyag* finally arrived at the Chinese port of Dalian, its current homeport.\*<sup>16</sup> Although it is unclear when the PLA officially gained control over the vessel, China has been working since 2004 to make the carrier operational. After the sea trial, the *Varyag* returned to Dalian for further work.<sup>17</sup> According to unnamed PLA sources, the carrier will not be launched officially until October 2012.<sup>18</sup> Unconfirmed rumors also posit that China is constructing one or more indigenous carriers for a future aircraft carrier fleet.<sup>19</sup> China is also developing the aircraft to be deployed along with the aircraft carriers. In April 2011, Internet photos revealed a test version of a carrier-based fighter, the J-15.<sup>20</sup> According to analysts, this aircraft appears to be a modified version of China's J-11B fighter, which in itself is an unlicensed adaptation of Russia's SU-27 Flanker. The J-15 is not expected to be deployed before 2016.<sup>21</sup> The PLA Navy is also developing the means to train future pilots in the dangerous task of taking off from and landing on an aircraft carrier. In June 2011, China's Guizhou Aviation Industry conducted the test flight of an advanced trainer aircraft, the JT-9 (also referred to as the JL-9H).<sup>22</sup> China has also constructed at least two land-based pilot training centers to teach PLA Navy pilots how to land on an aircraft carrier. Both centers have ski-jump platforms that mimic the shape of the *Varyag*'s deck.<sup>†</sup><sup>23</sup>

The People's Republic of China's (PRC) official position about the use of its aircraft carrier is that it will be used for "scientific research, experiment and training."<sup>24</sup> This corresponds with the U.S. Department of Defense's view, which maintains that China's first aircraft carrier "will likely serve initially as a training and evaluation platform and eventually offer a limited operational capability."<sup>25</sup> However, a Chinese Ministry of Defense spokesman noted in July 2011 that a carrier could be used for offensive or defensive purposes as well as for disaster relief and that China was pursuing its carrier program "in order to increase its ability to protect national security and world peace."<sup>26</sup> Another article in China's official press says that aircraft carriers are vital to China given China's "vast territorial waters" and the current inability of the PLA Navy to safeguard this region. The article also points out China's need to safeguard its global interests and protect the sea lanes upon which China's continued economic development rests.<sup>27</sup>

China's aircraft carrier development program currently poses little direct threat to the United States and is likely more of a concern to regional maritime states. In testimony to the U.S. Senate, Robert F. Willard, commander of the U.S. Pacific Forces, stated

\* Because the *Varyag* lacked engines and rudders, Turkish authorities were reluctant to allow it to be towed through the Bosphorus Strait, for fear of damaging the narrower portions of the strait. Ian Story and You Ji, "China's Aircraft Carrier Ambitions: Seeking Truth from Rumors," *Naval War College Review* LVII: 1 (Winter 2004): 83.

† Given the small flight deck of carriers compared to land-based runways, aircraft rely upon two means for successfully lifting off from an aircraft carrier. Conventional aircraft carriers, such as U.S. carriers, have a catapult system that assists the aircraft in reaching the requisite speed prior to take-off. Another method is to install a slight ramp on the end of the deck, referred to as a "ski-jump," that propels the aircraft up and out as it exits the ship's deck. China's *Varyag* aircraft carrier has a ski-jump type deck. Michael Wines, "Chinese State Media, in a Show of Openness, Print Jet Photos," *New York Times*, April 25, 2011. <http://www.nytimes.com/2011/04/26/world/asia/26fighter.html>.

that he was not concerned about the military impact of the carrier. However, Admiral Willard did note that it could have an impact on perceptions of China in the region.<sup>28</sup> When the *Varyag* is deployed, it will make China one of only ten countries that operate aircraft carriers, none of which are countries with which China has maritime disputes.\* Possession of an aircraft carrier would allow China to project force throughout the region, especially into the far reaches of the South China Sea, something it currently cannot fully do. Possibly in an attempt to temper regional fears of China's aircraft program, China's state-run news outlet Xinhua wrote, "[t]here should be no excessive worries or paranoid feelings on China's pursuit of an aircraft carrier, as it will not pose a threat to other countries, and other countries should accept and be used to the reality that we are developing the carrier."<sup>29</sup>

Given the complexity of conducting carrier operations, it is expected to be several years before China's aircraft carrier will be fully operational.<sup>30</sup> According to Michael McDevitt, a retired rear admiral in the U.S. Navy, the PLA Navy will face a number of challenges in the coming years integrating carrier and air wing operations.<sup>31</sup> Additionally, as defense analysts Nan Li and Christopher Weuve noted, "An aircraft carrier is not a solo-deploying ship. To be survivable in an intense combat environment, it needs escorts to protect it."<sup>32</sup> China has taken steps to develop such support systems, but their capabilities are uneven. For example, according to the same analysis, "While China has acquired new surface combatants with sophisticated antisurface and antiair capabilities, it continues to lag behind in the area of ASW [anti-submarine warfare]," which could seriously challenge carrier operations in certain scenarios.<sup>33</sup>

### ***The DF-21D antiship ballistic missile***

Over the past year, several developments concerning China's antiship ballistic missile, the DF-21D, have occurred. In December 2010, Admiral Willard described in the following exchange with a reporter how the DF-21D was possibly operational:

*Reporter: Let me go into China's anti-access/area denial (A2/AD) capabilities. What is the current status of China's anti-ship ballistic missile development, and how close is it to actual operational deployment?*

*Admiral Willard: The anti-ship ballistic missile system in China has undergone extensive testing. An analogy using a Western term would be 'initial operational capability,' whereby it has—I think China would perceive that it has—an operational capability now, but they continue to develop it. It will continue to undergo testing, I would imagine, for several more years.*

*Reporter: China has achieved IOC [initial operational capability]?*

---

\*The other nine countries currently possessing aircraft carriers are Brazil, France, India, Italy, Russia, Spain, Thailand, the United Kingdom, and the United States. China currently has maritime disputes in the East China Sea with Japan, and in the South China Sea with Brunei, the Philippines, Malaysia, Taiwan, and Vietnam.

*Admiral Willard: You would have to ask China that, but as we see the development of the system, their acknowledging the system in open press reporting and the continued testing of the system, I would gauge it as about the equivalent of a U.S. system that has achieved IOC [initial operational capability].*<sup>34</sup>

In July 2011, Chinese sources officially confirmed the development of the DF-21D for the first time. In an article in China's state-controlled *China Daily* newspaper, PLA Major General Chen Bingde, chief of the General Staff, acknowledged that the PLA is developing the DF-21D. However, Major General Chen dismissed the notion that the missile is currently operational, stating that the DF-21D "is still undergoing experimental testing" and that "it is a high-tech weapon and we face many difficulties in getting funding, advanced technologies and high-quality personnel, which are all underlying reasons why it is hard to develop this." The *China Daily* article further noted that the DF-21D is "a ballistic missile with a maximum range of 2,700 kilometers (km) and the ability to strike moving targets—including aircraft carriers—at sea."<sup>35</sup> Of import, the stated range of this missile is significantly greater than the DOD's estimate of "exceeding 1,500 km."<sup>36</sup> It is unclear what accounts for this discrepancy, although in response to a Commission question, the DoD attributed the differences in stated ranges to possible erroneous reporting by the Chinese press and remained "confident" about the department's original assessment.<sup>37</sup> (For more on the DF-21D and how it could play an integral part in China's efforts to deny U.S. military forces the ability to operate freely in the western Pacific, see chap. 2, sec. 2, of this Report.)

## **Official Statements**

### ***2011 defense budget***

In March 2011, China officially released its defense budget for the year. According to Chinese sources, China's defense budget for 2011 is \$91.5 billion, a 12.7 percent increase over 2010.<sup>38</sup> This represents the 20th increase in as many years. According to the DoD, between 2000 and 2010 "China's officially disclosed military budget grew at an average of 12.1 percent in inflation-adjusted terms," a percentage value that the DoD also notes tracks closely with the growth in China's gross domestic product for the same period.<sup>39</sup> However, western analysts readily discount Chinese figures for its defense budget as inaccurate. Because these statistics do not take into account all defense expenditures, the likely figure is much higher.<sup>40</sup> In testimony to the Commission, Mark Stokes, a former lieutenant colonel in the U.S. Air Force and current executive director of the Project 2049 Institute, stated, "While the PLA deserves credit for greater transparency, key areas of defense expenditure, such as research and development, remain opaque."<sup>41</sup> China's official defense budget also does not include foreign procurement.<sup>42</sup> Abraham Denmark, then fellow at the Center for New American Security, testified to the Commission that "given China's practice of significantly under-reporting defense expenditures, it is safe to estimate China's actual annual spending on its military power to be well over \$150 billion."<sup>43</sup> In its 2011 report to Con-

gress, the DoD noted that China's 2010 defense budget was likely about twice what Beijing reported, at over \$160 billion.<sup>44</sup>

***China's 2011 defense white paper***

On March 31, 2011, China released its seventh biannual defense white paper, *China's National Defense in 2010*, an authoritative statement of Beijing's views of China's security environment. This report posits a relatively optimistic picture, noting that "China is still in the period of important strategic opportunities for its development, and the overall security environment for it remains favorable." However, the paper lists several areas that Beijing views as a potential threat to China's stability and security: Taiwan, independence movements in China's Tibet and Xinjiang provinces, China's disputed maritime claims, nontraditional security concerns,\* and growing opposition to China stemming from China's rise. Of import, the white paper singles out the United States (the only nation mentioned by name) in the section on "threats and challenges" because of U.S. arms sales to Taiwan.<sup>45</sup>

As an important piece of China's strategic messaging, the primary audience for China's defense white papers is foreign actors.<sup>46</sup> This iteration in particular appears to be an attempt to allay fears of China's growing military capabilities in the region.<sup>47</sup> According to the Congressional Research Service, "The overall purpose of the defense white paper seems to be to counter what Beijing calls the 'China Threat Theory' and to affirm that the PRC remains a peaceful power pursuing 'Peaceful Development' with a military that is 'defensive in nature.'" <sup>48</sup> CNA China Studies Center, a Washington, DC-based, research institute, described how:

*The main message of the 2010 edition for external audiences is one of reassurance. The message being conveyed ... is that Beijing has not changed its defensive military posture despite its growing military capabilities and its various extraterritorial military deployments. ... These messages of assurance come on the heels of a period of about two years during which Chinese foreign policy and security policy initiatives were described by foreign observers as 'assertive' or uncharacteristically muscular. Consequently, one likely objective of this paper is to calm the waters, especially in the Asia-Pacific region.*<sup>49</sup>

Despite the stated goal of providing more transparency on China's military modernization efforts and intentions, the defense white paper falls short.<sup>50</sup> Phillip C. Saunders, director of studies at the Center for Strategic Research at the U.S. National Defense University, asserted that the 2010 white paper is less transparent than previous iterations.<sup>51</sup> The report provides few new details, leaving many critical questions unanswered.<sup>52</sup> For example, Shirley A. Kan, an Asian Defense Security analyst at the Congressional Research Service, noted that China's 2010 defense white paper provided:

---

\*The defense white paper lists the following nontraditional security concerns: terrorism, energy resources, financial problems, information security, and natural disasters. Information Office of the State Council, *China's National Defense in 2010* (Beijing, China: March 2011).

*no details on satellites, anti-satellite (ASAT) weapons, space program, aircraft carriers, ships, strategic and other submarines, fighters including the J-20 fighter that was flight tested during Defense Secretary Robert Gates' visit in January 2011, aerial refueling for operations far from China, new nuclear-armed intercontinental ballistic missiles, anti-ship ballistic missiles, land attack cruise missiles, or short-range ballistic missiles threatening Taiwan.*<sup>53</sup>

## **Military Operations**

### ***Antipiracy operations off the Horn of Africa***

In July 2011, the PLA Navy dispatched its ninth task force to conduct escort missions through the pirate-infested waters of the Gulf of Aden.<sup>54</sup> As the Commission noted in its 2009 report, since January 2009, the PLA Navy has assisted United Nations (UN) antipiracy operations around the Horn of Africa.<sup>55</sup> The PLA Navy's current task force consists of a destroyer, a frigate, a replenishment ship, and a small contingent of marines. According to Chinese statistics, to date the task forces have escorted approximately 4,000 Chinese and foreign-flagged cargo vessels in the region.<sup>56</sup> Since early 2010, the task forces have conducted regular monthly port calls for replenishment and overhaul, stopping mainly at three locations: Port of Salalah (Oman), Port of Djibouti (Djibouti), and Port of Aden (Yemen). PLA Navy ships from the task forces have also conducted at least 19 friendly port calls during their deployment in support of the China's military diplomacy efforts. During five of these port visits, the PLA Navy conducted joint maritime drills with the host nation's naval forces.\*<sup>57</sup>

The PLA Navy, similar to vessels from Russia, India, and Japan, primarily conducts antipiracy escort missions of civilian cargo vessels and does not participate in regional counterpiracy operations.† However, the PLA Navy does coordinate its antipiracy activities with the main counterpiracy task force, Combined Task Force 151, through a separate, monthly gathering called Shared Awareness and Deconfliction. China has even expressed an interest in assuming the chairmanship of this latter institution.<sup>58</sup> During a May 2011 visit to the United States, Major General Chen opened the door for the possible participation of Chinese forces in counterpiracy operations, stating that “for counterpiracy campaigns to be effective, we should probably move beyond the ocean and crash their bases on the land.”<sup>59</sup>

### ***Evacuation of Chinese civilians from Libya, February–March 2011***

During the fighting between pro-Qadaffi and anti-Qadaffi forces in Libya in February and March 2011, the Chinese government conducted what it considers to be its “largest and the most complicated overseas evacuation ever” and the first involving the

\*The maritime drills were conducted with the navies of Italy, Pakistan (twice), Singapore, and Tanzania. Open Source Center, “OSC Interactive Map: Chinese PLA Navy Escort Mission Port Calls,” *OSC Summary* (May 2, 2011). OSC ID: FEA20110503017394. <http://www.opensource.gov>.

†Counterpiracy operations are operations that seek actively to suppress piracy, as opposed to antipiracy operations, which are operations to prevent and deter piracy.



PLA.<sup>60</sup> Prior to the conflict, China had approximately 36,000 citizens working in Libya for 75 Chinese companies. As the fighting intensified, China's citizens and company facilities increasingly came under attack.<sup>61</sup> In an effort to ensure their safety, the Chinese government organized a complex evacuation operation that, according to the Chinese Ministry of Foreign Affairs, involved "91 domestic chartered flights, 12 flights by military airplanes, five cargo ferries, one escort ship, as well as 35 rented foreign chartered flights, 11 voyages by foreign passenger liners and some 100 bus runs." After eight days, "all Chinese in Libya who desired to go back and whose whereabouts were known by the foreign ministry—35,860 in number, had been evacuated."<sup>62</sup>

This was the first noncombatant evacuation operation from an active combat zone in which the PLA participated. On February 24, the PLA Navy dispatched the guided missile frigate *Xuzhou*, then participating in antipiracy operations off the Horn of Africa, to assist in the evacuation efforts. Arriving in the Mediterranean, the frigate began escorting chartered civilian ships evacuating Chinese citizens to Greece.<sup>63</sup> In another first, the PLA Air Force also dispatched four IL-76 transport aircraft to assist in the evacuation process. These aircraft, dispatched from China's westernmost province, Xinjiang, on February 28, began evacuating people to Khartoum, Sudan, the next day. According to Chinese reports, the aircraft flew over Pakistan, Oman, Saudi Arabia, and Sudan before landing in Sabha, Libya. During the flight to Libya, the aircraft refueled twice, in Karachi, Pakistan, and Khartoum, Sudan.<sup>64</sup>

## **U.S.-China Military-to-Military Relations**

### ***Secretary of Defense Robert F. Gates' visit to China***

On January 9–12, 2011, then U.S. Secretary of Defense Robert F. Gates visited China, marking the resumption of U.S.-China military-to-military relations that China cut off following the Obama Administration's January 2010 notification to Congress about potential U.S. arms sales to Taiwan. During his visit, Secretary Gates met with Chinese Minister of Defense General Liang Guanglie and General Secretary of the Chinese Communist Party (CCP) and President Hu Jintao and visited the headquarters of the Second Artillery (the PLA's strategic rocket forces). Over the course of the trip, the leaders discussed tensions on the Korean Peninsula, nuclear strategy, and the possible development of joint military exercises in maritime search and rescue, humanitarian assistance, disaster relief, counterpiracy, and counterterrorism, among other things.<sup>65</sup>

The stated goal of Secretary Gates' trip was to initiate a regular, bilateral defense dialogue over contentious issues like nuclear policy, missile defense, cybersecurity, and space security in order to avoid future miscommunication and miscalculation.<sup>66</sup> Observers perceived that this goal was only partially achieved, as General Liang declined to put forth a timetable for such talks, only agreeing that defense exchanges between the two countries would occur in the first half of 2011 and that the PLA was "studying" the proposal for a regular dialogue.<sup>67</sup> After the trip, Secretary Gates stated that he was satisfied with the overall visit, saying that "this is



not an area where you will see dramatic breakthroughs and new headlines, but rather evolutionary growth.”<sup>68</sup>

The unexpected highlight of the trip was the test flight of China’s new J-20 stealth fighter aircraft, which took place hours before Secretary Gates’ meeting with President Hu. When Secretary Gates inquired about the test flight, President Hu claimed to be unaware that it had occurred.<sup>69</sup> A Chinese defense ministry deputy director stated that the test was part of a “normal working schedule” and that it was not related to Secretary Gates’ visit.<sup>70</sup> According to the Commission testimonies of Andrew Scobell, senior political scientist at the RAND Corporation, and Mr. Denmark, it is inconclusive whether or not the test was planned to occur because of the visit.<sup>71</sup> The “surprise” test flight raised concerns that the PLA might be acting independently of China’s civilian leaders. In a speech in Tokyo following his trip to China, Secretary Gates noted that “[o]ver the last several years we have seen some signs of ... a disconnect between the military and the civilian leadership [in China].” He added that he was confident that President Hu and the CCP remained fully in control of the military.<sup>72</sup> Dr. Scobell, however, opined that “[f]undamentally, the J-20 episode underscores the fact that civilian control of the military is underinstitutionalized in 21st Century China.”<sup>73</sup>

#### ***PLA Chief of Staff Chen Bingde’s visit to the United States***

China’s pledge to enhance military-to-military exchanges in 2011 was upheld in May when the PLA Chief of General Staff, Major General Chen Bingde, visited the United States. During his trip, Major General Chen toured four military bases;\* delivered a speech at the U.S. National Defense University; and held talks with Secretary Gates, Secretary of State Hillary Rodham Clinton, and Admiral Mike Mullen, then chairman of the Joint Chiefs of Staff. He and his delegation also attended a goodwill concert featuring performances of the official bands of the U.S. Army and the PLA.<sup>74</sup>

A joint statement presented by Admiral Mullen and Major General Chen outlined six bilateral agreements reached from the visit: (1) a consensus that the two sides would work together within the framework agreed by President Hu and President Barack Obama; (2) the establishment of a direct telephone line between the Chinese Ministry of Defense and the U.S. Department of Defense; (3) plans to conduct joint naval exercises in the Gulf of Aden as part of the international antipiracy effort; (4) plans to conduct a humanitarian disaster rescue and relief joint training exercise in 2012; (5) an agreement to exchange medical information and conduct joint medical rescue training exercises; and (6) an invitation from China for the U.S. Army Band and shooting team to visit China.<sup>75</sup>

Although the two sides were able to reach several points of consensus, a number of differences were highlighted. During a press conference, General Chen commented on China’s opposition to sev-

\*General Chen toured Naval Station Norfolk, Virginia; Fort Stewart, Georgia; Nellis Air Force Base, Nevada; and the National Training Center at Fort Irwin, California. Agence France-Presse, “U.S. Rolls Out Red Carpet for China Military Chief,” May 14, 2011. <http://www.defensenews.com/story.php?i=6502345>.

eral U.S. military policies, including arms sales to Taiwan, reconnaissance activities along Chinese coasts by U.S. military aircraft and vessels, and restrictions on U.S. exports of high technologies to China.<sup>76</sup> Of note, some U.S. observers, including Members of Congress, were critical of Major General Chen's visit to U.S. military bases, saying those visits might violate the *2000 National Defense Authorization Act*, which bans Chinese military visitors to the United States from "inappropriate exposure" to information that could be used to enhance the PLA's capacity to conduct combat operations.<sup>77</sup>

#### ***Admiral Mullen's visit to China***

Admiral Mullen reciprocated Major General Chen's visit in July 2011. Admiral Mullen and his 39-person delegation visited Beijing as well as Shandong and Zhejiang provinces, where they met with a number of high-level government and military officials, including Vice President (and likely future President and Party Secretary) Xi Jinping. On the trip, Admiral Mullen visited units in the army, navy, air force, and the Second Artillery (strategic rocket forces) and was introduced to several pieces of Chinese military technology, including the Su-27, one of China's most advanced operational fighter jets, and a Type-39A *Yuan*-class diesel-electric submarine.<sup>78</sup> At a joint press conference, Admiral Mullen and Major General Chen announced plans to hold antipiracy maneuvers in the Gulf of Aden by year's end, to hold talks on operational safety in Hawaii and China, and to plan joint humanitarian relief exercises in 2012.<sup>79</sup>

Some divisive issues punctuated the visit. During a press conference, General Chen three times criticized recent joint naval exercises between the United States, Australia, and Japan in the South China Sea. He also raised complaints over controversial non-military issues such as the attitudes of some American politicians toward China and a U.S. visit by the Dalai Lama.<sup>80</sup> Admiral Mullen expressed concern over North Korea's recent provocative comments and actions and encouraged Beijing to use its strong ties with Pyongyang to ensure stability on the Korean Peninsula.<sup>81</sup>

#### **Implications for the United States**

As demonstrated above, China has progressed substantially over the past year in its military modernization efforts. These developments show that China is attempting to increase its ability to project power in the region. Developments in China's stealth fighter, aircraft carrier and carrier aircraft, and antiship ballistic missile programs, when completed, will provide the PLA with an increased capacity to exert control over the western Pacific and threaten regional states and U.S. forces operating within the region in the event of a conflict. These developments also embolden China and the PLA in its interactions with other nations, as evidenced during recent U.S.-China military-to-military dialogues.

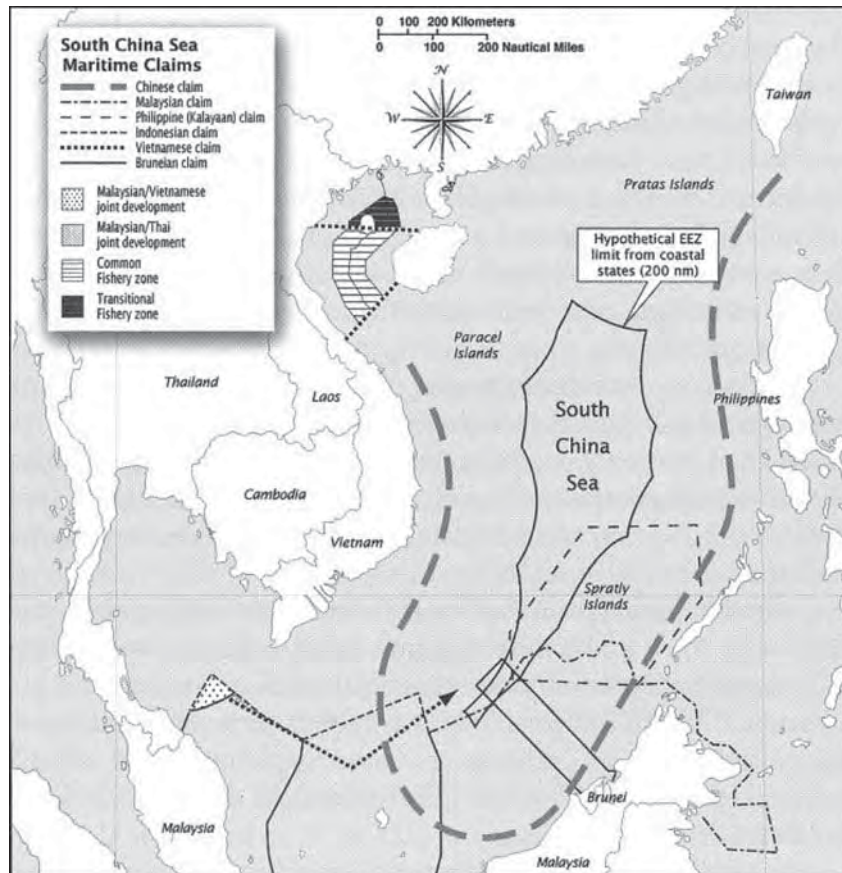
**Recent Chinese Assertiveness in the South China Sea**

Tension between China and other claimants in the South China Sea territorial disputes [see figure 1, below] has waxed and waned in recent years, with periods of confrontation and intimidation followed by attempts at reconciliation and confidence building.\* China displayed increasing territorial aggression in the spring and summer months of 2011. In June, Ian Storey, fellow at the Institute for Southeast Asian Studies in Singapore, noted that tensions in the disputed seas were at their highest levels since the end of the Cold War.<sup>82</sup> Notwithstanding China's intermittent displays of cooperation, China's expanding military, commercial, and rhetorical assertiveness in the South China Sea indicates that China is unlikely to concede any of its sovereignty claims in the area.<sup>83</sup> Expert witnesses testified to the Commission that China's patterns of assertiveness in the South China Sea call into question its "peaceful rise" as well as its long-term views toward its regional neighbors and the United States.<sup>84</sup>

---

\* Brunei, China, Malaysia, the Philippines, Taiwan, and Vietnam are claimants in maritime disputes in the South China Sea. For information on developments in the South China Sea in 2009 and 2010, see U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2010), pp. 132–137.

Figure 1: Territorial Disputes in the South China Sea



Source: James Clad, Sean M. McDonald, and Bruce Vaughn, eds., *The Borderlands of South-east Asia* (Washington, DC: National Defense University, 2011), p. 121. Note: Indonesia does not consider itself a claimant to any dispute in the South China Sea, even though its territorial claims in the region overlap with China's. Permanent Mission of the Republic of Indonesia to the United Nations, Circular Note No. 480/POL-703/VII/10, July 8, 2010. [http://www.un.org/Depts/los/clcs\\_new/submissions\\_files/mysvnm33\\_09/idn\\_2010re\\_mys\\_vnm\\_e.pdf](http://www.un.org/Depts/los/clcs_new/submissions_files/mysvnm33_09/idn_2010re_mys_vnm_e.pdf).

The following are examples of China's assertiveness in the South China Sea in the past year:

*Obstruction of resource exploration activities*—Chinese vessels obstructed resource exploration activities in the claimed territories of other countries at least three times in the first half of 2011. Each of these instances may constitute a violation of the United Nations Convention on the Law of the Sea, which allows any country sovereign rights to conduct economic or resource management activities in an exclusive economic zone (EEZ) up to 200 nautical miles from its shores and to which China is a signatory.<sup>†</sup> In March 2011,

<sup>†</sup> An exclusive economic zone is the maritime territory of a coastal state out to 200 nautical miles, where the coastal state enjoys "sovereign rights for the purpose of exploring and exploit-

Continued

two Chinese patrol boats aggressively approached and chased away a seismic survey vessel conducting an assessment of a gas field in the Philippines' EEZ near the disputed Spratly Islands. The vessel, chartered by the British energy consortium Forum Energy, was conducting work on behalf of the Philippine government.<sup>85</sup> The incident prompted harsh responses from the Philippines in the following months. Philippine President Benigno Aquino III announced plans to take the dispute over the Spratly Islands to the United Nations International Tribunal on the Law of the Sea.<sup>86</sup> He also vowed to bolster the Philippines' military power in order to protect its economic interests in the face of growing Chinese assertiveness. In June, the Philippines announced a \$252 million upgrade for its navy and deployed its largest warship to patrol the South China Sea.<sup>87</sup> In September, the Philippines allocated an additional \$118 million for the purchase of a navy patrol vessel, six helicopters, and other hardware to secure the perimeter of the country's largest gas extraction project, which is located 50 miles from a Philippine island near waters claimed by China.<sup>88</sup> President Aquino also called on the United States, a treaty partner, to help the Philippines stand up to the Chinese.<sup>89</sup>

Vietnamese officials reported that Chinese boats harassed Vietnamese oil and gas surveying ships operating in the South China Sea on two separate occasions in 2011. In the first incident, which occurred in late May, state oil company PetroVietnam alleged that while it was conducting seismic operations, Chinese airplanes harassed the company's ships, and three Chinese marine surveillance vessels subsequently cut the company's survey cables.<sup>90</sup> The second incident occurred in June and involved a Chinese patrol boat cutting the cable of a Vietnamese oil-drilling research vessel.<sup>91</sup> Both incidents occurred in Vietnam's EEZ, less than 200 nautical miles from the Vietnamese coast, and the second of the incidents occurred more than 600 nautical miles from China's island province of Hainan.<sup>92</sup> In previous years, Chinese patrol boats typically only harassed fishermen, not oil and gas vessels.<sup>93</sup>

*Deep sea oil rig stationed in the South China Sea*—China has built an advanced, deep-water oil rig that it plans to use in the South China Sea. Launched in the summer of 2011, the \$1 billion oil rig, owned by the Chinese state-owned oil company China National Offshore Oil Corporation, is China's first deep-water drilling rig and allows China to drill in deeper waters than ever before.<sup>94</sup> The exact location of the rig was unclear at the time of the publication of this Report. The Philippines has expressed concern and has asked China's embassy to clarify the exact location of the planned rig.<sup>95</sup>

*Harassment of Vietnamese and Philippine fishermen*—Vietnamese and Philippine fishermen reported an uptick in harassment by Chinese maritime patrol boats in early 2011, including the threatening of fishermen and the seizure and confiscation of fish

---

ing, conserving and managing the natural resources, whether living or non-living, of the waters superjacent to the sea-bed and of the sea-bed and its subsoil, and with regard to other activities for the economic exploitation and exploration of the zone, such as the production of energy from the water, currents and winds." United Nations, "Exclusive Economic Zones," *United Nations Convention on the Law of the Sea* (New York, New York: December 10, 1982). [http://www.un.org/Depts/los/convention\\_agreements/texts/unclos/part5.htm](http://www.un.org/Depts/los/convention_agreements/texts/unclos/part5.htm).



and equipment from “dozens” of Vietnamese vessels.<sup>96</sup> The increase in harassment coincided with China’s annual unilateral fishing ban in sections of the South China Sea, parts of which are disputed by Vietnam.<sup>97</sup> In June, four Vietnamese fishing boats in waters outside the disputed Spratly Islands reported that Chinese naval ships fired shots into the water near the fishermen’s boats and chased them away.<sup>98</sup> In July, a Chinese vessel threatened a Vietnamese fishing boat near the disputed Paracel Islands. The Vietnamese fishermen reported that ten armed Chinese “soldiers” boarded their boat, punched and kicked the captain, and confiscated one ton of fish.<sup>99</sup> These displays of aggression toward fishermen, as well as the cable cutting, fueled unrest in Vietnam and spurred weekend protests against China in Vietnamese cities throughout the summer.<sup>100</sup> Chinese vessels also harassed Philippine fishermen, despite the fact that claimed Philippine waters are not within the jurisdiction of China’s fishing ban. The authorities in Manila claimed that from February to June 2011, Chinese ships had entered into disputed Philippine territory and harassed local fishermen nine times.<sup>101</sup>

*Deployment of patrol ships in the South China Sea*—China’s increased assertiveness in disputed waters is attributable in part to a strategic increase in maritime patrols in regions considered especially important or sensitive to China. Responsibility for maritime patrolling is shared by five state agencies and several regional governments.<sup>102</sup> One of these agencies, China’s Bureau of Fisheries, announced in December 2010 that China would strengthen fisheries management in “sensitive” waters, including the South China Sea.<sup>103</sup> This pledge was put into practice in September 2011 when an additional fisheries patrol ship was sent to waters around the disputed Paracel Islands in order to “strengthen fishery administration in the waters around Xisha [the Paracel Islands], ensure fishery production order and safety of fishermen, and protect China’s sea sovereignty and fishery interest,” according to an Agriculture Ministry official.<sup>104</sup>

In June, another agency, China’s State Oceanic Administration, announced that China’s regular maritime surveillance would be strengthened in China’s claimed maritime areas in the South China Sea.<sup>105</sup> China Marine Surveillance, which is the main maritime patrolling body under the State Oceanic Administration, plans to significantly increase personnel and patrol vessels and vehicles in the period during the 12th Five-Year Plan (2011–2015).<sup>106</sup> According to Li Mingjiang, assistant professor at S. Rajaratnam School of International Studies in Singapore, this expansion will enable China Marine Surveillance to conduct daily patrols in areas where it currently has the capacity for only one or two patrols each month.<sup>107</sup>

Also in June, the Chinese Maritime Safety Administration ship *Haixun-31* arrived in Singapore on what was noted in the press to be both a goodwill visit and a demonstration of China’s “national rights and sovereignty” in the South China Sea.<sup>108</sup> Singapore does not claim any part of the disputed South China Sea, but one day after *Haixun-31* made its port call, the Singaporean Defense Ministry called on China to clarify its claims in the South China Sea,



saying that ambiguity over China's claimed territory was causing "serious concerns" in the international community.<sup>109</sup>

In late August 2011, the *Financial Times* reported on another apparent instance of Chinese patrolling of disputed waters. The newspaper reported that a Chinese warship "confronted" an Indian navy vessel located 45 nautical miles off the Vietnamese coast on July 22. The vessel was returning from a scheduled port call in the southern Vietnamese port of Nha Trang.<sup>110</sup> India's Foreign Ministry quickly denied the report, noting only that an unseen caller identifying himself as the "Chinese Navy" contacted the Indian ship, the *INS Airavat*, and stated "you are entering Chinese waters," after which the *INS Airavat* proceeded on its journey. Chinese Foreign Affairs spokesman Ma Zhaoxu said that China had received no diplomatic protest from India over any naval incident.<sup>111</sup>

*Military exercises in the South China Sea*—China has conducted at least four series of military exercises in the South China Sea since November 2010.<sup>112</sup> According to testimony from Jim Thomas, vice president for Studies at the Center for Strategic and Budgetary Assessments, and Stacy Pedrozo, a U.S. Navy captain and military fellow at the Council on Foreign Relations, the PLA Navy conducted several significant exercises in 2010, including a November 2010 amphibious assault exercise that demonstrated PLA Navy capabilities to seize islands and project military power beyond mainland shores.<sup>113</sup> In June 2011, the PLA Navy staged similar drills off the coast of Hainan, China's island province in the South China Sea.<sup>114</sup> A PLA exercise took place along the Vietnam-China border in August 2011 as well, fueling media speculation that a large buildup of Chinese troops in the region could be related to South China Sea tensions.<sup>115</sup>

These exercises demonstrate the modernization of China's naval forces and China's will to project force beyond its shores, developments that have been met with considerable unease in the region. According to Mr. Thomas:

*[T]he stakes in the South China Sea could not be higher. ... In the last year ... China has made a series of provocative moves that, when coupled with the continuation of its arms buildup and the development of its naval power projection capabilities, have raised concerns throughout the region about its intentions and potential expansionist designs in the East and South China Seas.*<sup>116</sup>

*Construction on the disputed Spratly Islands, South China Sea*—In early June 2011, the Philippines' Department of Foreign Affairs stated that Philippine ships had witnessed a Chinese maritime surveillance vessel and PLA Navy ships unloading building materials and erecting a number of posts and a buoy on Amy Douglas Bank.<sup>117</sup> The bank, a small feature in the Spratly Islands, is located within what both China and the Philippines consider their EEZs.<sup>118</sup> The 2002 *Declaration on the Conduct of Parties in the South China Sea*, a legally nonbinding agreement between China and the Association of Southeast Asian Nations (ASEAN),\* which

\* ASEAN is a regional geopolitical and economic organization comprising the Southeast Asian nations of Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore,

provides guidelines for dealing with disputes in the South China Sea, declares that claimants should refrain from occupying previously uninhabited features in disputed areas.<sup>119</sup> According to Dr. Storey, if these reports are true, “it would be one of the most serious violations of the 2002 *Declaration of Conduct* to date.” Prior to China’s construction on Amy Douglas Bank, no claimant was proven to have begun construction on unclaimed islands and rocks since the declaration was signed.<sup>120</sup>

*Intimidating claimants with harsh rhetoric and closed-door directives*—Even during periods of conciliation and cooperation between China and other claimants, Southeast Asian claimants felt pressured to appease China on issues related to maritime disputes, according to officials and experts whom the Commissioners met during a December 2010 trip to Southeast Asia.<sup>121</sup> For instance, Secretary Clinton’s reference to the South China Sea as a “national interest” of the United States during her speech at the 2010 ASEAN Regional Forum was met with mixed reactions in Southeast Asia.<sup>†</sup> While some regional powers welcomed Secretary Clinton’s speech as reassurance of U.S. commitment to the region, Commissioners were told that her remarks, and China’s adverse reaction to them, prompted some claimant countries to minimize the territorial disputes publicly so as not to attract China’s ire.<sup>122</sup> For this apparent reason, a joint statement from a U.S.-ASEAN Leaders Meeting in September 2010 in New York City made no mention of the South China Sea, even though an earlier draft of the statement included explicit references to the disputes. According to a Singaporean government official who met with Commissioners, Vietnam’s representative at the New York meeting insisted that all references to the South China Sea be taken out of the statement.<sup>123</sup> Commissioners were also told that China had approached all ASEAN members separately and directed them to refrain from discussing the South China Sea, even among themselves.<sup>124</sup>

China’s insistence that claimants not discuss the disputes among themselves was challenged in September 2011, when ASEAN representatives met for two days to discuss a multilateral dispute resolution proposal offered by the Philippines. Senior Philippine diplomats said that Beijing had protested against the meeting, and a Chinese Defense Ministry spokesman remarked shortly after the gathering that China opposes “any move which is designed to multilateralize or internationalize the South China Sea issue.”<sup>125</sup>

Of import, China’s party-run media outlets have published a number of strongly worded editorials advocating that China use its military might to assert its sovereignty over disputed areas in the South China Sea. One such editorial, published in the party-run publication *Global Times*, asserted that China should “punish”

Thailand, and Vietnam. The Official Website of the Association for Southeast Asian Nations, “Overview,” [http://www.asean.org/about\\_ASEAN.html](http://www.asean.org/about_ASEAN.html).

<sup>†</sup>In an address during the 2010 ASEAN Regional Forum, Secretary Clinton asserted that the United States has a strategic interest in the “freedom of navigation, open access to Asia’s maritime commons, and respect for international law in the South China Sea.” She also offered for the United States to play a facilitating role in establishing a binding code of conduct for the claimants. These comments met harsh criticism in China, and China’s Foreign Ministry announced that Secretary Clinton’s remarks were “in effect an attack on China.” U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2010), pp. 132–139.

other claimant countries, namely Vietnam and the Philippines, by launching small-scale battles against their forces in the region.<sup>126</sup>

### Implications for the United States

China's intensified rhetoric and expanding presence in the South China Sea carry significant implications for the United States. China's growing maritime power could threaten U.S. interests in the Pacific and could lead to Chinese attempts to limit the freedom of navigation that the United States and other countries enjoy in the region. Mr. Thomas testified that as China develops its antiaccess capabilities and becomes increasingly competent operating in its regional maritime environment, China could possibly create a sea denial network stretching from the East China Sea to the South China Sea, eroding the ability of the United States to operate in the region.<sup>127</sup> (For more information on the PLA's ability to exert control over the western Pacific, see sec. 2 of this chapter.) Such a strategy, according to Captain Pedrozo, aligns with a 1982 Chinese naval maritime plan in which China would replace the United States as the dominant military power in the Pacific and Indian oceans by 2040.<sup>128</sup> Balbina Hwang, visiting professor at Georgetown University, echoed these concerns in her written testimony to the Commission:

*[T]he increasingly assertive Chinese maritime behavior we are witnessing today may be part of a broader strategy to exercise authority over smaller neighbors in the near term by pushing U.S. forces away from its maritime borders to demonstrate rights over the entire South and East China Seas. . . . One necessary concession in China's view will be the reduction of U.S. influence in the region.*<sup>129</sup>

Another implication of China's growing assertiveness, especially its harassment and intimidation of foreign vessels, is a growing risk of escalation due to miscommunication and miscalculation between claimants.<sup>130</sup> Foreign and Chinese analysts agree that China's various maritime enforcement actors often are not sufficiently coordinated with each other.<sup>131</sup> Combined with insufficient mechanisms to report unsafe practices at sea and encourage adherence to international laws and norms, minor incidents could escalate into larger problems. As chances of confrontation grow, issues could be raised for the United States, which has mutual defense obligations with the Philippines and other Asia-Pacific countries including Australia, Japan, New Zealand, South Korea, and Thailand.\*

### Cyber Issues

In continuation of previous practice, China in 2011 conducted and supported a range of malicious cyber activities.† These included

\* For more information on defense obligations between the United States and other countries, see Office of the U.S. Department of State, *Treaties in Force: A List of Treaties and Other International Agreements of the United States In Force on January 1, 2011* (Washington, DC: U.S. Department of State, 2011). <http://www.state.gov/documents/organization/169274.pdf>.

† Recent Commission Reports on the subject include U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, D.C.: U.S. Government Printing Office, November 2009), chapter 2, section 4; and U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, D.C.: U.S. Government Printing Office, November 2010), chapter 5.

network exploitations to facilitate industrial espionage and the compromise of U.S. and foreign government computer systems. Evidence also surfaced that suggests Chinese state-level involvement in targeted cyber attacks. Expert testimony to the Commission explained and contextualized China's strategy for the use of such attacks to achieve military objectives. In parallel to these developments, China asserted a greater level of control on domestic Internet content and engaged in various online surveillance activities.<sup>‡</sup>

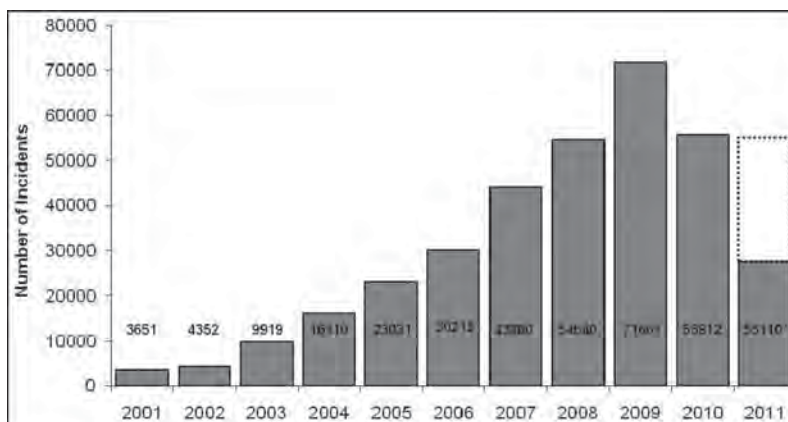
**Malicious Cyber Activities on  
U.S. Department of Defense Networks**

As the Commission reported in 2010, the U.S. government as a whole does not publish comprehensive statistics about malicious cyber activities on its networks. The Commission uses statistics published by the Department of Defense about exploitations and attacks on the department's information systems as one indicator of overall trends in the cybersecurity environment. Figure 2, below, demonstrates changes in the volume of such activities over the past decade. Not all of the incidents depicted below specifically relate to China (the department has not made available that level of detail).

---

<sup>‡</sup>This subsection's findings follow from numerous studies and reports over the past year that implicate China. Many times, investigators attribute incidents on the basis of technical or operational information, the details of which rarely become public. Other times, conclusions rely on inference. In either case, professional investigators typically offer attribution assessments with a specified degree of confidence. Such qualifications sometimes are inadequately conveyed, especially in secondary reports. Moreover, third parties likely use a variety of measures to make their attacks appear as coming from China in order to conceal their identities. (This model is a reasonable explanation for some penetrations, such as those for intellectual property theft, but less so for others, such as those that target Chinese dissidents.) Still, in the aggregate, the developments described below present compelling evidence of Chinese intrusions in practice.

**Malicious Cyber Activities on  
U.S. Department of Defense Networks—Continued**  
**Figure 2: Department of Defense Reported Incidents of Malicious Cyber  
Activity, 2001–2010, with Projection for 2011**



\*The figure for 2011 represents a projection based on incidents logged from January 1, 2011, to June 30, 2011. The projection assumes a constant rate of malicious activity throughout the year.

Sources: U.S.-China Economic and Security Review Commission, *Hearing on China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities*, testimony of Gary McAlum, May 20, 2008; Name withheld (staff member, U.S. Strategic Command), telephone interview with Commission staff, August 28, 2009; Name withheld (staff member, U.S. Cyber Command), e-mail interview with Commission staff, August 17, 2010; Name withheld (staff member, U.S. Cyber Command), e-mail interview with Commission staff, September 6, 2011.

### Computer network exploitation

In 2011, U.S. and foreign government organizations, defense contractors, commercial entities, and various nongovernmental organizations experienced a substantial volume of network intrusions and attempts with various ties to China. In March, security firm RSA announced that hackers had breached their networks and compromised elements of one of the firm's security products.\* Although the company did not name China specifically, subsequent research demonstrated that components of the attack utilized a tool called "HTran," developed by a well-known member of the hacking group "Honker Union of China."† An error in the tool's configuration revealed that the attackers attempted to obscure their location by routing command instructions from mainland China through serv-

\*The affected product was "SecurID," a two-factor authentication system where a token generates a unique number that users must provide in order to log into a protected account. Art Coviello, "Open Letter to RSA Customers" (Bedford, MA: RSA, March 17, 2011). <http://www.rsa.com/node.aspx?id=3872>.

†Joe Stewart, "HTran and the Advanced Persistent Threat" (Atlanta, GA: Dell SecureWorks, August 3, 2011). <http://www.secureworks.com/research/threats/htran/>. The tool's developer, Lin Yong, who also goes by the name "Lion," recently announced plans to reconstitute the Hacker Union of China after several years of inactivity. See Owen Fletcher, "Patriotic Chinese Hacking Group Reboots," *Wall Street Journal China Real Time Report*, October 5, 2011. <http://blogs.wsj.com/chinarealtime/2011/10/05/patriotic-chinese-hacking-group-reboots/>.



ers in Japan, Taiwan, Europe, and the United States.<sup>‡</sup> The perpetrators then used information about the compromised RSA security product in order to target a number of the firm's customers, including at least three prominent entities within the U.S. defense industrial base. Those intrusions and intrusion attempts, according to some reports, also originated in China and appeared to be state sponsored.<sup>132</sup>

Many intrusions linked to China involve numerous victims, sometimes spanning sectors and national borders.<sup>133</sup> When researchers identify and gain access to elements the systems used to effectuate the intrusion, such as servers that maintain contact with compromised systems, it becomes possible to identify related victims. The breadth of victims itself can suggest state involvement if the diversity in targets exceeds any conceivable scope of interest to a lone, subnational actor (or even a coalition of subnational actors).<sup>\*</sup> Although links to China are speculative and come from secondary reporting, a case study by McAfee, called *Operation Shady RAT* [remote access tool], illustrates this principle.<sup>†</sup> The 2011 study catalogues a series of penetrations affecting over 70 victim organizations that span numerous sectors, including federal, state, local, and foreign governments; energy and heavy industry; electronics and satellite communications; defense contractors; financial industry; and international sports institutions, think tanks, and nonprofits.<sup>134</sup> In discussing the possible actors behind the penetrations, the report states:

*The [perpetrators'] interest in the information held at the Asian and Western national Olympic Committees, as well as the International Olympic Committee (IOC) and the World Anti-Doping Agency in the lead-up and immediate follow-up to the 2008 Olympics was particularly intriguing and potentially pointed a finger at a state actor behind the intrusions, because there is likely no commercial benefit to be earned from such hacks. The presence of political nonprofits, such as a private western organization focused on promotion of democracy around the globe or a US national security think tank is also quite illuminating. Hacking the United Nations or the Association of Southeast Asian Na-*

<sup>‡</sup>The tool is probably available from Chinese websites and chat rooms. Whether the servers in mainland China were the true origin of the command traffic can only be verified with cooperation from China Unicom, a Chinese state-owned firm and the relevant network operator. Joe Stewart, "HTran and the Advanced Persistent Threat" (Atlanta, GA: Dell SecureWorks, August 3, 2011). <http://www.secureworks.com/research/threats/htran/>; and Gregg Keizer, "Researcher follows RSA hacking trail to China," *Computerworld*, August 4, 2011. [http://www.computerworld.com/s/article/9218857/Researcher\\_follows\\_RSA\\_hacking\\_trail\\_to\\_China](http://www.computerworld.com/s/article/9218857/Researcher_follows_RSA_hacking_trail_to_China).

<sup>\*</sup>This applies for penetrations that seek to maintain surveillance capabilities or extract information without inherent monetary value. Considerations of target scope do not apply for penetrations targeting personally identifiable or sensitive financial information, along with penetrations that seek to compromise systems for the purposes of creating a botnet.

<sup>†</sup>For the original report, see Dmitri Alperovitch, *Revealed: Operation Shady RAT* (Santa Clara, CA: McAfee: August 2011). <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>. The report itself does not mention China. For suggestions that China may be behind the intrusions, see Ellen Nakashima, "Report on 'Operation Shady RAT' identifies widespread cyber-spying," *Washington Post*, August 3, 2011. <http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI-story.html>; and Mathew J. Schwartz and J. Nicolas Hoover, "China Suspected of Shady RAT Attacks," *InformationWeek*, August 3, 2011. <http://www.informationweek.com/news/security/attacks/231300165>.



*tions (ASEAN) Secretariat is also not likely a motivation of a group interested only in economic gains.*<sup>135</sup>

Cyber penetrations that do not target diverse victims can still indicate state involvement. A February case study, called *Night Dragon*, profiled an exploitation campaign against global companies in the energy and petrochemical sectors. These sectors are of special interest to the Chinese government, which has designated seven “strategic industries” for “absolute state control,” including the power generation and distribution industry, the oil and petrochemicals industry, and the coal industry.<sup>136</sup> (For more information about China’s strategic industries, see chap. 1, sec. 2, of this Report.) In another indication of institutional involvement, the *Night Dragon* study’s authors noted that:

*[A]ll of the identified data exfiltration activity occurred from Beijing-based IP [intellectual property] addresses and operated inside the victim companies weekdays from 9:00 a.m. to 5:00 p.m. Beijing time, which also suggests that the involved individuals were ‘company men’ working on a regular job, rather than freelance or unprofessional hackers.*<sup>137</sup>

While the study’s authors could not definitely identify the perpetrators, an opaque web-hosting company and its Shandong-based operator appeared to be involved.<sup>138</sup> As described below, Shandong Province is connected to several other penetrations over the past several years.

China-based hackers increasingly use indirect approaches to gain access to sensitive information systems. In June, Google announced that it had discovered a widespread but targeted “phishing” campaign that had compromised Google Mail (Gmail) accounts.\* The company disclosed that:

*This campaign, which appears to originate from Jinan, China, affected what seem to be the personal Gmail accounts of hundreds of users including, among others, senior U.S. government officials, Chinese political activists, officials in several Asian countries (predominantly South Korea), military personnel and journalists.*<sup>139</sup>

Aside from Gmail users, the campaign reportedly affected certain U.S. government e-mail accounts at the Department of State, the Department of Defense, and the Defense Intelligence Agency. The perpetrators leveraged access to compromised accounts to perpetuate the campaign by spreading malicious software to the victims’ contacts.† As the Commission reported in 2009, Jinan, Shandong Province, is the home of one of China’s Technical Reconnaissance

\*“Phishing” is “an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent web site that appears legitimate. The user then may be asked to provide personal information such as account usernames and passwords that can further expose them to future compromises. Additionally, these fraudulent web sites may contain malicious code.” U.S. Computer Emergency Readiness Team (U.S.-CERT), “Report Phishing.” [http://www.us-cert.gov/nav/report\\_phishing.html](http://www.us-cert.gov/nav/report_phishing.html).

†This is called the “man-in-the-mailbox” technique. John Markoff and David Barboza, “F.B.I. to Investigate Gmail Attacks Said to Come From China,” *New York Times*, June 2, 2011. [http://www.nytimes.com/2011/06/03/technology/03google.html?\\_r=1](http://www.nytimes.com/2011/06/03/technology/03google.html?_r=1).

Bureaus. These entities serve as a computer network exploitation arm for the Third Department of the PLA's General Staff Department, which collects signals intelligence.<sup>140</sup> A vocational school linked to the December 2009 Google penetration is also located in Jinan.<sup>141</sup>

During a Commission trip to China in August 2011, representatives of foreign businesses that operate in China placed computer network intrusions alongside mandated technology transfers and invasive technical standards inspection schemes as the most serious threats to their intellectual property. Chinese efforts suggest that, for firms without a physical presence in China, computer network intrusions may pose the most serious threat to intellectual property.

### Computer network attack

Along with the considerable computer network exploitation capabilities described above, the Chinese government has computer network attack capabilities. As the Department of Defense's 2011 annual report to Congress on *Military and Security Developments Involving the People's Republic of China* states, "[t]he PLA has established information warfare units to develop viruses to attack enemy computer systems and networks."<sup>\*</sup> This has implications for military and nonmilitary targets. For example, a 2011 global survey of critical infrastructure operators conducted by McAfee and the Center for Strategic and International Studies identified government-sponsored sabotage as a central cyber threat. The plurality of respondents, 30 percent, identified the Chinese government as the greatest concern.<sup>142</sup> While the survey measured perceptions rather than events, its findings illustrate the concerns of those on the "frontlines" of infrastructure protection.<sup>†</sup>

Perhaps the most compelling evidence that surfaced in 2011 linking the Chinese government to cyber attacks was a July documentary presented on China Central Television 7 (CCTV-7), the government's military and agricultural channel. A brief segment demonstrated what appears to be a PLA "point and click" distributed denial of service attack launched against a Falun Gong-related website hosted on a network at the University of Alabama in Birmingham. Based on Internet Protocol data exposed in the program and information from the school's network administrators, the attack appears to have taken place in 2001 or earlier.<sup>‡</sup> According to the footage, the PLA's Electrical Engineering University developed the software used to launch the attack.<sup>143</sup> Some reports about this

<sup>\*</sup>Parallel developments include "tactics and measures to protect friendly computer systems and networks." Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: Department of Defense, 2011), p. 37.

<sup>†</sup>China also faces challenges in securing infrastructure. For example, see Paul Roberts, "Glass Dragon: China's Cyber Offense Obscures Woeful Defense," *Threatpost*, April 27, 2011. [http://threatpost.com/en\\_us/blogs/glass-dragon-chinas-cyber-offense-obscures-woeful-defense-042711](http://threatpost.com/en_us/blogs/glass-dragon-chinas-cyber-offense-obscures-woeful-defense-042711). See also Jim Finkle, "Exclusive: China software bug makes infrastructure vulnerable," *Reuters*, June 16, 2011. <http://www.reuters.com/article/2011/06/17/us-cybersecurity-china-idUSTRE75G0CV20110617>.

<sup>‡</sup>Other attacks have been documented more recently, including in 2011. See, for example, Benjamin Joffe-Walt, "U.S. Congresswoman Condemns Chinese Attack on Change.org," *Change.org Blog*, April 26, 2011. <http://blog.change.org/2011/04/u-s-congresswoman-condemns-chinese-attack-on-change-org/>.

incident suggested that the attack shown was rudimentary, apparently on the basis of the program's graphical user interface and the attack method itself. However, the scope and implications of the attack cannot be determined from the footage.\* Initially posted on the broadcaster's website, the documentary episode was promptly removed by CCTV when international media started to report the story. This measure, along with the offhanded manner by which the show presented the material, led most reports to characterize the footage as an accidental disclosure.<sup>144</sup>

### **Military strategies**

Like the United States and other nations with modern militaries, China seeks to leverage cyber capabilities to achieve or help achieve military objectives. As the Department of Defense's 2011 annual report to Congress on *Military and Security Developments Involving the People's Republic of China* states, China's military could use cyber warfare "to constrain an adversary's actions or slow response time by targeting network-based logistics, communications, and commercial activities."<sup>145</sup> Expert testimony to the Commission in 2011 provided details about how China would seek to employ such techniques. David A. Deptula, a retired U.S. Air Force lieutenant general, testified that China has "identified the U.S. military's reliance on information systems as a significant vulnerability that, if successfully exploited, could paralyze or degrade U.S. forces to such an extent that victory could be achieved."<sup>146</sup> Specifically, General Deptula categorized cyber attacks on U.S. C4ISR [command, control, communications, computers, intelligence, surveillance, and reconnaissance] assets as a key action that China's military would take "to impede U.S. military access to the Asian theater in the event of a U.S.- China conflict."<sup>147</sup>

Martin C. Libicki, senior management scientist at the RAND Corporation, testified that operational cyber attacks, such as those that would degrade U.S. logistics systems, present a serious challenge to U.S. military forces. As such, the "[U.S.] Department of Defense needs to take the prospect of *operational* cyberwar seriously enough to understand imaginatively and in great detail how it would carry out its missions in the face of a full-fledged attack" (emphasis in original).<sup>148</sup> He characterized *strategic* cyberwar, such as "a cyberattack on the U.S. power grid, throwing the Midwest into the dark," as less likely in the context of a Taiwan contingency, a conceivable backdrop to hostilities between the United States and China. Because China's leadership would likely seek to keep the United States out of such a contingency, a strategic cyber attack on the United States might have the opposite effect and could therefore serve as a "very poor coercive tool."<sup>149</sup> However, this assessment may not hold for other types of contingencies.

\*A graphical user interface could easily be mated with a controller capable of launching a signification distributed denial of service attack. A military organization would likely use such an interface in order to make its computer network operations tool more accessible to its force. With respect to the method of attack itself, computer security experts generally regard distributed denial of service attacks as one of the more manageable threats. However, certain techniques are sophisticated and difficult to mitigate. For a brief discussion of what constitutes a significant distributed denial of service attack, see Craig Labovitz, "The Internet Goes to War" (Chelmsford, MA: Arbor Networks, December 14, 2010). <http://asert.arbornetworks.com/2010/12/the-internet-goes-to-war/>.

### Surveillance and censorship

The Chinese government asserted a greater level of control over domestic Internet access and content in 2011. In May, it created a new State Council-level entity to centralize “online content management,” a euphemism in China for various forms of regulation and censorship.<sup>150</sup> More recently, China’s censors blocked web-based speculation by Chinese citizens about the health and possible death of former Chinese President Jiang Zemin following his failure to appear at a celebration of the 90th anniversary of the CCP’s founding.<sup>151</sup> This year’s social media-assisted demonstrations in the Arab world, sometimes leading to regime change, appear to have intensified the Chinese government’s traditional apprehension about political discourse.<sup>152</sup>

Other new measures appear to be technical outgrowths of existing policies. Fang Binxing, the creator of China’s “great firewall,” acknowledged in February that he personally used six virtual private networks to test whether they could overcome China’s traffic-blocking measures.<sup>153</sup> Subsequently, several times throughout 2011, new Chinese censorship measures disrupted this previously reliable method used to circumvent local restrictions on overseas web content.<sup>154</sup> Chinese authorities also curtailed domestic web content. The Chinese Academy of Social Sciences announced in July that the government shuttered 1.3 million websites throughout 2010.<sup>155</sup> Some percentage of these sites probably hosted malicious software as opposed to content deemed undesirable to the Chinese government (such as pornography or political speech), but the government does not make available figures with that level of specificity.

In at least one instance this year, U.S. Internet traffic improperly transited Chinese networks.<sup>156</sup> Following a series of similar incidents documented in the Commission’s 2010 Annual Report, select U.S.-generated Internet traffic from social networking site Facebook travelled on a route through Chinese state-owned telecommunications firm China Telecom on March 22, 2011.\* The exact path of the diversion could not be reconstructed, but the affected traffic may have traversed networks physically located in China.† Although perhaps accidental, such an incident demonstrates a vulnerability that could be used for exploitation or attack. The capability to initiate or exploit erroneous traffic routes exists for all Internet Service Providers, but state ownership of the entire sector in China (as another “strategic industry”) elevates the risk of systemic abuse, either as an intentional measure directed against external Internet users or a side effect of internal censorship policies.

### Implications for the United States

China appears to use computer network exploitations to conduct espionage against governments and military entities, commercial entities, and nongovernmental organizations. In parallel, the PLA maintains capabilities to execute computer network attacks. These

\*The data also traversed Hanaro Telecom South Korea’s networks.

†Alternatively, the data could have traversed China Telecom networks physically located in North America. BGPmon.net, Untitled, March 26, 2011. <http://bgpmon.net/blog/?p=499>.

practices have myriad implications for the United States. Computer network exploitation directed against government entities jeopardizes their ability to handle sensitive information securely and reliably. Network exploitations and attacks on military entities may compromise large-scale weapons systems, delay deployments, or cause a number of other events that harm U.S. national security and regional stability in Asia. China's exploitations that compromise commercial entities' proprietary information and intellectual property likely bolster Chinese firms' capabilities and erode U.S. businesses' remaining technological advantages. In addition, Chinese penetrations of, and assaults on, nongovernmental organizations' networks complicate their operations and could pose security risks for their members and affiliates.

### Conclusions

- Over the past year, China has demonstrated progress in modernizing the PLA. Recent developments confirm that the PLA seeks to improve its capacity to project force throughout the region.
- Continued improvements in China's civil aviation capabilities, as first noted in the Commission's 2010 Annual Report, enhance Chinese military aviation capabilities because of the close integration of China's commercial and military aviation sectors.
- In an effort to calm regional fears, China attempts to broadcast a benign image of its growing military capabilities. Official statements from Beijing over the past year describe China as a status quo power and downplay its military modernization efforts.
- In 2011, China continued a pattern of provocation in disputed areas of the South China Sea. China's policy in the region appears driven by a desire to intimidate rather than cooperate. Many of China's activities in the region may constitute violations of the *United Nations Convention on the Law of the Sea* and the *Declaration on the Conduct of Parties in the South China Sea*. While China sometimes demonstrates a willingness to cooperate with other claimants to disputed waters in the South China Sea, it is unlikely that China will concede any of its claims.
- China's government or military appeared to sponsor numerous computer network intrusions throughout 2011. Additional evidence also surfaced over the past year that the Chinese military engages in computer network attacks. These developments are consistent with the PLA's known missions and organizational features, as noted by the Commission's *2009 Annual Report to Congress* and contracted research study *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*.\*
- China's military strategy envisions the use of computer network exploitation and attack against adversaries, including the United States. These efforts are likely to focus on operational systems, such as command, control, communications, computers, intel-

---

\*This report was prepared for the Commission by Northrop Grumman and is available on the Commission's website at [http://www.uscc.gov/researchpapers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper\\_FINAL\\_Approved%20Report\\_16Oct2009.pdf](http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf).

ligence, surveillance, and reconnaissance assets. This could critically disrupt the U.S. military's ability to deploy and operate during a military contingency. Chinese cyber attacks against strategic targets, such as critical infrastructure, are also possible.



## SECTION 2: CHINA’S “AREA CONTROL MILITARY STRATEGY”

### Introduction

During the 2011 report cycle, the Commission examined China’s military strategy. At its core, this strategy provides guidance to the People’s Liberation Army (PLA) on how to defeat a technologically superior opponent and can be summarized as having three themes. First, it emphasizes degrading an opponent’s technological advances in an effort to level the playing field. Second, it is a military strategy that prioritizes striking first in a conflict to seize the initiative. Third, its geographic focus centers on controlling China’s periphery, especially the western Pacific Ocean. Over the past decade, these themes have been reflected in China’s military modernization efforts. As a result, it appears that the PLA is acquiring improved capacities to counter U.S. military capabilities and exploit U.S. military weaknesses. Furthermore, because the focus of China’s military strategy has expanded beyond just a Taiwan scenario, it increasingly impacts China’s neighbors, especially those in the western Pacific Ocean. Finally, the strategy’s emphasis on striking first opens the door to the possibility of miscalculations and inadvertent conflict.

As a note of clarification, although China’s military strategy is commonly referred to as an “antiaccess” or “area denial” strategy in western writings,<sup>157</sup> this Report will refer to this strategy as an “Area Control Strategy.” Referring to China’s strategy as an “antiaccess” or “area denial” strategy posits an overly U.S.-centric viewpoint, giving the impression that this strategy is intended solely to prevent U.S. forces from approaching China in the event of a conflict. While deterring, delaying, or denying U.S. forces from operating along China’s periphery is still a key PLA goal, the Commission’s *2009 Annual Report to Congress* demonstrated that PLA missions have expanded.<sup>158</sup> Additional contingencies now include, for example, the defense of China’s disputed territorial claims in the East and South China Seas.\* As such, a continued U.S.-centric approach downplays the point that China’s military strategy can be just as effectively used against other militaries throughout East Asia. Conventionally armed missiles that can target U.S. bases and forces in East Asia can just as easily strike Japanese, Philippine, or even Vietnamese bases and forces in the event of a conflict.

Summarizing the Commission’s findings from a hearing, fact-finding trips to the U.S. Pacific Command and Asia, and staff research, this section of the Report describes the PLA’s Area Control Strategy and the implications for the United States and East Asia.

---

\*For more on recent PLA activities in the South and East China Seas, see section 1 of this chapter.

It concludes with summary points and recommendations for Congress.

**Congressional Remarks on  
China's Area Control Military Strategy**

Presenting his views to the Commission on China's Area Control Strategy, Congressman Robert J. Wittman (R-VA) noted that "China's military policies are aimed at translating the nation's growing economic resources into a world-class war fighting organization" and that the rapid pace of its military modernization has "already [put] regional military balances at risks." The congressman also described his view that China's Area Control Strategy could deny the United States the ability to project power into the region, without which "the integrity of U.S. alliances and security partnerships could be called into question, reducing U.S. security and influence and increasing the possibility of conflict." In order to prevent this from occurring, the congressman recommended that the United States needs to focus "on force posture, maintaining alliances, and maintaining the current footprint of strategically located bases in the western Pacific."<sup>159</sup>

Senator Daniel K. Inouye (D-HI) submitted a written statement to the Commission, stating that China has "increased the size of [its] navy, created formidable cyber warfare capabilities, developed new anti-ship and anti-satellite missiles, initiated a new stealth fighter, and begun construction of an aircraft carrier." The senator also expressed his concern that the PLA is "investing so heavily in anti-access weapons, almost certainly to counter our power projection capabilities." However, he also stated that it is important to look at China's military developments through the prism of capabilities the U.S. military is developing and not solely "those we currently possess." In order to maintain stability in the region, Senator Inouye suggested that the United States should continue to reassure its friends and allies in the region, maintain a strong forward military presence, and promote improved ties between the mainland and Taiwan.<sup>160</sup>

**China's Area Control Military Strategy**

At its core, the PLA's Area Control Strategy is a set of guidelines to help the PLA win in a conflict with a technologically superior military.<sup>161</sup> As Roger Cliff, then senior political scientist at the RAND Corporation, concluded, China's military strategy embodies "ways in which a country with less-advanced military capabilities might seek to diminish the advantage enjoyed by a country with greater military capabilities."<sup>162</sup> Cortez A. Cooper, a senior international relations analyst at the RAND Corporation, testified that "[t]he PLA's most authoritative modern work on military strategy, *The Science of Military Strategy*, states that in the current threat environment, preparing for a local war against a technologically superior adversary is 'the center of gravity of strategy'."<sup>163</sup> This influential book continues, noting that China's strategic guidance fo-

cuses on how “to defeat a technically superior enemy equipped with high-tech weaponry in the background of relative [Chinese] lag of military technology” [sic].<sup>164</sup> Official PLA regulations, such as Beijing’s annual training guidance to the PLA, codify the notion of being able to defeat a better-equipped enemy.<sup>165</sup> As Oriana Skylar Mastro, a Ph.D. candidate at Princeton University and a visiting fellow at The George Washington University, testified, China’s strategists believe that “not all wars are won by the strongest side,” a view fueled in part by their belief that China successfully overcame technologically superior U.S. forces during the Korean War.<sup>166</sup>

In an effort to defeat a superior military, China’s Area Control Strategy can be summarized as having three themes:

- It emphasizes degrading a superior opponent’s technological advances;
- It stresses striking first in order to seize the initiative; and
- It centers on controlling China’s periphery, especially the western Pacific Ocean.

Each theme will be discussed in turn below.

#### **Historical Legacy of China’s Military Strategy: The “Active Defense”**

Officially, China refers to its military strategy as the “Active Defense.” This term has evolved from its original usage in a 1936 Mao Zedong article, where Communist Party Chairman Mao severely critiqued the communist forces’ strategy used to fight the then ruling Nationalist Party during China’s civil war. According to Chairman Mao, the communists had been fighting a passive, defensive war against the much better-equipped Nationalist Army, which resulted in frequent and severe losses for the communists. Instead of defensive operations, Chairman Mao urged the communists to take the initiative and bring the fight to the nationalists at a time and place best suited to the communists. This strategy would allow the inferior communist forces to overcome their technological disadvantages when confronting the nationalist forces. He referred to such a strategy as the Active Defense, noting that:

*The active defense is also known as offensive defense, or defense through decisive engagements. Passive defense is also known as purely defensive defense or pure defense. Passive defense is actually a spurious kind of defense, and the only real defense is active defense, defense for the purpose of counter-attacking and taking the offensive.*<sup>167</sup>

#### **Theme 1: It Is a Strategy that Focuses on Degrading an Opponent’s Technological Advantages**

As several expert witnesses described to the Commission, China’s Area Control Strategy heavily emphasizes the necessity of degrading an opponent’s technological advantages.<sup>168</sup> Ms. Mastro noted that in order to hinder a superior military from operating off of

China's periphery, the PLA seeks to employ "an enhanced conventional precision strike system consisting mainly of cruise and ballistic missiles as well as attacks on key enabling capabilities, such as space-based [command, control, and surveillance systems] and computerized networks."<sup>169</sup> The PLA's *The Science of Military Strategy*, for example, instructs senior PLA commanders that:

*In order to win the future local war under high-tech conditions, the PLA must take 'destruction war' or 'paralysis and destruction warfare' as the overall and basic forms of war. The so-called 'destruction warfare' is to employ several kinds of means to disrupt the integrity of the enemy's operational systems and the sequence of his operations, to change the balance of strength in the battlefield by making the enemy lose his combat capabilities as a whole, and to create situation and conditions which are beneficial to preserve ourselves and destroy the enemy. [sic]*<sup>170</sup>

One way the PLA seeks to degrade an opponent's technological advantages is to target the vulnerable, yet important, nodes that undergird the opponent's technologically based combat capabilities.<sup>171</sup> For example, the authoritative PLA textbook on military campaigns, *The Science of Campaigns*, notes that:

*The enemy's combat system depends upon the various systems comprised of high technology equipment, closely linked to each other, whose mutual dependency is strong, thus having a certain weakness. Whenever a key part or key segment is destroyed, this can influence the entire system, even causing the entire system to be paralyzed. Therefore, we need to be good at grasping the key parts of the enemy's combat system and destroying them, like assaulting and destroying the enemy's command and control system, information system, weapons system, and important support system.*<sup>172</sup>

Dr. Cliff provided an example of a target set that Chinese defense writings discuss when mentioning striking an opponent's logistics system. Such targets could include, at a minimum:<sup>173</sup>

- |   |  |
|---|--|
| • Air bases, especially runways                 | • Transport and aerial refueling aircraft  |
| • Naval ports                                   | • Naval troop transports                   |
| • Fuel, munitions, and other storage facilities | • Tankers and underway replenishment ships |
| • Fuel pipelines                                | • Railroads                                |
| • Support facilities                            | • Bridges                                  |

### ***Theme 2: It Is a Strategy that Emphasizes Striking First***

Despite Beijing's claim that its military strategy is defensive, the PLA's Area Control Strategy places a high priority on carrying out the first strike against an opponent in a conflict. Officially, China's national security policy is "defensive in nature," and China does not initiate military operations.<sup>174</sup> Instead, China "adheres to the principle of implementing defensive operations, self-defense and gaining mastery by counterattacking" after its interests are at-

tacked.\*<sup>175</sup> However, this claim downplays the offensive nature of the PLA's Area Control Strategy. This is partly due to Beijing's ambiguous views on what it perceives as an infringement on its interests. The DoD in 2010 wrote:

*[T]he authoritative work, The Science of Military Strategy, makes it clear that the definition of an enemy strike is not limited to conventional, kinetic military operations. Rather, an enemy 'strike' may also be defined in political terms. Thus: 'Striking only after the enemy has struck' does not mean waiting for the enemy's strike passively. ... It doesn't mean to give up the 'advantageous chances' in campaign or tactical operations, for the 'first shot' on the plane of politics must be differentiated from the 'first shot' on that of tactics. [This section continues] if any country or organization violates the other country's sovereignty and territorial integrity, the other side will have the right to 'fire the first shot on the plane of tactics.' [emphasis added]*<sup>176</sup>

Historical PLA military operations reflect this ambiguity. For example, in 1979 China initiated a short, intense border war with Vietnam after Vietnam invaded the then Chinese client state of Cambodia. Although China initiated combat operations, Beijing's view is that this was a defensive operation and officially labels it the "Self-Defense Counter-Attack Against Vietnam."<sup>177</sup> Beijing similarly describes PLA operations during the Korean War (1950–53) and during China's border conflicts with India (1962) and Russia (1969).<sup>178</sup> One well-respected scholar on the PLA referred to China's frequent labeling of offensive military operations as defensive as a "Chinese cult of the defense," where Beijing engages in "offensive military operations as a primary alternative in pursuit of national goals, while simultaneously rationalizing them as being defensive and a last resort."<sup>179</sup>

Regardless of the ambiguity at the political level, once Beijing determines that China's interests have been infringed upon, the strategy takes a clear offensive focus. According to David A. Deptula, U.S. Air Force lieutenant general (retired):

*Once hostilities have begun, the essence of [China's military strategy] is to take the initiative and to annihilate the enemy. Strategically, the guidelines emphasize active defense, in military campaigns the emphasis is placed on taking the initiative in 'active offense.' [emphasis as in original]*<sup>180</sup>

PLA writings stress striking first in order to ensure the advantage of surprise over the opponent.<sup>181</sup> According to Dr. Cliff, one reason why the PLA values the element of surprise is because the PLA sees modern warfare as "one of rapid-paced, short-duration conflicts," where defeat or victory can quickly occur.<sup>182</sup> While the PLA views the U.S. experiences in Afghanistan and Iraq as evidence that some wars may be protracted, in general the PLA focuses on being able to conclude a conflict as rapidly as possible.<sup>183</sup>

\*For more on the political narratives of China's defense policy, see chapter 4 of this Report, "China's Public Diplomacy Initiatives Regarding Foreign and National Security Policy."



Therefore, the PLA maintains the view that it is imperative to seize the initiative from the outset of a conflict.<sup>184</sup> This concept is reflected in *The Science of Military Strategy*, which posits that the PLA “should do all [it] can to dominate the enemy by striking first.”<sup>185</sup>

Of note is the PLA’s predisposition to attack while the opponent is still building up its forces. According to Dr. Cliff:

*Preemption [i.e., striking first] is seen as an excellent way of seizing the initiative as well as of achieving surprise. Preemption also strongly supports the concept of employing access-denial measures as, if an adversary is allowed time to fully build its forces up in theater, the effectiveness of access-denial measures will be greatly reduced. If, on the other hand, a preemptive attack is launched well before the adversary is fully prepared for conflict, then anti-access measures can lengthen the amount of time that the local military advantage preemption provides will last.*<sup>186</sup>

The notion of striking first is extensive throughout Chinese military writings. *The Science of Campaigns* writes, for example, that:

*It is now possible to achieve our operational goals through rapid and sudden activities before the enemy can react. Compared to using concealment to achieve suddenness, rapid actions are not only capable of using firepower damage and troop attack activities to directly weaken the enemy’s combat capabilities, but are also able to catch the enemy unaware, causing psychological fear and awe in the enemy—and thus dominating and destroying the enemy’s will to resist. . . . If the PLA is in combat with a high-tech and strong enemy, then there is a large gap between their weapons and equipment and ours. If we want to achieve operational suddenness, in addition to retaining traditional concealment, camouflage, and deception, we need to stress even more the PLA’s traditional specialties of maneuver warfare and flexible tactics, require the breaking of norms in operational distance, speed, and combat methods; and strike the enemy unprepared through rapid actions and asymmetric methods and means.*<sup>187</sup>

***Theme 3: It Is a Strategy that Stresses the Need to Control China’s Periphery, Especially the Western Pacific Ocean***

China’s Area Control Strategy has a specific geographic focus, seeking to establish a defensive zone of control around China’s territory. The primary focus of this zone of control concentrates on the maritime region off of China’s eastern seaboard, especially within what is referred to as the “First Island Chain” [see figure 1, below].\*<sup>188</sup> For China, there are at least three reasons why control over this region is critical. First, it provides important benefits to China’s economy: China’s most economically developed areas are located along its coast; China’s economy is heavily dependent upon the trade and energy sea lanes that transverse this region; and en-

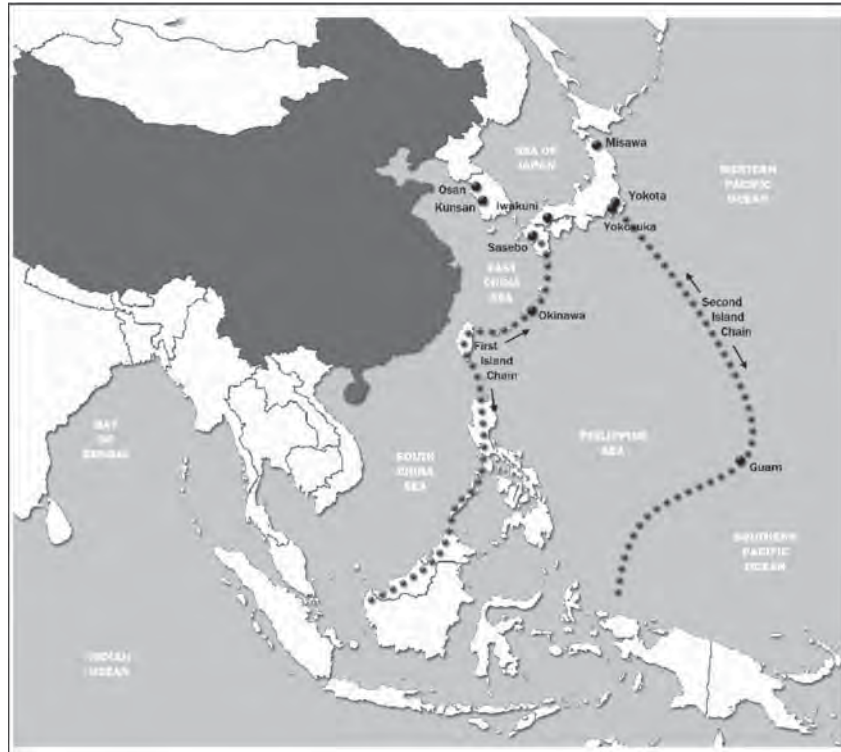
\*The “First Island Chain” represents a line of islands running from Japan, the Senkaku (Diaoyu) Islands, Taiwan, and the west coast of Borneo to Vietnam.



ergy and natural resources in the region are necessary for China's continued economic growth. Second, China has several disputed territorial claims in this region, the most important of which is its sovereignty claim over Taiwan, an island that enjoys de facto, albeit disputed, independence from Beijing.\* Several nations also dispute Beijing's maritime territorial claims, and the accompanying resources, in the South and East China Seas.†<sup>189</sup> Third, China's understanding of modern warfare posits the importance of preventing an enemy from being able to operate freely close to China's territory. According to *The Science of Military Strategy*:

*As long as the battlefield is concerned, we should not passively fight against the enemy in our border regions, coastal regions and related air space. On the contrary, after the launching of the war, we should try our best to fight against the enemy as far away as possible, to lead the war to enemy's operational base, even to his source of war, and to actively strike all the effective strength forming the enemy's war system. [sic]*<sup>190</sup>

**Figure 1: The First and Second Island Chains**



Source: Jan Van Tol et al., *AirSea Battle: A Point of Departure Operational Concept* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), p. 13.

\*For more on the Sino-Taiwan dispute, see chapter 3, section 3, of this Report.

†In the South China Sea, China has maritime territorial disputes with Taiwan, the Philippines, Malaysia, Brunei, and Vietnam. In the East China Sea, Japan disputes China's claim to the Senkaku/Diaoyutai Islands.

Of import, the PLA's geographic focus is expanding. Over the past five years, the PLA has expanded its mission beyond a Taiwan contingency also to cover potential conflicts in the East and South China Seas.<sup>191</sup> This change was highlighted during Commissioners' discussions with senior Singaporean officials in December 2010.<sup>192</sup> The Commission concluded in both its 2009 and 2010 Reports that the Chinese leadership has tasked the PLA to be capable of conducting operations increasingly farther from China's territory,<sup>193</sup> a point underscored in several of China's defense white papers.<sup>194</sup> The U.S. Department of Defense, in its most recent assessment of the PLA, goes so far as to state that "the PLA has been developing new platforms and capabilities that will extend its operational reach to address other concerns within the East and South China Seas, and possibly to the Indian Ocean and beyond the second island chain in the western Pacific."<sup>195</sup> According to Stacy A. Pedrozo, a captain in the U.S. Navy and military fellow at the Council on Foreign Relations, this expansion reflects the influence of the PLA's strategy to extend its control gradually out past what is often referred to as the "Second Island Chain."\* Said Captain Pedrozo:

*In the first stage, from 2000 to 2010, China was to establish control of waters within the First Island Chain that links Okinawa Prefecture, Taiwan, and the Philippines. In the second stage, from 2010 to 2020, China would seek to establish control of waters within the Second Island Chain that links the Ogasawara Island chain, Guam, and Indonesia. In the final stage, from 2020 until 2040, China would put an end to U.S. military dominance in the Pacific and Indian Oceans, using aircraft carriers as a key component of their military force.*<sup>196</sup>

### **The Implementation of the PLA's Area Control Strategy**

Fueled by decades of strong economic growth, China has been able to ramp up spending on its military modernization efforts (see sec. 1 of this chapter for more on China's military budget). Many of these efforts closely mirror the requirements for China's Area Control Strategy. Below are detailed briefly the PLA's military developments that are most relevant to its Area Control Strategy.

*Submarines:* As noted by General Deptula, "China's submarine force is a key component of their sea denial strategy."<sup>197</sup> Of particular importance are the PLA Navy's diesel-electric attack submarines, which have the requisite stealth capabilities for sea control operations. Although the submarines were originally acquired from Russia, China is now able to produce its own modern diesel-electric submarines.<sup>198</sup> Since 1995, China has deployed 27 modern diesel-electric attack submarines with advanced capabilities. For example, China's most modern submarine, a *Yuan*-class launched in September 2010, is almost as difficult to detect as the most advanced Russian diesel-electric submarine. In addition, this submarine likely employs an air-independent propulsion system, allowing it to stay submerged for longer periods of time.<sup>199</sup>

\*The "Second Island Chain" concept denotes the set of islands that run in a north-south line from Japan, the Bonin (Ogasawara) Islands, the Mariana Islands, and Indonesia.

*Conventional ballistic missiles:* China has the most active missile development program in the world. In its 2010 report, the Commission described in detail the growing capabilities of China's conventional ballistic missile forces, noting that the PLA has over 1,100 short-range ballistic missiles\* as well as over 100 medium-range ballistic missiles, most of which are deployed opposite Taiwan.<sup>200</sup> According to General Deptula, China's ballistic missiles "have a variety of ranges, payloads, and capabilities to strike aircraft carriers, airfields, command and control facilities, logistics nodes, ports, and military bases."<sup>201</sup> Of significance to the PLA's Area Control Strategy is China's antiship ballistic missile, the DF-21D. According to the U.S. Department of Defense's 2011 report to Congress on China's military power, the DF-21D "is intended to provide the PLA [with] the capability to attack ships, including aircraft carriers, in the western Pacific Ocean."<sup>202</sup> When deployed, this missile will provide the PLA with the ability to strike naval targets within all of the First Island Chain and large portions of the Second Island Chain. (For more information on recent developments of the DF-21D, see sec. 1 of this chapter.)

*Conventional land-attack cruise missiles:* The PLA augments its ballistic missile forces with a growing arsenal of conventional land-attack cruise missiles.† In particular is the PLA's DH-10, a land-attack cruise missile, which can be launched by ground or air. When outfitted on a Chinese H-6H medium bomber, the DH-10 provides the PLA with the capability to hit targets up to 3,700 kilometers away, more than sufficient to strike Andersen Air Force Base on the island of Guam.<sup>203</sup> The U.S. Department of Defense writes in its 2011 report to Congress that China currently possesses between 200 and 500 such missiles.<sup>204</sup>

*Naval mine warfare capabilities:* China's growing naval mine warfare capabilities provide a cheap and efficient means for controlling maritime territories around China's periphery.<sup>205</sup> According to Ronald O'Rourke, a naval specialist at the Congressional Research Service, the PLA Navy's mine warfare ships went from zero in 2005 to 40 in 2009.<sup>206</sup> Augmenting China's dedicated mine warfare vessels are surface warships, submarines, aircraft, and converted civilian merchant or fishing vessels that can also deliver naval mines.<sup>207</sup>

*Air strike capabilities:* The Commission's 2010 Report noted that the PLA Air Force is undergoing a major transformation and is currently developing the ability to conduct offensive strikes outside China's territory, a sea change from a decade ago. In recent years,

\*Ballistic missiles are missiles fired from ground launchers or submarines in an arc to its target, usually exiting and reentering the earth's atmosphere along its flight path. Ballistic missiles are usually classified according to their range: short range (<1,000 kilometers [km]), medium range (1,000–3,000 km), intermediate range (3,000–5,500 km) and intercontinental ballistic missiles (>5,500 km). National Air and Space Intelligence Center, *Ballistic and Cruise Missile Threat* (Dayton, OH: Department of the Air Force, April 2009), pp. 6–7.

†Cruise missiles are self-propelled missiles that fly along a direct trajectory to the target and can be fired from an aircraft, ship, submarine, or ground-based launcher. Cruise missiles are classified according to mission: land-attack or antiship cruise missiles. National Air and Space Intelligence Center, *Ballistic and Cruise Missile Threat* (Dayton, OH: Department of the Air Force, April 2010), pp. 26–27.

the PLA Air Force has developed two advanced 4th generation\* fighters, the J-10 and the J-11B. Earlier this year, the PLA Air Force also revealed a developmental 5th generation stealth fighter, the J-20 (For more on China's J-20 stealth fighter, see sec. 1 of this chapter.). These operational fighters (J-10 and J-11B) provide Beijing with both the ability for precision strikes along China's periphery and an advanced capability to defend against an opponent's air attacks.<sup>208</sup>

*Advanced air defense capabilities:* As noted in the Commission's 2010 Annual Report, Beijing has prioritized "strengthening China's air defense capabilities." To that effect, the PLA is constructing a highly capable integrated air defense system, comprised of a growing number of advanced air defense missile launchers deployed in overlapping rings. China has also deployed a national air defense network to integrate these various individual launchers.<sup>209</sup> When coupled with improvements in China's combat fighter capabilities discussed above, China acquires "one of the most sophisticated and densely integrated air defense systems (IADS) in the world,"<sup>210</sup> according to General Deptula.

*Electronic warfare capabilities:* As the U.S. Department of Defense notes, the PLA emphasizes the importance of warfare in the electromagnetic spectrum† for conducting modern military operations. To that end, the PLA seeks to improve its capacity to conduct both defensive and offensive electronic warfare.‡<sup>211</sup> Defensively, the PLA has been hardening its various computer-based systems to withstand an opponent's electronic attacks.<sup>212</sup> For example, China's recent defense white paper notes that the PLA developed a networked communication system that relies more on fiber optical cable rather than on satellite or radio communications, thus weakening a potential opponent's ability to intercept PLA communications.<sup>213</sup> Offensively, the PLA is developing advanced electronic warfare capabilities in order to render a technologically superior opponent "deaf, dumb, and blind."<sup>214</sup> In addition, the PLA increasingly conducts field training exercises that emphasize the use of offensive and defensive electronic operations in order to improve the troops' ability to conduct and withstand electronic warfare operations.<sup>215</sup>

\*Jet engine combat fighters are generally categorized by generations according to their capabilities: 4th generation fighters (c. 1980s and 1990s) are equipped with sophisticated avionics and weapons systems and emphasize maneuverability over speed; 5th generation fighters (c. 2000) have a combination of advanced capabilities such as stealth, advanced radar, high-capacity data links, and supercruise capability. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), p. 77.

†The electromagnetic spectrum includes radio waves, microwaves, infrared, visible light, ultraviolet light, x-rays, and gamma rays.

‡Although a precise definition of electronic warfare is elusive, it generally implies any contested military action that involves the use of the electromagnetic spectrum. Electronic warfare is a crucial feature of military operations given the growing reliance of modern militaries on the electromagnetic spectrum for communications with friendly forces and identification, surveillance, and targeting of enemy forces. See, for example, Secretary of the Air Force, *Electronic Warfare*, Air Force Doctrine Document 2-5.1 (Washington, DC: U.S. Air Force, November 5, 2002); and Secretary of the Army, *Electronic Warfare in Operations*, Field Manual 3-36 (Washington, DC: U.S. Army, February 2009).

*Cyber warfare capabilities:* As a Commission-sponsored report previously noted, the PLA has a growing cyber warfare capability fueled in part by a belief that modern militaries, including the U.S. military, are overly reliant on networked computer systems to conduct combat operations. In the PLA's view, this creates an opening to be exploited in an effort to paralyze or degrade a superior opponent's combat capabilities.<sup>216</sup> A recent study by a U.S. think tank, the Center for Strategic and Budgetary Assessments, described how Chinese defense writings emphasize cyber attacks "against U.S. battle networks aimed at disrupting logistics, corrupting [command and control] systems, degrading fire control radars, denying essential services, and degrading U.S. counter-space control, space situational awareness and space ground control stations."<sup>217</sup>

*Counterspace capabilities:* As section 3 of this chapter details, the PLA has sought to develop its abilities to deny the use of space to a technologically superior opponent. Describing the reasoning behind the PLA's drive for counterspace capabilities, General Deptula wrote:

*China recognizes the overwhelming advantage the US has in the space domain and its key role in our ability to collect, analyze and rapidly share data. They understand how dependent U.S. warfighters have become upon space products and services for commanding deployed troops, passing [intelligence, surveillance, and reconnaissance] data, and enabling precision targeting and engagement. China views that reliance as a significant, exploitable vulnerability and has written extensively about the subject in both open source journals and military doctrine. As a result, they are actively pursuing a comprehensive array of space and counterspace programs intended to degrade, disrupt, deny, or destroy our ability to gain and maintain access to the region in the event of a conflict.*<sup>218</sup>

*Joint operations:* According to Mr. Cooper, in 1999 the Chinese Communist Party emphasized that the PLA focuses on acquiring the ability to conduct joint operations\* as a means successfully to counter a more capable enemy.<sup>219</sup> In General Deptula's assessment, the ability successfully to conduct joint operations will strongly improve the PLA's overall combat capacity.<sup>220</sup> Currently, the PLA's ability to conduct joint operations remains a work in progress. However, Mr. Cooper described in detail three ways in which the PLA is currently attempting to improve its ability to do so:

- Deploy a command system that integrates into one networked system the PLA's disparate command and control, communications, electronic warfare, targeting, and logistics systems.

\* Joint operations are a form of military operations that involve two or more separate military services working to conduct highly integrated combat operations where the synthesized combat power is more than the individual capabilities simply added together. A textbook example of a joint operation is Operation Desert Storm (1991), where the U.S. military and coalition forces expelled occupying Iraqi forces from Kuwait. See, for example, Joint Chiefs of Staff, *Joint Military Operations Historical Collection* (Washington, DC: Department of Defense, July 15, 1997), pp. V-1—V-15.



- Implement the necessary organizational changes for joint operations, such as developing a more flexible command and control structure.
- Develop a cohort of military personnel capable of conducting joint operations. For example, in its 12th Five Year Plan (2011–2015), the PLA leadership determined that joint training would be a major goal for the military.<sup>221</sup>

*“Three Warfares” Strategy:* Since 2003, the PLA has been developing the ability to integrate public media, international law, and psychological warfare in support of its Area Control Strategy. Dean Cheng, a research fellow at The Heritage Foundation, described to the Commission how this strategy, collectively referred to in Chinese defense writings as the “Three Warfares,” seeks to undermine the opponent’s will to fight, weaken international support for the opponent’s cause, and reinforce China’s domestic support for military operations. Reflecting the PLA’s emphasis on offensive operations, Mr. Cheng noted that this strategy would likely be deployed prior to the actual outbreak of hostilities.<sup>222</sup> The three individual components of this strategy include the following:

- Psychological warfare, which targets the leadership and population of the opponent, of third parties, and domestically in China;
- Public opinion warfare, where China would use “various mass information channels, including the Internet, television, radio, newspapers, movies, and other forms of media” to guide domestic and international public opinion in a way favorable to Beijing; and
- Legal warfare, which relies on the “use of domestic law, the laws of armed conflict, and international law” to demonstrate that China actions are legal, and the opponent is violating the law.<sup>223</sup>

### Implications for the United States

China’s Area Control Strategy has several implications for the United States and the Asia-Pacific Region. First, because the central tenet of the PLA’s Area Control Strategy is to provide a means to defeat a superior military, many of the PLA’s emerging capabilities appear intended directly to counter U.S. and allied military capabilities and exploit an opposing military’s weaknesses. As Ms. Mastro noted:

*China is fielding capabilities designed to deter, deny, disrupt, and delay the deployment of U.S. forces into the theater in the case of a conflict. China seeks to capitalize on U.S. vulnerabilities, specifically the great distances the U.S. needs to travel to engage China militarily as well as U.S. reliance on unimpeded access to and use of ports, airfields, air and sea bases, and littoral waters.*<sup>224</sup>

U.S. military capabilities and military bases long thought to be beyond the PLA’s reach are increasingly vulnerable without proper countermeasures. According to Mr. Cooper, “China’s greatly im-



proved detection, tracking, targeting, and long-range missile systems will soon pose a very real threat to U.S. carrier groups operating to the west of Guam.”<sup>225</sup> Jim Thomas, vice president for Studies, Center for Strategic and Budgetary Assessments, described how “the steady expansion of China’s maritime reconnaissance-strike complex is creating ‘no-go zones’ in the Western Pacific, gradually eroding America’s ability to project military power into a region of longstanding vital interest.”<sup>226</sup> The Commission noted in its 2010 Report that all six U.S. air bases in East Asia are vulnerable to PLA air and missile attacks.\*<sup>227</sup> Summarizing the effects of what improved PLA area control capabilities could mean for U.S. military operations in East Asia, General Deptula provided the following prediction:

*U.S. operations, both air, missile and maritime, from mainland Japan, Okinawa, and the Philippines will be severely impacted. The PLA will likely be able to degrade and/or deny U.S. air- and space-based surveillance and reconnaissance capabilities in the region. Command and control of deployed U.S. forces will likely be disrupted, and it will be more difficult to logistically support operations in the western Pacific. It is also likely that U.S. aircraft carriers will be forced to operate at distances far from the PRC [People’s Republic of China] mainland.*<sup>228</sup>

#### **Example of a Possible PLA Cyber Attack Against the U.S. Military**

In testimony to the Commission, Martin C. Libicki, a senior management analyst at the RAND Corporation and a well-known expert on cyber warfare, described to the Commission a plausible scenario where the PLA undertakes offensive cyber operations against the U.S. military in an attempt to disrupt U.S. deployment of forces to the western Pacific. In his scenario, the Chinese Communist Party decides to retake Taiwan forcefully and anticipates that the United States will intervene on behalf of the island. According to Dr. Libicki:

*China takes steps to complicate and hence delay the U.S. transit of the Pacific, so that by the time the United States does arrive, the war [with Taiwan] will be over, or at least the Chinese will have a secure lodgment on the island. So, [PLA forces] carry out a full-fledged operational cyberattack on the United States military information systems with the hopes of turning data into unusable nonsense.*<sup>229</sup>

\*These bases include Osan and Kunsan Air Bases in South Korea; Kadena, Misawa, and Yokota Air Bases in Japan; and Andersen Air Force Base on Guam. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), p. 90.

**Example of a Possible PLA Cyber Attack  
Against the U.S. Military—Continued**

In particular, he suggested that a prime target for the PLA might be the U.S. military's logistics data system, referred to as the time-phased force and deployment data.<sup>230</sup> Although the data are stored and transmitted over unclassified networks, they "provide detailed information about what gets moved, conveyances, routes, and start and stop times."<sup>231</sup> If the PLA were able to intercept, disrupt, or obstruct these data, it could result in serious implications for U.S. warfighters. However, it is important to note that, according to a Commission-contracted study, the PLA appears to be aware that a cyber attack on the U.S. military's logistics system would not cause the military to be unable to function. Rather, it is seen as one method to slow or hinder the deployment of U.S. forces into the region.<sup>232</sup>

Second, because it posits the need to exert control over a growing area of the western Pacific, the PLA's Area Control Strategy increasingly impacts other regional actors, not just the United States and Taiwan. During the Commission's May 2011 meeting with scholars from the East-West Center in Hawaii, the center's Senior Fellow Denny Roy noted that military threats are one way that China seeks to establish a "sphere of influence" in East Asia, especially Southeast Asia.<sup>233</sup> General Deptula pointed out how improved PLA area control capabilities are:

*a growing threat to the U.S. and other countries in the region. These augmented capabilities can be used in coercive diplomacy and to contest territorial disputes by force, or threat of force. Increasingly, the PRC is focusing on developing capabilities that project power throughout the region, enhancing China's position in Asia and the world military hierarchy.*<sup>234</sup>

Robert F. Willard, commander of the U.S. Pacific Command, echoed this sentiment when he stated in December 2010 that:

*[China's] anti-access/area denial systems, more or less, range countries, archipelagos such as Japan, the Philippines and Vietnam, so there are many countries in the region that are falling within the envelope of this, of an [anti-access/area denial] capability of China. That should be concerning, and we know is concerning, to those countries. While it may be largely designed to assure China of its ability to affect military operations within its regional waters, it is an expanded capability that ranges beyond the first island chain and overlaps countries in the region. For that reason, it is concerning to Southeast Asia, and it remains concerning to the United States.*<sup>235</sup>

Furthermore, were the PLA to have the capacity to control major portions of the western Pacific, it could allow China to exert more influence throughout the region (see figure 2, below). Beijing could use PLA area control capabilities to deny states access to regional

maritime resources, such as underwater oil and natural gas in the South and East China Seas. Beijing could also pressure regional actors by threatening or conducting a blockade of major sea lanes traversing the region. Possession of additional land features outside of China's recognized maritime borders could further extend PLA capabilities to project force throughout the region by allowing the PLA to establish military-relevant platforms, such as sensors and supply depots, deeper into the East and South China Seas. In the event of a conflict, China could also use the military's area control capabilities to deny regional and outside actors the ability to operate in the international bodies of water located within the First Island Chain.

**Figure 2: Portions of the Western Pacific Most Vulnerable to Chinese Area Control Capabilities**



Source: Roger Cliff et al., *Entering the Dragon's Lair: Chinese Anti-Access Strategies and Their Implications for the United States* (Arlington, VA: RAND Corporation, 2007), p. 112.

Finally, the opaque nature of Beijing's views of what constitutes hostilities, coupled with the PLA's inclination toward offensive operations, could result in a serious miscalculation and inadvertent conflict in the region. The crux of this argument centers on the notion of deterrence, which seeks to persuade through the threat of force "a potential enemy that he should in his own interest avoid courses of activity."<sup>236</sup> However, because of the PLA's tendency to strike first, Beijing could cause a conflict to escalate dramatically. For example, General Deptula noted that "Chinese leaders might consider preemptively attacking U.S. forces as they are deploying to a region in what U.S. policymakers intend as an action to *deter* a conflict" [emphasis in original].<sup>237</sup> The 1995–96 Taiwan Strait Crisis, where Beijing attempted to intimidate Taiwan to reject fur-

ther moves toward independence, provides the historical backdrop for an example of how this could play out. Beginning in mid-1995, the PLA conducted a series of military exercises a short distance from Taiwan's territory. Just prior to Taiwan's presidential election in March 1996, the PLA again carried out military exercises, this time a series of live-fire missile tests that targeted the waters just outside of two major Taiwan ports. In response, then President Clinton dispatched two aircraft carriers to the region to demonstrate Washington's resolve to maintain stability. Subsequently, tensions between all sides diminished without the outbreak of conflict.<sup>238</sup> If this scenario were repeated today, however, China's capabilities to respond would be much greater than they were in 1996.

### **Conclusions**

- The PLA's military strategy is best described as an Area Control Strategy. At its core, this strategy seeks to provide guidance to the PLA on how to defeat a technologically superior opponent.
- In order to defeat a superior opponent, the Area Control Strategy emphasizes degrading an opponent's technological advantages; striking first in a conflict; and establishing military control over China's periphery, especially the maritime region off of China's eastern coast.
- Many of the PLA's force modernization efforts reflect China's Area Control Strategy. As a result, the PLA is acquiring capabilities that allow it to conduct surprise attacks aimed at degrading a superior military's advantages and preventing an opponent from effectively operating along China's periphery.
- Many of the PLA's evolving capabilities appear aimed at directly countering U.S. military capabilities or to exploit potential weaknesses in U.S. military operations. In addition, as the PLA expands its force projection capabilities, China's Area Control Strategy and supporting means will increasingly impact regional states. Finally, the heavy focus on offensive operations inherent in the PLA's Area Control Strategy could serve to undermine stability in the region.

## SECTION 3: THE IMPLICATIONS OF CHINA'S CIVIL AND MILITARY SPACE ACTIVITIES

### Introduction

Decades of high prioritization and steady investment from Chinese leaders, coupled with incremental indigenous achievements by Chinese scientists and engineers, place China among the top space powers in the world today.\* Qualitatively, China's space industries now produce state-of-the-art systems for certain applications, such as guided weapons that use space assets for targeting. Quantitatively, numerous active programs continue to increase China's inventory of satellites and other space assets. China's capabilities still generally lag behind those of the United States, Russia, and perhaps other nations by some measures. But of note, particularly as many nations' space programs proceed with relatively modest goals, China's civil and military space programs are in the ascendancy, in some cases on a steep trajectory.

Commission research and hearings held over the past year found that the implications of this trend for the United States and the rest of the world depend considerably on how the Chinese government seeks to use its increasingly robust space capabilities. Official statements emphasize reasonable and nonthreatening goals: prestige, scientific experimentation, exploration, and the attendant commercial and economic benefits. However, the substantial role the People's Liberation Army (PLA) plays in most facets of China's space activities demonstrates their heavily military orientation. Notwithstanding the inherently dual-use nature of many space activities, programmatic decisions such as concerted investment in counterspace technologies also indicate the centrality of military objectives. This raises questions about the Chinese government's willingness to be a responsible actor in the space domain. Threats to space infrastructure, particularly massive, orbital debris-creating events like the PLA's 2007 antisatellite demonstration (discussed below), have the potential to deny the benefits of space activities and technologies to the entire international community.

### Basic Features

China's space capabilities are advancing on several fronts. Information about China's current, space-related infrastructure illus-

---

\* Although subjective, space program capabilities and expenditure levels suggest that the term "space powers" would also include the United States, Russia, Japan, and the European Union. For figures, see The Space Foundation, "The Space Report 2011" (Colorado Springs, CO: 2011), p. 42; and Union of Concerned Scientists, "UCS Satellite Database (through 4/30/11)" (Cambridge, MA: 2011). [http://www.ucsusa.org/nuclear\\_weapons\\_and\\_global\\_security/space\\_weapons/technical\\_issues/ucs-satellite-database.html](http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html).

trates the depth of China's space programs. Three areas in particular bear mentioning: terrestrial infrastructure, launch vehicles, and satellites.

### ***Terrestrial Infrastructure***

Ground-based infrastructure enables all space operations. China has three active launch sites, located in Jiuquan, Gansu Province; Xichang, Sichuan Province; and Taiyuan, Shanxi Province (see figure 1, below). A fourth site is under construction at Wenchang, Hainan Island, and could become operational by 2013. In addition to these facilities, China operates two mission control centers: the Beijing Aerospace Flight Control Center, used for manned flight and lunar missions; and the Xi'an Satellite Telemetry and Control Center, used for tracking and controlling satellite data. Finally, an overseas tracking station in Swakopmund, Namibia, and four PLA-operated space tracking ships provide greater coverage areas for particular missions.<sup>239</sup>

**Figure 1: China's Operational Terrestrial Space Infrastructure \***



TT&C: Telemetry, Tracking, and Command. (Ship placement is for illustrative purposes only.)

Source: Globalsecurity.org, "Chinese Space Facilities," undated. <http://www.globalsecurity.org/space/world/china/facility.htm>.

\* Domestic and maritime infrastructure only.



### ***Launch Vehicles***

In 2010, China conducted 15 successful satellite launches, as many as the United States and behind only Russia, according to testimony to the Commission by Clay Moltz, associate professor at the Naval Postgraduate School.<sup>240</sup> China relies primarily on the Chang Zheng (“CZ,” or “Long March”) family of rockets to launch objects into orbit. Although less capable than some American, European, and Russian launch vehicles, the Chang Zheng has amassed an impressive reliability rate.\* A new variant of the vehicle, the CZ-5, could enter service as soon as 2014, according to a Commission-sponsored report on China’s aerospace industry.<sup>241</sup> In contrast to this program, China has experienced substantial setbacks with its next-generation family of rockets, called Kaituozhe (“KT,” or “Pioneer”). Though the Pioneer has been in development since 2000, two out of a possible five tests have failed, and the future of the program remains uncertain.<sup>242</sup>

### ***Satellites***

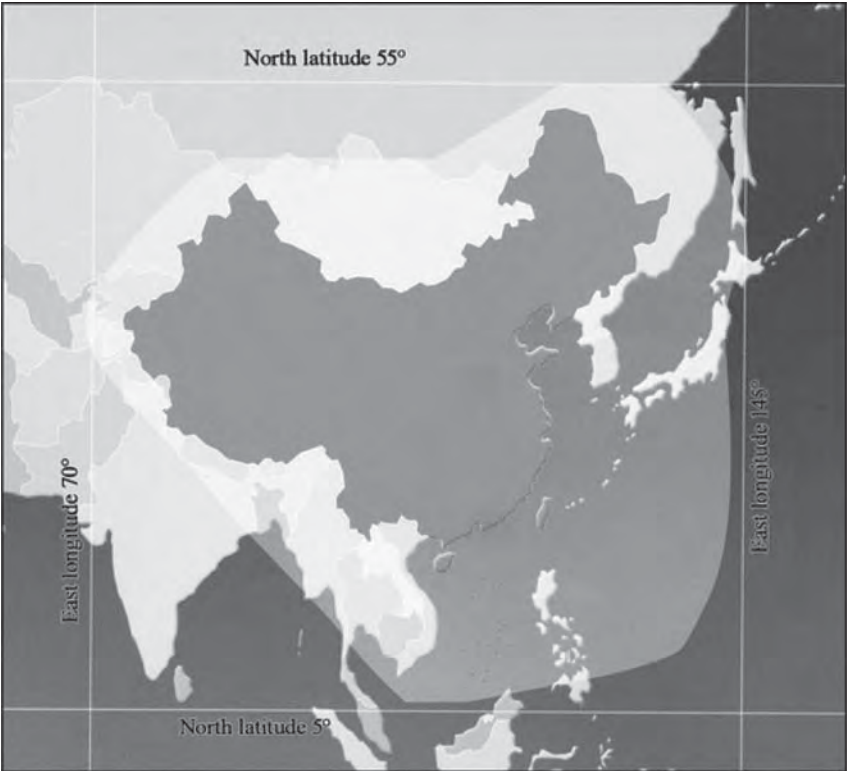
China controls approximately 70 satellites.† Chinese civil entities and state-owned enterprises (or commercial entities that involve state-owned enterprises), operate about 13, and other government or military entities control the remainder.<sup>243</sup> China’s satellites fill numerous roles, including a variety of experimental functions; communications and data relay; earth observation; weather; imagery and reconnaissance; synthetic-aperture radar; and potentially signals intelligence or electronic intelligence.<sup>244</sup> In addition, an indigenous satellite navigation capability (similar to the U.S. Global Positioning System) appears to be a high priority for Beijing, which is developing a comparable system called Beidou. Beidou-1, an experimental constellation, currently provides limited coverage (see figure 2, below). Beidou-2, a follow-on system that already includes nine operational satellites, should provide regionwide coverage from 12 satellites by 2012. By 2020, the system intends to provide global coverage with 35 satellites (see table 1, below).<sup>245</sup>

---

\* Since a string of failures from 1992 to 1996 (after which American firms offered troubleshooting advice) the CZ has had only two failures: one in 2009 and one in 2011. There are some discrepancies about the CZ’s precise success rate over the life of the program. By one count, there have been 132 CZ-2, -3, and -4 launches since 1974. Of those, only seven, or about 5.3 percent, failed. This includes not just catastrophic failures but also those in which the payload failed to reach its intended orbit (in some cases, a satellite in the wrong orbit can still perform certain functions). For information about the involvement of American firms with the CZ program in the early and mid-1990s, see Shirley A. Kan, “China: Possible Missile Technology Transfers Under U.S. Satellite Export Policy—Actions and Chronology” (Washington, DC: Congressional Research Service, updated October 6, 2003). [http://assets.opencrs.com/rpts/98-485\\_20031006.pdf](http://assets.opencrs.com/rpts/98-485_20031006.pdf). For information about CZ failures in 2009 and 2011, see Stephen Clark, “Chinese rocket fails to orbit experimental satellite,” *Spaceflight Now*, August 18, 2011. <http://spaceflightnow.com/news/n1108/18longmarch/>. For data on the CZ’s success rate, see Ed Kyle, “2011 Space Launch Report,” *Space Launch Report*, September 18, 2011. <http://www.spacelaunchreport.com/log2011.html#rate>.

† By way of comparison, the United States controls over 450 satellites, Russia controls over 100, and Japan controls over 40. See Union of Concerned Scientists, “UCS Satellite Database (through 4/30/11)” (Cambridge, MA: 2011). [http://www.ucsusa.org/nuclear\\_weapons\\_and\\_global\\_security/space\\_weapons/technical\\_issues/ucs-satellite-database.html](http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html).

**Figure 2: Representation of Beidou-1's Coverage Area**



Source: Junping Zhao et al., “The Design and Implementation of a Rescue Terminal with Vital Signs Telemonitoring Based on Beidou 1 Navigation Satellite System,” *Telemedicine and e-Health* 2:17 (March 2011): 76–79.

**Table 1: Select Chinese Satellites (operational only)**

Type	Series	Quantity
Communications	Dongfanghong 3, 4	6
Weather	Fengyun 1, 2, 3	5
Civilian Earth Observation	China-Brazil Earth Resources 2	1
	Huanjing 1	2
	Haiyang 1	1
Military Reconnaissance	Fanhui Shi Weixing*	—
	Ziyuan	3
	Yaogan 2, 3, 4, 5, 6, 7, 8, 9, 10	9
Satellite Navigation	Beidou 1, 2	11

**Table 1: Select Chinese Satellites (operational only)—Continued**

Type	Series	Quantity
Other	Shijian 6, 7, 11, 12	9
	Beijing 1	1
	Chuangxin 1	1
	Shiyan 1, 2, 3	3
	Naxing 1	1
	Zheda Pixing 1	3
	Xiwang 1	1

\* Five different models exist and are used on a temporary basis. Together, they have flown 22 missions ranging between 18 and 27 days.

Source: Roger Cliff, Chad J.R. Ohlandt, and David Yang, “Ready for Takeoff: China’s Advancing Aerospace Industry” (contracted research paper for the U.S.-China Economic and Security Review Commission, 2011). [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf). Satellite navigation quantities updated to reflect subsequent launches.

## Civil Space Activities

This subsection provides background information on China’s civil space activities. It discusses China’s strategic approach to civil space and the space sector’s organizational features. It then surveys China’s recent developments and accomplishments. Finally, it discusses some apparent limitations.

### Strategy

China’s leadership views all space activities through the prism of “comprehensive national power,”<sup>246</sup> a construct that seeks to measure nations’ relative strength in politics, economics, military capabilities, science and technology, and foreign affairs.<sup>247</sup> China’s most recent official white paper on space, released in 2006, characterizes space development efforts “as a strategic way to enhance” China’s standing in these areas.<sup>248</sup> Parallel to its military efforts (described below in the “Military Space Activities” subsection), Beijing has put forward initiatives in each area.

*Politics:* China’s space endeavors serve to bolster the nation’s standing both at home and abroad. For domestic purposes, “the [Chinese] government is using civil space activities to promote its legitimacy in the eyes of its people,” according to Dr. Moltz.<sup>249</sup> Space activities for external consumption have both symbolic and concrete rationales. For example, Scott Pace, director of The George Washington University Space Policy Institute, testified that “Chinese astronauts are helpful to promoting the China ‘brand’ in promotional videos and international conferences.”<sup>250</sup> More directly, “Conspicuous and autonomous achievements in space also reinforce China’s great power status and its membership in the elite club of advanced spacefaring countries,” according to testimony to the Commission by Alanna Krolikowski, visiting scholar at The George Washington University Space Policy Institute. She continued, “Achieving significant space capabilities ensures that China will have a ‘seat at the table’ when decisions about space are made.”<sup>251</sup>

China's leadership appears to value space exploration's inherent prestige, for both domestic and external audiences, above any potential economic benefits. Ms. Krolikowski testified that:

*The areas of space technology known to generate the most direct and reliable contributions to economic development are those with concrete applications, such as telecommunications satellites and remote-sensing satellites for resource management and weather monitoring. ... In China, over the past two decades, resources devoted to civil space have been concentrated not in these relatively productive areas, but in a costly human spaceflight engineering program of no evident direct benefit to the national economy. The symbolism of human spaceflight has been an important driver of this effort.*<sup>252</sup>

**Economics:** China's economy benefits from the country's national space programs, regardless of certain programmatic decisions that emphasize prestigious accomplishments. Numerous firms, chiefly state-owned conglomerates (described below in the "Organization" subsection), engage in the research and development, design, engineering, production, launch, and maintenance of space and space-related systems. The firms employ over 200,000 people and produce systems with commercial applications. Ms. Krolikowski noted that "China is entering a phase of space-sector development during which even greater emphasis is placed on the commercialization of space technology."<sup>253</sup> Space technology also has spin-off benefits for other industries; for example, "[r]equirements for human space flight are used to improve the quality control of Chinese industries," according to Dr. Pace.<sup>254</sup> Finally, the use of space itself can have economic benefits, according to researchers at the China Institute for International Strategic Studies. During a 2010 Commission trip to China, researchers at the institute explained that China's earth observation satellites can help the agricultural sector understand soil conditions and other environmental factors, which can aid in yielding more productive crops.\*

**Science and technology:** China's leadership recognizes the strategic value of space-related technologies. "High-end manufacturing and information technology, which include satellites and telecommunications, are among the seven new strategic sectors identified in the 2011–2015 [12th] Five Year Plan to receive policy support and public investment," according to Ms. Krolikowski. She testified that "[s]pace-related industries figure in government plans for building a knowledge economy, increasing domestic consumption, especially of high-technology products, fostering indigenous innovation, and building a sophisticated scientific, technical, and industrial base."<sup>255</sup> Beijing views science and technology development as inseparable from economic and defense imperatives (described above and below, respectively).<sup>256</sup>

**Foreign affairs:** China uses space cooperation and diplomacy to fulfill a range of space-related objectives and more general diplo-

---

\* Researchers also explained that Chinese scientists have found that seeds irradiated via exposure to space produce higher crop yields. (Director of Strategic Studies at the China Institute for International Strategic Studies), presentation to Commission, Beijing, July 28, 2010.

matic and foreign policy goals. China cooperates with other nations on various space projects in order to develop its domestic space capacity. A notable codevelopment project is the China-Brazil Earth Resources Satellite series, which include imagery capabilities sufficient for certain military applications.<sup>257</sup> China has also secured space-related components or systems from Russia, France, the United Kingdom, and Germany.<sup>258</sup> The United States and China have cooperated on space issues during several limited windows over the past 20-plus years.\* Recent discussions at U.S.-China summits and a high-level National Aeronautics and Space Administration delegation to China suggested new momentum.<sup>259</sup> However, Representative Frank Wolf (R-VA) testified to the Commission that recent legislation prohibits any further cooperation.†

A key Chinese foreign policy objective is to secure natural resources.‡ According to Dr. Pace, China's "[o]ffers of space technology to developing countries are used to secure access to needed raw materials for the Chinese economy."<sup>260</sup> Dr. Moltz testified that China's "space deals with Nigeria and Venezuela, for example, were motivated by Chinese interests in long-term energy security."<sup>261</sup> Ms. Krolikowski testified that:

*China's approach to space exports also leverages its firms' and government's unique advantage at operating in developing-world markets. Chinese satellite manufacturers are in a position to offer generous terms to buyers in developing countries, for whom price can be a decisive factor. Offering concessional financing terms, providing development assistance (formally or informally) tied to satellite purchases, and even accepting payment for satellites in barter has made it possible for China to create buyers of satellites where none previously existed.*<sup>262</sup>

Finally, a Chinese diplomatic objective is "to portray itself as a 'purveyor' of space know-how and technology to lesser-developed states in Asia and elsewhere," according to Dr. Moltz.<sup>263</sup> To this end, China founded the Asia-Pacific Multilateral Cooperation in Space Technology and Applications in 1992. In 2008, China led a subset of that group to form the Asia-Pacific Space Cooperation Or-

\*For a brief history of U.S.-China space relations, see Carl E. Behrens, "Space Launch Vehicles: Government Activities, Commercial Competition, and Satellite Exports" (Washington, DC: Congressional Research Service, March 20, 2006 (updated)), pp. 10–14. <http://www.fas.org/sgp/crs/space/IB93062.pdf>.

†The relevant section states that: "None of the funds made available by this division may be used for the National Aeronautics and Space Administration or the Office of Science and Technology Policy to develop, design, plan, promulgate, implement, or execute a bilateral policy, program, order, or contract of any kind to participate, collaborate, or coordinate bilaterally in any way with China or any Chinese-owned company unless such activities are specifically authorized by a law enacted after the date of enactment of this division. (b) The limitation in subsection (a) shall also apply to any funds used to effectuate the hosting of official Chinese visitors at facilities belonging to or utilized by the National Aeronautics and Space Administration." United States Congress, H.R. 1473, Section 1340, 112th Cong., 1st sess.; and U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, testimony of Frank Wolf, May 11, 2011.

‡For examples of the role of natural resources in China's foreign policy, see U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2010), pp. 128–30; and U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2009), pp. 216–18.



ganization, modeled on the European Space Agency.\* These groups allow China to facilitate its cooperation agenda.

### **Organization**

China's civil space organization includes the PLA, two state-owned conglomerates, and the China National Space Agency.

*People's Liberation Army:* The PLA plays a central role in civil space activities such as exploration. Consequently, "China does not have a fully separate civil space program in the model of NASA [National Aeronautics and Space Administration] and U.S. civil space activities," according to Dr. Pace. Manned space is also an essentially military function. Ms. Krolkowski testified that "[i]n civil space, the [General Armaments Department] acts mainly in and through the Manned Space Engineering Office, the entity responsible for the human spaceflight program." She also testified that individual military services serve certain functions. For example, the PLA Air Force conducts astronaut training and medical activities.<sup>264</sup>

*China National Space Agency:* Created in 1993 under the State Council, the China National Space Agency was intended by Chinese planners to become a National Aeronautics and Space Administration equivalent.<sup>265</sup> However, the China National Space Agency never gained control of many research and development, production, and operations functions executed by the military and defense industry.<sup>266</sup> The agency now mainly facilitates and executes international agreements and other aspects of international cooperation.<sup>267</sup>

*Space industrial base:* China's space industrial base is composed of two primary state-owned conglomerates: the Chinese Aerospace Science and Technology Corporation and the China Aerospace Science and Industry Corporation. The two organizations took their present form in 1999 when Beijing reorganized the space sector to create greater competition, according to a Commission-sponsored report on China's defense industries.<sup>†</sup><sup>268</sup>

- *China Aerospace Science and Technology Corporation.* The formation of this corporation brought together scores of research institutes and production complexes. China's National Medium- to Long-Term Plan for Development of Science and Technology (2005 to 2020) designated the corporation as one of 15 select, state-owned enterprises to receive special policy incentives and extra funds for research and development, accord-

\*Seven dues-paying members compose the Asia-Pacific Space Cooperation Organization: China, Bangladesh, Iran, Mongolia, Pakistan, Peru, and Thailand. According to Dr. Moltz, the group "engages in joint research and data-exchange efforts, as well as formal training courses for scientists and engineers from the Asian-Pacific region in space technology and remote sensing."

†Both China Aerospace Science and Technology Corporation and China Aerospace Science and Industry Corporation (described below) are currently subordinate to the umbrella organization, State Administration for Science, Technology, and Industry for National Defense, which, in turn, is subordinate to the "super"-Ministry of Industry and Information Technology. See U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011. Additionally, like other major state-owned enterprises, both entities are administratively subordinate to the State-owned Assets Supervision and Administration Commission of the State Council.



ing to a Commission-sponsored report on China's science programs.<sup>269</sup> The industrial giant primarily focuses on powerful launch vehicles and large satellites.<sup>270</sup> It includes entities such as the China Great Wall Industry Corporation, the organization that markets launch services and satellite systems to international clients, and the China Satellite Communications Corporation, which operates telecommunications satellites.<sup>271</sup>

- *China Aerospace Science and Industry Corporation*: Although smaller than its counterpart, this corporation is composed of 180 enterprises and employs over 100,000 people. It specializes in “tactical ballistic missiles, anti-ship and land attack cruise missiles, air defense missile systems, direct ascent anti-satellite (ASAT) interceptors, small tactical satellites and associated tactical satellite launch vehicles,” according to a report by the Project 2049 Institute. The China Aerospace Science and Industry Corporation appears to be the lead entity behind China's efforts to develop an antiship ballistic missile program, which seeks the ability to target moving vessels at sea.<sup>272</sup> (For more information on the antiship ballistic missile program, see the “Military Space Activities” subsection, below, as well as sec. 1 of this chapter.)

Most of these organizations operate within tightly controlled, vertically structured bureaucracies. Ad hoc steering groups, called “Leading Small Groups,” composed of prominent individuals from the leadership of relevant Chinese Communist Party, Chinese government, and corporate organizations, provide guidance and make decisions.<sup>273</sup> Chinese officials generally do not disclose the existence of such groups or their membership. However, space-specific, leading small groups reportedly exist for “lunar projects, human spaceflight, Earth observation satellites, and heavy-lift launch vehicle development,” according to Ms. Krolikowski.<sup>274</sup>

### **Notable Developments**

China's civil space activities have progressed at a cautious but steady rate. China's leadership values manned missions and focuses on that area. According to Dr. Pace, “It is not a question of whether China will have a full range of human space flight capabilities, but a question of when and what they intend to do with those capabilities.”<sup>275</sup> After successful manned missions in 2003, 2005, and 2008, the last of which included a space walk, China's space planners have identified a range of increasingly ambitious plans through the mid-2020s. China is currently developing a series of three small space laboratory modules that it plans to launch over the coming decade. The first of the series, “Tiangong-1,” launched in September 2011.<sup>276</sup> These laboratories will conduct research for, among other things, a future permanent space station. Though modest in size and scope in comparison to the International Space Station, China's planned space station will require substantial capabilities to orbit. The station will be composed of three separate modules—slated to launch in 2020, 2021, and 2022—that will need to rendezvous in space.<sup>277</sup> Like other aspects of China's manned space activities, the space station will be run by the PLA.<sup>278</sup>

China's leadership also places a high priority on lunar missions, which it views as perhaps the most visible and prestigious space-related accomplishment. Chinese experts and foreign observers anticipate several breakthroughs in China's lunar exploration activities over the next decade. Chinese planners describe lunar exploration in terms of three discrete stages. Stage one, which lasted from 2002 to 2007, involved orbiting the moon. Stage two, which began in 2008 and is set to conclude in 2014, involves a moon landing and the use of a rover to collect data from the lunar surface. Stage three, scheduled to take place from 2015 to 2020, involves the collection of samples from the lunar surface and their return to Earth.<sup>279</sup> A manned lunar mission (perhaps as "stage 4") may also take place as soon as 2024.<sup>280</sup> Dr. Pace testified that although "China does not publicly have a formal program for sending humans to the moon," they are "making progress toward acquiring the capabilities necessary to conduct such missions."\*

### **Limitations**

China's civil space endeavors face various constraints, including substantial bureaucratic and organizational inefficiencies. Chinese planners have yet to complete major systemic reforms, the most recent round of which began in 2008 and sought to "inject greater civilian management and innovation" into China's space industries, according to Dr. Moltz.<sup>281</sup> However, according to China space expert Eric Hagt, China's space industries remain "dispersed, bloated, and located in geographically isolated regions."<sup>282</sup> This is consistent with other Chinese state-run industries that, according to Dr. Moltz, "continue to suffer from legacy inefficiencies of the socialist economy."<sup>283</sup> These characteristics limit the potential for China's space developments to benefit other Chinese industries.<sup>284</sup>

### **The Advantages of State Control**

The numerous reorganizations of China's space sector indicate persistent dissatisfaction with industrial performance. However, state control provides China's space industrial base with certain advantages. For example, the entire sector "has been insulated from many of the pressures affecting the rest of the economy, mainly by its status as a strategic sector and its largely non-market internal relationships," according to Ms. Krolikowski. Benefits of this special status include "direct public investment in research and development; fiscal, tax, and financial policies to support major national [science and technology] projects and indigenous innovation; measures to improve market access; concessional pricing systems for land and utilities; and government oversight of mergers and acquisitions." Finally, benefits extend to predictable procurement trends, which allow China's space industrial base to forecast staffing, investment, and research and development needs. Ms. Krolikowski testified that:

\*For example, China's spacesuit "has boots with heels—and other features for walking on a surface as well as floating outside a spacecraft." See U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Scott Pace, May 11, 2011.

**The Advantages of State Control—Continued**

*[China's] space industry enjoys stable, predictable demand for its products from government customers and a stable space policy environment. CASC [China Aerospace Science and Technology Corporation] and CASIC's [China Aerospace Science and Industry Corporation] near- and long-term demand expectations are based on the Five-Year Plans and even longer-term national strategies. These companies do not contend with abrupt program changes and fluctuating budgets in the way firms in other countries do.*<sup>285</sup>

With respect to commercial activities, China faces potential obstacles for satellite sales and launch services. Notwithstanding China's efforts to replace a satellite it built for Nigeria, which failed in November 2008, the incident may cause reluctance on the part of future partners. Ms. Krolikowski testified that despite a "string of recent deals, expectations for Chinese satellite exports, especially beyond developing markets, remain modest. China's satellite-manufacturing industry is not yet internationally competitive."<sup>286</sup> China has also experienced setbacks in its launch services. While China's launch tempo increased substantially starting in 2010, failed Chang Zheng launches in August 2009 and August 2011 tarnished somewhat the impressive success rate that vehicle had achieved since the mid-1990s. Future deals based on these systems may be subject to higher insurance rates, which could marginalize the cost benefits of using Chinese systems.\* Higher costs, when combined with persistent delays in China's follow-on launch vehicle, may drive potential customers to look elsewhere for launch services, such as to Russia, Europe, or perhaps the United States.†

China's relative isolation from other major spacefaring nations serves as a further strategic limitation. Export controls, such as International Traffic in Arms Regulations, complicate China's participation in international space markets.‡ This includes foreign technology acquisition as well as China's ability to provide launch services for systems that contain controlled technologies. However, several International Traffic in Arms Regulations-free initiatives are underway or under discussion.§ Another factor that isolates

\* Roger Cliff, Chad J.R. Ohlandt, and David Yang, "Ready for Takeoff: China's Advancing Aerospace Industry," (contracted research paper for the U.S.-China Economic and Security Review Commission, 2011), p. 112. [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf). However, representatives of China Great Wall Industry Corporation told the Commission during the Commission's 2011 trip to China that the firm's insurance rates are comparable to those of international competitors.

† Representatives of China Great Wall Industry Corporation also told the Commission that potential international competitors for launch services include firms such as Proton, Arianne, and SpaceX.

‡ The International Traffic in Arms Regulations, administered through the U.S. Department of State, control the permanent and temporary export (and temporary import) of certain defense articles and services. See U.S. Department of State, "The International Traffic in Arms Regulations (ITAR)," (Washington, DC: updated January 21, 2009). [http://www.pmddtc.state.gov/regulations\\_laws/itar.html](http://www.pmddtc.state.gov/regulations_laws/itar.html).

§ For different assessments about the state of (and prospects for) the "ITAR [International Traffic in Arms Regulations]-free" industry, see U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011; and U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

China, according to Dr. Moltz, is the nation's lack of close allies and partners in space endeavors. He testified that "[w]hile [China] cooperates with Russia, the two sides do not share strategic interests, and the bulk of China's cooperative agreements involve developing countries."<sup>287</sup> As a result, China could not necessarily rely on any other country to provide support in the event of a crisis.<sup>288</sup>

### **Military Space Activities**

This subsection describes China's military space activities. It discusses China's strategic approach to military space operations and the Chinese military's organizational features as they relate to space operations. It also describes China's recent developments and initiatives. Finally, it highlights some current limitations on China's military space programs.

#### **Strategy**

Several obstacles prevent outsiders from truly understanding China's military space activities. According to testimony by Bruce MacDonald, senior director of the Nonproliferation and Arms Control Program at the U.S. Institute of Peace, "[a] fundamental problem we face is that China says little at an official level about its military space policy and doctrine."<sup>289</sup> It is clear, however, that China's leadership recognizes the growing importance of space, as well as the domain's military utility. For example, President Hu Jintao in late 2004 issued a new set of missions to the PLA, which included the requirement to protect China's expanding national interests in space.<sup>290</sup> Official operational information is similarly rare. According to testimony to the Commission by Dean Cheng, research fellow at The Heritage Foundation, the lack of available information is so complete that "there is still no indication of whether the PLA has developed a formal space doctrine governing military operations in space."<sup>291</sup>

Authoritative Chinese military publications, however, provide some insight into China's strategic thinking. The book *Military Astronautics*, by Chang Xianqi, a major general in the PLA, serves as a key example. The text explains two critical, space-related "guiding ideas." \* First, China should seek "space supremacy," defined as "the power to control a certain area of space for a certain period of time." † In this context, the PLA would use communications, reconnaissance, and related activities for the purposes of enhancing its ability to conduct operations. Simultaneously, China would conduct offensive and defensive space operations to attack and defend space-based and terrestrial military targets. The text subsequently describes space supremacy as a "precondition to seizing air suprem-

\* Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005). OSC ID: CPP20091231572001. The source describes these guiding ideas as "anticipatory in nature." However, China's counterspace programs increasingly provide tools to implement such concepts. For a fuller description of these ideas and their implications, see U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Dean Cheng, May 11, 2011.

† The source alternatively uses the term "space control." Major General Chang characterizes space supremacy as relative, asserting that "the side which has space supremacy usually can only expect that the other side's interference will not undermine its operational plan, but cannot expect that the other side will be completely unable to respond." Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005). OSC ID: CPP20091231572001.

acy, sea supremacy, and ground supremacy, and a key to seizing and maintaining the initiative on the battlefield, thus directly affecting the process and outcome of the war.”<sup>292</sup>

Second, China’s military should seek to integrate all available means into military space operations, according to *Military Astronautics*. This idea manifests in numerous ways. For example, with respect to actors, China “should break the boundaries between the military and the civilian, and implement unified planning, unified commanding, and unified coordinating of the military, civil, and commercial space powers.” In addition, it means China should strive to conduct simultaneous and mutually reinforcing offensive and defensive actions.\*

These guiding ideas are supplemented by several “basic principles” for space operations. Notably, these principles advocate that China take the initiative in offensive space operations; attack key points in vulnerable systems; and use stealthy, abrupt actions, among other things. According to analysis by Mr. Cheng, these concepts and principles “suggest that, in the event of a Sino-American confrontation, the PLA would seek to engage American space systems early in the crisis.”<sup>293</sup> Conceptually, these strategies align with China’s larger military imperatives for area control. (For more information, see chap. 2, sec. 1: “China’s Area Control Strategy.”)

### **Organization**

The PLA dominates China’s space activities. According to Mark Stokes, executive director of the Project 2049 Institute, “[w]ithin a broad and fragmented [Chinese Communist Party] and government policy framework, the PLA plays a central role in coordinating, defining, and managing national space requirements.”<sup>294</sup> On an operational level, “[c]ritical space infrastructure, including existing launch facilities, and the day-to-day management of civil space operations, especially in the human spaceflight program, are the responsibility of PLA organs,” according to Ms. Krolikowski.<sup>295</sup> Select PLA administrative (“headquarters-level”) entities and service-level entities play a role in China’s space programs.

*Headquarters-level entities:* The PLA headquarters organization consists of four components: the General Staff Department, the General Political Department, the General Logistics Department, and the General Armaments Department. Specifically, the General Staff Department and the General Armaments Department have space interests. According to Mr. Stokes, “[f]unctional offices within the [General Staff Department] shape operational requirements for militarily relevant space-based sensors, aerospace surveillance systems, and communications satellites.”<sup>296</sup> In addition, “[t]he PLA’s [General Armaments Department] oversees the development and acquisition of technical solutions to satisfy [General Staff Department] operational requirements, and manages launch, tracking, and control of civilian and military satellites and other orbital systems.”<sup>297</sup> Ms. Krolikowski testified that “[w]ithin the PLA, the

---

\*Note that in Chinese usage, the terms “offensive” and “defensive” describe mission types rather than specific means. For example, both types of missions might leverage reconnaissance assets or antisatellite weapons. This differs from typical western usage, which considers most counterspace weapons to be offensive tools.



[General Armaments Department] plays the most important role in space activities.”<sup>298</sup>

*Service-level entities:* The PLA Air Force, the Second Artillery,\* and the PLA Navy are primary customers of space-based systems.<sup>299</sup> Although they do not currently control China’s space assets, the PLA Air Force and Second Artillery in particular appear to seek some degree of operational control over military space activities. Roger Cliff, senior political scientist at the RAND Corporation, testified in 2010 that while “[t]he ultimate outcome of this bureaucratic contest is difficult to predict,” any change could alter the balance of space-related responsibilities within the PLA.<sup>300</sup>

#### **Congressional Remarks on China’s Space Programs**

In testimony to the Commission, Representative Frank Wolf (R-VA) discussed the importance of space and the character of China’s space programs. He stated that:

*Space is the ultimate ‘high ground’ that has provided the U.S. with countless security and economic advantages. . . . It should not be surprising that many countries have taken notice of the tremendous benefits that the American space program has yielded. It is clear that we are now entering an era of much greater civil, defense and commercial competition in space. Most countries expanding their space programs are strong U.S. allies that are primarily interested in advancing science research or building a commercial space industry. The Chinese [space programs], however, do not fall into this category.*

*What concerns me most about the Chinese space program is that . . . it is being led by the People’s Liberation Army (PLA). There is no reason to believe that the PLA’s space program will be any more benign than the PLA’s recent military posture.*<sup>301</sup>

#### **Notable Developments**

China’s military space-related activities appear focused on two areas: using space assets and other advanced sensors for guided weapons applications (“reconnaissance-strike complexes”) and using various means to disrupt, degrade, deny, and destroy adversary space assets (“counterspace” weapons). In each area, China’s military has demonstrated substantial improvements in the past several years.

*Reconnaissance-strike complexes.* China is developing combinations of advanced sensors and guided weapons to form systems commonly referred to as “reconnaissance-strike complexes.”† Spe-

\*Also known as the “Strategic Rocket Forces,” the Second Artillery is a service-level entity under the direct control of China’s Central Military Commission.

†U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Barry D. Watts, May 11, 2011. For a more thorough explanation, see Barry D. Watts, “Six Decades of Guided Munitions and Battle Networks: Progress And Prospects” (Washington, DC: Center for Strategic and Budgetary



cifically, China's military is working to "fuse data from an extensive and diverse sensor network," according to testimony by Wayne A. Ulman, China issue manager at the U.S. Air Force National Air and Space Intelligence Center.<sup>302</sup> This sensor network appears to include layers of systems: over-the-horizon radars, unmanned aerial vehicles, and remote-sensing satellites.\* Chinese analyses envision that satellites will play an important role in this architecture, as they would cue, or direct, other sensors in the network. Data from each layer, particularly once integrated, could be used to provide targeting data to guided weapons.<sup>303</sup>

Although the United States has the world's only combat-proven global precision strike capability, China is "the country that appears to be making the greatest strides toward fielding regional [reconnaissance-strike complexes]," according to Barry D. Watts, senior fellow at the Center for Strategic and Budgetary Assessments. Space plays a key role in this effort. For example, Mr. Watts testified that "to provide accurate, real-time target information for the ... antiship ballistic missile (ASBM), the Chinese [military has] been considering the integration of data from a variety of space-based sensors, including electro-optical (EO), synthetic-aperture radar (SAR), electronic reconnaissance, and ocean surveillance satellites" (see table 2, below).<sup>304</sup> China seeks to use data inputs from these systems, combined with data from other platforms within its sensor architecture, to correct antiship ballistic missiles' course after launch in order to target moving ships at sea. This system appears to be operational.†

**Table 2: Select Chinese Satellites with Potential Capabilities for Reconnaissance-strike Integration**

Satellite function	Explanation	Potential examples (quantity) type
<b>Electro-optical</b>	Collects imagery. Different platforms have different capabilities, but the Yaogan type may have a resolution of up to 0.8 meters.	(5) Yaogan (1) Shijian (1) CBERS <sup>1</sup>
<b>Synthetic-aperture radar</b>	Uses a microwave transmission to image objects. Effective on land or maritime targets day or night and in all-weather conditions. Can image ship wakes to determine speed and heading.	(4) Yaogan
<b>Electronic reconnaissance</b>	Potentially collects electromagnetic, acoustic, infrared, and/or radar signatures. Can be used to identify ships on that basis.	(6) Shijian <sup>2</sup> (1) Yaogan

Assessments, March 2007). <http://www.csbaonline.org/wp-content/uploads/2011/06/2007.03.01-Six-Decades-Of-Guided-Weapons.pdf>.

\* Unmanned aerial vehicles would include "conventional" platforms, perhaps on the model of the U.S. Global Hawk, as well as a separate class of promising high-altitude, long-endurance airships optimized for reconnaissance functions. See Mark Stokes, untitled draft research paper (prepared by the Project 2049 Institute for the U.S.-China Economic and Security Review Commission, forthcoming.)

† For more on China's antiship ballistic missile, see section 1 of this chapter.

**Table 2: Select Chinese Satellites with Potential Capabilities for Reconnaissance-strike Integration—Continued**

Satellite function	Explanation	Potential examples (quantity) type
<b>Ocean reconnaissance</b>	Also detects electronic emissions. Utilizes a combination of infrared sensors and collection antennas. The use of three satellites could locate an emitter based on triangulation.	(1) Yaogan (includes two subsatellites)

Note: This table is an attempt to assemble, collate, and analyze the limited available information on these platforms. Satellite types recur when different series within a given type are thought to host different sensors. Some of these satellites may host multiple types of sensors.

<sup>1</sup> This satellite is nominally under civilian control, but one electro-optical sensor has a high enough resolution to be militarily useful.

<sup>2</sup> Some of these satellites may have signals intelligence functions.

Sources: Roger Cliff, Chad J.R. Ohlandt, and David Yang, “Ready for Takeoff: China’s Advancing Aerospace Industry,” (contracted research paper for the U.S.-China Economic and Security Review Commission, 2011). [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf); Mark Stokes, untitled draft research paper (prepared by the Project 2049 Institute for the U.S.-China Economic and Security Review Commission, forthcoming.)

*Counterspace activities.* China seeks the capabilities to attack an adversary’s space systems in the event of conflict. In written testimony to the Commission, United States Air Force Lieutenant General (Retired) David A. Deptula described the rationale for this trend:

*China’s leaders probably view [antisatellite weapons] and offensive counterspace systems as force multipliers. As one Chinese defense analyst noted: ‘For countries that can never win a war with the United States by using the method of tanks and planes, attacking the US space system may be an irresistible and most tempting choice.’<sup>305</sup>*

To this end, the Chinese military has initiated numerous counterspace systems. On the basis of several tests over the past decade, some of the programs appear to be currently operational (see text box, below).

#### **China’s Antisatellite Capability Demonstrations**

*September 2005:* Media reports indicate that China has conducted satellite jamming tests.<sup>306</sup>

*August–September 2006:* China used a laser to temporarily blind (or “dazzle”) U.S. reconnaissance satellites, according to media reports.\* More recently, China dazzled French satellites, according to a European Space Agency official.<sup>307</sup>

\* For the original source, see Muradian Vago, “China Attempted To Blind U.S. Satellites With Laser,” *Defense News*, September 28, 2006. For an alternative interpretation, see Union of Concerned Scientists, “Satellite Laser Ranging in China” (Cambridge, MA: UCS Working Paper, January 8, 2007). [http://www.ucsusa.org/nuclear\\_weapons\\_and\\_global\\_security/space\\_weapons/technical\\_issues/chinese-lasers-and-us.html](http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/chinese-lasers-and-us.html). Note that even satellite laser ranging activities have counterspace applications.

**China's Antisatellite Capability Demonstrations—  
Continued**

*January 2007:* China conducted a direct-ascent antisatellite demonstration that used a ballistic missile to destroy an obsolete Chinese weather satellite, creating thousands of pieces of space debris. In April 2011, a piece of this debris came so close to the International Space Station that its occupants, concerned about the possibility of a collision, needed to take shelter in an escape capsule.<sup>308</sup>

*January 2010:* China conducted a kinetic energy (also called “hit-to-kill”) ballistic missile intercept. More difficult to execute than an antisatellite attack, this technology has clear antisatellite applications and “strategic implications for U.S. security interests,” according to Mr. MacDonald.<sup>309</sup>

*June–August 2010:* Two Chinese satellites conducted a series of orbital rendezvous maneuvers that appear to have included “bumping” into each other,” according to Mr. Cheng.<sup>310</sup> In describing this incident, General Deptula testified that “China could conceivably want to experiment with close space maneuvers, given its plans to build a space station. ... However, the lack of official Chinese information about the maneuvers has allowed room for speculation” that China actually demonstrated a coorbital antisatellite capability.\*<sup>311</sup>

None of these incidents involved prior notification or announcement,<sup>312</sup> and several have not been acknowledged officially.

Chinese military theorists take a holistic view of counterspace operations. They advocate for the use of both “soft” kill (i.e., informational, temporary, or reversible) attacks and “hard” kill (i.e., destructive or permanently disabling) attacks against every aspect of space power: ground-based systems, space-based systems, and communications links.<sup>313</sup>

*Ground-based systems:* According to *Military Astronautics*, “[d]estroying the enemy on the ground is the most effective way of seizing space supremacy.” This can be accomplished in several ways. “Hard” kill attacks could include air raids, missile attacks, or sabotage by special operations forces.<sup>314</sup> “Soft” kill attacks could include computer network exploitations or attacks directed against key ground facilities that interact with space-based assets (see text box, below).<sup>315</sup> The text identifies several key aspects to target, such as launch systems and command and control facilities.<sup>316</sup>

*Space-based systems:* *Military Astronautics* identifies two key methods to attack satellites: kinetic attacks and directed energy attacks. Kinetic attacks could include direct ascent antisatellite

\* However, it bears mentioning that western space firms are developing their own rendezvous capabilities in order to service satellites in orbit. Barry Watts testified that “these capabilities could also be used to neutralize satellites, thereby opening the door to the de facto weaponization of space.” U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Barry Watts, May 11, 2011.

weapons or coorbital satellite weapons. Such “hard” kill attacks, while effective, are immediately evident, easy to attribute, and create harmful debris. Therefore, the text identifies a preference for directed energy attacks, including various laser, microwave, particle beam, and low-power electromagnetic pulse weapons.<sup>317</sup> These attacks could take the form of either “hard” or “soft” kill, depending on the attack method and target. Key targets include power sources (e.g., batteries and solar panels), communications systems (e.g., transmission antennae), and sensors.<sup>318</sup>

*Communications links:* Critical information passes between ground- and space-based systems through electronic links, which are subject to electronic manipulation. This could take the form of either jamming or deception. Jamming includes different types of electronic interference or signals that flood communications channels, whereas deception involves the interception or forgery of transmissions to or from adversary space systems. Most of these attacks would fall into the “soft” kill category. However, deception allows the possibility for “hard” kills through self-destruction commands or measures designed to cause terminal loss of control.<sup>319</sup> Key targets for communications link attacks are the satellite uplink (which transmits information from ground stations to the satellite) and, more importantly from the Chinese perspective, the satellite downlink (which transmits information from the satellite to the ground station).<sup>320</sup>

#### **Malicious Cyber Activities Directed Against U.S. Satellites**

Malicious actors can use cyber activities to compromise, disrupt, deny, degrade, deceive, or destroy space systems. Exploitations or attacks could target ground-based infrastructure, space-based systems, or the communications links between the two.\* As noted above, authoritative Chinese military writings advocate for such activities, particularly as they relate to ground-based space infrastructure, such as satellite control facilities.

Satellites from several U.S. government space programs utilize commercially operated satellite ground stations outside the United States, some of which rely on the public Internet for “data access and file transfers,” according to a 2008 National Aeronautics and Space Administration quarterly report.† The use of the Internet to perform certain communications functions presents potential opportunities for malicious actors to gain access to restricted networks.

\*For an informed description of several potential vulnerabilities in space-related networks, see Stephen Farrell and Vinny Cahill, “Security Considerations in Space and Delay Tolerant Networks” (paper presented to the 2nd IEEE [Institute of Integrated Electrical Engineers] International Conference on Space Mission Challenges for Information Technology, 2006, esp. sec. 5).

†Sunny Tsiao, “The Enduring Legacy of the ‘Invisible Network’” (Washington, DC: NASA History Division, *News and Notes*, August 2008), p. 4. <http://history.nasa.gov/nltr25-3.pdf>.

**Malicious Cyber Activities  
Directed Against U.S. Satellites—Continued**

Notably, at least two U.S. government satellites have each experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems: \*

- On October 20, 2007, Landsat-7, a U.S. earth observation satellite jointly managed by the National Aeronautics and Space Administration and the U.S. Geological Survey, experienced 12 or more minutes of interference. This interference was only discovered following a similar event in July 2008 (see below).†
- On June 20, 2008, Terra EOS [earth observation system] AM-1, a National Aeronautics and Space Administration-managed program for earth observation, experienced two or more minutes of interference.‡ The responsible party achieved all steps required to command the satellite but did not issue commands.
- On July 23, 2008, Landsat-7 experienced 12 or more minutes of interference. The responsible party did not achieve all steps required to command the satellite.
- On October 22, 2008, Terra EOS AM-1 experienced nine or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands.

The National Aeronautics and Space Administration confirmed two suspicious events related to the Terra EOS satellite in 2008 and the U.S. Geological Survey confirmed two anomalous events related to the Landsat-7 satellite in 2007 and 2008.§

If executed successfully, such interference has the potential to pose numerous threats, particularly if achieved against satellites with more sensitive functions. For example, access to a satellite's controls could allow an attacker to damage or destroy the satellite. The attacker could also deny or degrade as well as forge or otherwise manipulate the satellite's transmission. A high level of access could reveal the satellite's capabilities or information, such as imagery, gained through its sensors. Opportunities may also exist to reconnoiter or compromise other terrestrial or space-based networks used by the satellite.

\* Unless otherwise noted, the following information is derived from a briefing the U.S. Air Force provided to the Commission on May 12, 2011.

† For information on the Landsat program, see James R. Irons, "The Landsat Program" (Washington, DC: National Aeronautics and Space Administration, updated September 20, 2011). <http://landsat.gsfc.nasa.gov/>.

‡ For information on the Terra program, see Marc Imhoff, "Terra" (Washington, DC: National Aeronautics and Space Administration, updated September 23, 2011). <http://terra.nasa.gov/>.

§ Name withheld (staff member, National Aeronautics and Space Administration), email interview with Commission staff, November 8, 2011; and Name withheld (staff member, U.S. Geological Survey), email interview with Commission staff, November 8, 2011.

**Malicious Cyber Activities  
Directed Against U.S. Satellites—Continued**

These events are described here not on the basis of specific attribution information but rather because the techniques appear consistent with authoritative Chinese military writings. For example, according to *Military Astronautics*, attacks on space systems “generate tremors in the structure of space power of the enemy, cause it to suffer from chain effects, and finally lose, or partly lose, its combat effectiveness.” One tactic is “implanting computer virus and logic bombs into the enemy’s space information network so as to paralyze the enemy’s space information system.”<sup>321</sup>

***Limitations***

Despite pockets of considerable capabilities, China has weak or moderate military space capabilities in other areas. China has few communications satellites available for military purposes, even assuming that the PLA would appropriate Chinese government-controlled assets during a crisis. Many PLA military platforms have modest bandwidth requirements, which, when combined with the PLA’s heavy reliance on buried fiber-optic military communications networks, may offset this disadvantage in the context of a potential, near-term U.S.-China contingency on China’s periphery. However, naval forces at sea and ground forces operating outside the Chinese mainland (even as close as Taiwan) would still require secure, mobile communications for military functions such as command and control.<sup>322</sup> New communications satellites or some functional equivalent, like unmanned aerial vehicles, could potentially fill this gap in coming years, depending on PLA investment priorities.

China has limited capabilities in other areas. It operates few weather satellites, which could pose a problem for Chinese military operations, particularly in the absence of information from other nations. China still lacks comprehensive satellite navigation capabilities, even within its own region, though the Beidou system is poised to close this gap over the next several years. China’s optical imagery satellites, while sufficient for many military applications, still offer lower resolution imagery than is available in commercial markets. Finally, several satellite and launch failures over the past few years have led to various program delays.<sup>323</sup>

**Implications for the United States**

The U.S. Department of Defense’s current approach to space, according to testimony by Gregory L. Schulte, deputy assistant secretary of Defense for space policy, “is designed to confront the ‘three C’s’—a space environment that is increasingly congested, contested, and competitive. China has contributed to all three.”<sup>324</sup>

***Congested***

Space, particularly low Earth orbit, is beset with natural and manmade objects. Quantities of manmade objects, including debris,



have increased dramatically over the past five years, beginning with China's 2007 antisatellite test. According to Ambassador Schulte, that test produced 14 percent of the approximately 22,000 manmade objects in orbit tracked by the U.S. Strategic Command, the entity responsible for U.S. space situational awareness. Strategic Command issues "conjunction warnings," or notices about potential collisions between these objects, to numerous commercial entities and foreign governments. Of the 1,983 conjunction warnings issued in 2010, approximately 700 related to potential collisions with debris from China's 2007 antisatellite test.<sup>325</sup> Even absent further kinetic antisatellite tests, China's increased space activities will continue to add to the congested nature of space. Launches leave behind rocket bodies, and satellites have finite life spans. These items can clutter useful orbits long after their operational lives.

### ***Contested***

Space is a domain of warfare in its own right and bolsters operational capacity in all other domains of warfare: land, air, sea, and cyberspace. In this context, China's advancements in military space functions present two primary implications for the United States. First, China increasingly leverages space assets for the purposes of force enhancement. As Mr. Cheng testified, "With each passing year, China's satellite constellations will provide better information to military users."<sup>326</sup> This information will benefit most aspects of China's military capabilities but will enhance in particular China's communications as well as intelligence, surveillance, and reconnaissance activities. As a corollary, China's reconnaissance-strike complexes, already advanced in some areas, appear poised to improve. This will lead not only to greater accuracy and reliability but also to the ability to attack a geographically extended range of targets. According to Mr. Stokes, "In a future contingency requiring U.S. intervention, space-enabled long-range precision strike assets could seek to suppress U.S. operations from forward bases in Japan, from U.S. aircraft battle groups operating in the Western Pacific, and perhaps over the next five to 10 years from U.S. bases on Guam."<sup>327</sup>

Second, China's counterspace programs seek the capability to compromise, disrupt, deny, degrade, deceive, or destroy U.S. space assets. These efforts could prevent the U.S. military's use of space for functions such as communications; intelligence, surveillance, and reconnaissance; and guided weapons applications. Notwithstanding China's increasing reliance on space for military and civil purposes, Chinese military planners still view space assets as an attractive target. Ambassador Schulte testified that with "geography the way it is, we are probably always going to find ourselves more reliant on space than [China] . . . so for the foreseeable future, that's an asymmetry they're going to look to exploit as they pursue an antiaccess/area denial approach."<sup>328</sup> According to General Deptula, "Continued Chinese investment in the design, development, deployment and employment of space and counterspace systems will increasingly challenge our traditional space dominance and could dramatically reduce our freedom of action in the event of a conflict in the region."<sup>329</sup>

### **Competitive**

According to Ambassador Schulte, “China’s nascent commercial space ambitions and increasing outreach to emerging spacefaring nations is a part of the more competitive nature of space.”<sup>330</sup> Additionally, China has several substantial goals for the mid-2020s. Some characterize as too modest U.S. plans over the same period. For example, Dr. Pace testified that:

*The United States appears to have forgotten the strategic value of a national human space flight program regardless of the existence of successful private endeavors. This may not have a near-term economic impact on the United States, as a robust range of unmanned programs will continue. However, the lack of visible U.S. leadership in human space flight may have serious foreign policy and international security impacts. It is a long-standing truism that the rules of international relations in new domains are created by those who show up and not by those who stay home.*<sup>331</sup>

Additionally, as noted above, China’s initiatives for the political, economic, science and technology-related, and diplomatic aspects of space yield a comprehensive view of the space domain and its prospects. For this reason, Dr. Moltz testified that:

*[V]iewing China’s space program solely from the perspective of its military activities is misleading. While China is active in the military sector and is seeking to check current U.S. advantages in the area, China’s challenge to the United States in space may eventually be equally significant in the civil space sector, where China’s expanding infrastructure, growing cadre of space scientists and engineers, and active international outreach puts it in a favorable position for long-term competition.*<sup>332</sup>

### **Conclusions**

- China is one of the top space powers in the world today. The nation’s capabilities, which are state of the art in some areas, follow from decades of substantial investment and high prioritization by China’s top leaders. The prestige of space exploration and the national security benefits of space systems serve as primary motivators for Chinese decisionmakers.
- China views all space activities in the context of “comprehensive national power.” This concept includes many dimensions, but military aspects are fundamental. The PLA’s primacy in all of China’s space programs, including nominally civil activities, illustrates this emphasis.
- China’s civil space programs have made impressive achievements over the past several decades. If Chinese projections hold, these programs are poised for continued accomplishments over the next ten to 15 years, such as the development of a space laboratory and eventually a space station. As part of an active lunar exploration program, China may attempt to land a man on the moon by the mid-2020s.

- China seeks new opportunities to sell satellites as well as satellite and launch services in international commercial space markets. Chinese firms' prospects for greater success in this field remain uncertain over the near term. However, China's international space-related diplomatic initiatives and their firms' ability to offer flexible terms on sales to developing countries may provide additional opportunities.
- In the military sphere, China appears to seek "space supremacy." The PLA aims to implement this policy through two tracks. First, they increasingly utilize space for the purposes of force enhancement. The best example is China's integration of space-based sensors and guided weapons. Second, they seek the capabilities to deny an adversary the use of space in the event of a conflict. To this end, China has numerous, active, counterspace weapons programs with demonstrated capabilities. China's military space and counterspace activities are part of a larger strategy for area control.

## RECOMMENDATIONS

### ***China’s “Area Control Military Strategy”***

The Commission recommends that:

- The relevant Congressional committees investigate the adequacy of security for the Department of Defense’s logistics data system, the time-phased force deployment data system, to ensure that the data therein are secure from a cyberattack.
- Congress assess the adequacy of Department of Defense capabilities to conduct major operations in a degraded command, control, communications, computer, intelligence, surveillance, and reconnaissance environment for an extended period of time.
- Congress direct the Government Accountability Office to evaluate the Department of Defense’s early warning systems to ensure that the department will have sufficient timely warning of a PLA attack in the event of a conflict.
- Congress require that the Department of Defense conduct periodic peaceful naval and air exercises in the East Asian maritime region to demonstrate the U.S. commitment to freedom of navigation.
- Congress assess the adequacy of funding for Department of Defense programs that ensure the military’s ability to operate effectively against China’s Area Control Strategy measures. Such programs could include, at a minimum, robust theater ballistic missile defense, antisubmarine warfare, advanced air-to-air combat, command and control, and electronic warfare capabilities.
- Congress encourage the administration to continue to work diplomatically and militarily with regional allies and friends to improve their capacity to resist China’s Area Control Strategy capabilities.

### ***The Implications of China’s Civil and Military Space Activities***

The Commission recommends that:

- Congress mandate that the Department of Defense (and other government space operators, as appropriate) assess and report upon their preparedness for potential Chinese counterspace activities. To the extent that commercial entities provide essential services, assessments should also cover their systems.

- Congress assess the adequacy and regularity of U.S. military exercises and training activities that simulate the destruction, denial, degradation, or manipulation of U.S. space assets. In addition, Congress should periodically evaluate whether the Department of Defense is taking sufficient measures to diversify its traditionally space-oriented capabilities, such as in navigation, communications, intelligence, surveillance, and reconnaissance.

## ENDNOTES FOR CHAPTER 2

1. Jeremy Page, "Test Flight Signals Jet Has Reached New Stage," *Wall Street Journal*, January 11, 2011. <http://online.wsj.com/article/SB10001424052748704515904576075852091744070.html>.
2. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), pp. 95–96.
3. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: Department of Defense, 2011), p. 32. See also Tai Ming Cheung, "What the J-20 Says About China's Defense Sector," *Wall Street Journal*, January 13, 2011. <http://blogs.wsj.com/chinarealtime/2011/01/13/what-the-j-20-says-about-chinas-defense-sector/?mod=rss> WSJBlog&mod=chinablog.
4. Nathan Hodge, "China's J-20 Fighter: Stealthy or Just Stealthy-Looking?" *Wall Street Journal*, January 19, 2011. <http://blogs.wsj.com/washwire/2011/01/19/chinas-j-20-fighter-stealthy-or-just-stealthy-looking/>; and Emmanuelle Tzeng and Bear Lee, "Experts doubt 'stealth' capability of Chinese fighters," Central News Agency, December 4, 2011. [http://focustaiwan.tw/ShowNews/WebNews\\_Detail.aspx?Type=aALL&ID=201101040034](http://focustaiwan.tw/ShowNews/WebNews_Detail.aspx?Type=aALL&ID=201101040034). For an alternate take on the J-20's design weaknesses, see Carlo Kopp, "An Initial Assessment of China's J-20 Stealth Fighter," *China Brief* 11:8 (May 6, 2011). [http://www.jamestown.org/uploads/media/cb\\_11\\_8\\_04.pdf](http://www.jamestown.org/uploads/media/cb_11_8_04.pdf).
5. GE Aviation, "GE and AVIC [Aviation Industry Corporation of China] Sign Agreement for Integrated Avionics Joint Venture," Press Release, January 21, 2011. [http://www.geae.com/aboutgeae/presscenter/systems/systems\\_20110121.html](http://www.geae.com/aboutgeae/presscenter/systems/systems_20110121.html).
6. GE Aviation, "GE and AVIC [Aviation Industry Corporation of China] Sign Agreement for Integrated Avionics Joint Venture," Press Release, January 21, 2011. [http://www.geae.com/aboutgeae/presscenter/systems/systems\\_20110121.html](http://www.geae.com/aboutgeae/presscenter/systems/systems_20110121.html).
7. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), p. 96.
8. Roger Cliff, Chad J.R. Ohlandt, and David Yang, *Ready for Takeoff: China's Advancing Aerospace Industry* (Arlington, VA: RAND Corporation, 2011), p. 39. This report was sponsored by the U.S.-China Economic and Security Review Commission.
9. Boeing, "Boeing and AVIC [Aviation Industry Corporation of China] to Open Manufacturing Innovation Center in China; Boeing Awards 737 Rudder Contract to AVIC's CCAC [Chengfei Commercial Aircraft Co.]," Press Release, June 20, 2011. <http://boeing.mediaroom.com/index.php?s=43&item=1795>.
10. Boeing, "Boeing Celebrates Opening of New Factory in China," Press Release, April 18, 2011. <http://boeing.mediaroom.com/index.php?s=43&item=1708>.
11. Boeing, "Boeing Celebrates Opening of New Factory in China," Press Release, April 18, 2011. <http://boeing.mediaroom.com/index.php?s=43&item=1708>.
12. Carlo Kopp, "PLA-AF [People's Liberation Army Air Force] and PLA-N [People's Liberation Army Navy] Legacy Fighters," AirPowerAustralia.net, updated June 2011. <http://www.ausairpower.net/APA-PLA-Fighters.html#mozTocId441599>; and Carlo Kopp, "XAC (Xian) H-6 Badger," AirPowerAustralia.net, updated January, 2011. <http://www.ausairpower.net/APA-Badger.html>.
13. Hu Yinan, Li Xiaokun, and Cui Haipei, "Official confirms China building aircraft carrier," *China Daily*, July 12, 2011. [http://www.chinadaily.com.cn/china/2011-07/12/content\\_12881089.htm](http://www.chinadaily.com.cn/china/2011-07/12/content_12881089.htm).
14. Michael Wines, "China Begins Sea Trials of its First Aircraft Carrier," *New York Times*, August 10, 2011. [http://www.nytimes.com/2011/08/11/world/asia/11china.html?\\_r=1](http://www.nytimes.com/2011/08/11/world/asia/11china.html?_r=1); and Jeremy Page, "China Says Carrier Won't Alter Naval Strategy," *Wall Street Journal*, July 28, 2011. <http://online.wsj.com/article/SB10001424053111903635604576472014072981554.html>.
15. BBC, "China's first aircraft carrier 'starts sea trials,'" August 10, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-14470882>; and Ian Story and You Ji, "China's Aircraft Carrier Ambitions: Seeking Truth from Rumors," *Naval War College Review* LVII: 1 (Winter 2004): 82–83.
16. Ian Story and You Ji, "China's Aircraft Carrier Ambitions: Seeking Truth from Rumors," *Naval War College Review* LVII: 1 (Winter 2004): 83.
17. Michael Wines, "China Begins Sea Trials of its First Aircraft Carrier," *New York Times*, August 10, 2011. [http://www.nytimes.com/2011/08/11/world/asia/11china.html?\\_r=1](http://www.nytimes.com/2011/08/11/world/asia/11china.html?_r=1).
18. Agence France-Presse, "China's first aircraft carrier to begin sea trials," June 21, 2011. <http://www.defensenews.com/story.php?i=6877585&c=ASI>.
19. Kathrine Hille and Mure Dickie, "China reveals new aircraft carrier plans," *Financial Times*, December 17, 2010. <http://www.ft.com/intl/cms/s/0/fa7f5e6a-09cc->



11e0-8b29-00144feabdc0.html#axzz1XNytDPPd; Bill Gertz, "China begins to build its own aircraft carrier," *Washington Times*, August 1, 2011. <http://www.washingtontimes.com/news/2011/aug/1/china-begins-to-build-its-own-aircraft-carrier/?page=1>; and Michael Wines, "China Begins Sea Trials of its First Aircraft Carrier," *New York Times*, August 10, 2011. [http://www.nytimes.com/2011/08/11/world/asia/11china.html?\\_r=1](http://www.nytimes.com/2011/08/11/world/asia/11china.html?_r=1).

20. Gabe Collins and Andrew Erickson, "China's J-15 No Game Changer," *Diplomat* (Tokyo, Japan), June 23, 2011. <http://the-diplomat.com/flashpoints-blog/2011/06/23/china%E2%80%99s-j-15-no-game-changer/>; and Associated Press, "China's first aircraft carrier begins sea trials amid concerns over Asian giant's ambitions," August 10, 2011. [http://www.washingtonpost.com/world/asia-pacific/chinas-first-aircraft-carrier-starts-sea-trial-as-rebuilding-and-test-work-continue/2011/08/09/gIQA6tBV5I\\_story.html](http://www.washingtonpost.com/world/asia-pacific/chinas-first-aircraft-carrier-starts-sea-trial-as-rebuilding-and-test-work-continue/2011/08/09/gIQA6tBV5I_story.html).

21. David A. Fulghum, "New Chinese Ship-Based Fighter Progresses," *Aviation Week*, April 28, 2011. <http://www.aviationweek.com/aw/generic/story.jsp?id=news/asd/2011/04/27/02.xml&channel=defense>.

22. J. Michael Cole, "China Unveils Carrier Trainer on State TV," *Jane's Defence Weekly*, 48: 26 (June 29, 2011): 15.

23. *Kanwa Intelligence Review*, "PLA Navy's Grander Carrier Development Program," September 20, 2010; and *Kanwa Intelligence Review*, "PLA Navy Building Flight Training Base at Yanliang," August 20, 2010. <http://www.kanwa.com/cindex.html>.

24. Hu Yinan, Li Xiaokun, and Cui Haipei, "Official confirms China building aircraft carrier," *China Daily*, July 12, 2011. [http://www.chinadaily.com.cn/china/2011-07/12/content\\_12881089.htm](http://www.chinadaily.com.cn/china/2011-07/12/content_12881089.htm); and Bill Gertz, "China begins to build its own aircraft carrier," *Washington Times*, August 1, 2011. <http://www.washingtontimes.com/news/2011/aug/1/china-begins-to-build-its-own-aircraft-carrier/?page=1>.

25. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: Department of Defense, 2011), p. 3.

26. Jeremy Page, "China Says Carrier Won't Alter Naval Strategy," *Wall Street Journal*, July 28, 2011. <http://online.wsj.com/article/SB10001424053111903635604576472014072981554.html>.

27. Meng Na and Zhang Chunxiao, "Aircraft carrier will not change defensive nature of China's policies," *Xinhua*, August 10, 2011. [http://news.xinhuanet.com/english2010/indepth/2011-08/10/c\\_131041116.htm](http://news.xinhuanet.com/english2010/indepth/2011-08/10/c_131041116.htm).

28. Jonathan Watts, "China admits 'secret' aircraft carrier is nearly ready for launch," *Guardian* (United Kingdom), June 8, 2011. <http://www.guardian.co.uk/world/2011/jun/08/china-aircraft-carrier-near-launch>.

29. Meng Na and Zhang Chunxiao, "Aircraft carrier will not change defensive nature of China's policies," *Xinhua*, August 10, 2011. [http://news.xinhuanet.com/english2010/indepth/2011-08/10/c\\_131041116.htm](http://news.xinhuanet.com/english2010/indepth/2011-08/10/c_131041116.htm).

30. Michael Wines, "China Begins Sea Trials of its First Aircraft Carrier," *New York Times*, August 10, 2011. [http://www.nytimes.com/2011/08/11/world/asia/11china.html?\\_r=1](http://www.nytimes.com/2011/08/11/world/asia/11china.html?_r=1).

31. Michael McDevitt (rear admiral in the U.S. Navy (Retired)), e-mail correspondence with Commission staff, September 20, 2011.

32. Nan Li and Christopher Weuve, "China's Aircraft Carrier Ambitions," *U.S. Naval War College Review* 63: 1 (Winter 2010): 25. <http://www.usnwc.edu/Research-Gaming/China-Maritime-Studies-Institute/Publications/documents/China-s-Aircraft-Carrier-Ambitions-An-Update1.pdf>.

33. Nan Li and Christopher Weuve, "China's Aircraft Carrier Ambitions," *U.S. Naval War College Review* 63: 1 (Winter 2010): 25. <http://www.usnwc.edu/Research-Gaming/China-Maritime-Studies-Institute/Publications/documents/China-s-Aircraft-Carrier-Ambitions-An-Update1.pdf>.

34. Yoichi Kato, "U.S. commander says China aims to be a 'global military' power," *Asahi Shimbun* (Japan), December 28, 2010. <http://www.asahi.com/english/TKY201012270241.html>.

35. Hu Yinan, Li Xiaokun, and Cui Haipei, "Official confirms China building aircraft carrier," *China Daily*, July 12, 2011. [http://www.chinadaily.com.cn/china/2011-07/12/content\\_12881089.htm](http://www.chinadaily.com.cn/china/2011-07/12/content_12881089.htm).

36. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: Department of Defense, 2011), p. 3.

37. Matthew M. Gula (congressional liaison at the U.S. Department of Defense), e-mail correspondence with Commission staff, September 20, 2011.

38. Xinhua, "China's defense budget to grow 12.7 pct in 2011: spokesman," March 4, 2011. [http://news.xinhuanet.com/english2010/china/2011-03/04/c\\_13761030.htm](http://news.xinhuanet.com/english2010/china/2011-03/04/c_13761030.htm).

39. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: Department of Defense, 2011), p. 41.

40. Andrew S. Erickson and Adam P. Liff, "Understanding China's Defense Budget: What it Means, and Why it Matters," *PacNet* 16 (Honolulu, HI: March 9, 2011).

41. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of Mark Stokes, March 10, 2011.

42. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: Department of Defense, 2011), p. 41.

43. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of Abraham Denmark, March 10, 2011.

44. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: Department of Defense, 2011), p. 41.

45. Information Office of the State Council, *China's National Defense in 2010* (Beijing, China: March 2011).

46. J. Michael Cole, "China hints at capability improvements," *Jane's Defence Weekly* 48:15 (April 13, 2011): 15; and Michael S. Chase, "China's 2010 National Defense White Paper: An Assessment," *China Brief* XI: 7 (April 22, 2011): 10.

47. Michael S. Chase, "China's 2010 National Defense White Paper: An Assessment," *China Brief* XI: 7 (April 22, 2011): 10.

48. Shirley A. Kan, "China's Defense White Paper," *Memorandum to Representative Randy Forbes* (Washington, DC: Congressional Research Service, April 5, 2011), p. 1.

49. CNA China Studies Center, "PRC [People's Republic of China] White Paper Themes," 1998–2010," March 2011.

50. Phillip C. Saunders and Ross Rustici, "Chinese Military Transparency: Evaluating the 2010 Defense White Paper," *Strategic Forum* 269 (July 2011); J. Michael Cole, "China hints at capability improvements," *Jane's Defence Weekly* 48:15 (April 13, 2011): 15; Dean Cheng, "The Limits of Transparency: China Releases 2010 Defense White Paper," *The Heritage Foundation Web Memo*, 3215 (April 7, 2011); Michael S. Chase, "China's 2010 National Defense White Paper: An Assessment," *China Brief* XI: 7 (April 22, 2011); and Shirley A. Kan, "China's Defense White Paper," *Memorandum to Representative Randy Forbes* (Washington, DC: Congressional Research Service, April 5, 2011), p. 2.

51. Phillip C. Saunders and Ross Rustici, "Chinese Military Transparency: Evaluating the 2010 Defense White Paper," *Strategic Forum* 269 (July 2011): 1.

52. Michael S. Chase, "China's 2010 National Defense White Paper: An Assessment," *China Brief* XI: 7 (April 22, 2011): 11.

53. Shirley A. Kan, "China's Defense White Paper," *Memorandum to Representative Randy Forbes* (Washington, DC: Congressional Research Service, April 5, 2011), p. 2.

54. Xinhua, "Chinese navy sends escort fleet to Gulf of Aden," July 3, 2011. [http://www.china.org.cn/world/2011-07/03/content\\_22911950.htm](http://www.china.org.cn/world/2011-07/03/content_22911950.htm); and DefenceWeb (South Africa), "Chinese naval escort returns from pirate patrol," August 30, 2011. [http://www.defenceweb.co.za/index.php?option=com\\_content&view=article&id=18487:chinese-naval-escort-returns-from-pirate-patrol&catid=51:Sea&Itemid=106](http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=18487:chinese-naval-escort-returns-from-pirate-patrol&catid=51:Sea&Itemid=106).

55. U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), pp. 118–119.

56. Xinhua, "Chinese navy sends escort fleet to Gulf of Aden," July 3, 2011. [http://www.china.org.cn/world/2011-07/03/content\\_22911950.htm](http://www.china.org.cn/world/2011-07/03/content_22911950.htm).

57. Open Source Center, "OSC Interactive Map: Chinese PLA Navy Escort Mission Port Calls," *OSC Summary* (May 2, 2011). OSC ID: FEA20110503017394. <http://www.opensource.gov>.

58. Lauren Ploch et al., "Piracy off the Horn of Africa" (Washington, DC: Congressional Research Service, April 27, 2011), pp. 24–25. <http://www.fas.org/sgp/crs/row/R40528.pdf>.

59. Greg Torode, "Hit pirates on land, says top China general," *South China Morning Post*, May 20, 2011. <http://topics.scmp.com/news/china-news-watch/article/Hit-pirates-on-land-says-top-China-general>.

60. Xinhua, "35,860 Chinese evacuated from unrest-torn Libya," March 3, 2011. [http://news.xinhuanet.com/english/2011/03/03/c\\_13759456.htm](http://news.xinhuanet.com/english/2011/03/03/c_13759456.htm).
61. Adam Rawnsley, "Chinese Missile Ship Races to Libya," February 25, 2011. <http://www.wired.com/dangerroom/2011/02/chinese-missile-ship-races-to-libya-for-rescue-duty/>; and Josh Chin, "China Vows to Protect Chinese in Libya," *Wall Street Journal*, February 25, 2011. <http://online.wsj.com/article/SB10001424052748703905404576164321645905718.html>.
62. Xinhua, "35,860 Chinese evacuated from Libya all back home," March 6, 2011. [http://www.china.org.cn/world/2011-03/06/content\\_22066694.htm](http://www.china.org.cn/world/2011-03/06/content_22066694.htm).
63. Gabe Collins and Andrew Erickson, "China dispatches warship to protect Libya evacuation mission: Marks the PRC's first use of frontline military assets to protect an evacuation mission," *China SignPost* 25 (February 24, 2011). <http://www.chinasignpost.com/2011/02/china-dispatches-warship-to-protect-libya-evacuation-mission-marks-the-prc%E2%80%99s-first-use-of-frontline-military-assets-to-protect-an-evacuation-mission/>.
64. Tanjie, "PLA Air Force transporters evacuate compatriots from Libya," *PLA Daily*, March 2, 2011. [http://eng.mod.gov.cn/DefenseNews/2011-03/02/content\\_4228001.htm](http://eng.mod.gov.cn/DefenseNews/2011-03/02/content_4228001.htm).
65. Daniel Dombey, "Gates struggles to deepen ties with China," *Financial Times*, January 10, 2011. <http://www.ft.com/intl/cms/s/0/9cd104d4-1c97-11e0-a106-00144feab49a.html#axzz1XOUJ8VNX>.
66. Daniel Dombey, "Gates struggles to deepen ties with China," *Financial Times*, January 10, 2011. <http://www.ft.com/intl/cms/s/0/9cd104d4-1c97-11e0-a106-00144feab49a.html#axzz1XOUJ8VNX>.
67. Daniel Dombey, "Gates struggles to deepen ties with China," *Financial Times*, January 10, 2011. <http://www.ft.com/intl/cms/s/0/9cd104d4-1c97-11e0-a106-00144feab49a.html#axzz1XOUJ8VNX>.
68. John Pomfret, "China tests stealth fighter jet just before Gates, Hu visit," *Washington Post*, January 11, 2011. [http://www.washingtonpost.com/wp-dyn/content/article/2011/01/11/AR2011011101338\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2011/01/11/AR2011011101338_pf.html).
69. Elizabeth Bumiller and Michael Wines, "Gates Warns of North Korea Missile Threat to U.S.," *New York Times*, January 11, 2011. <http://www.nytimes.com/2011/01/12/world/asia/12military.html>.
70. Julian E. Barnes, "Gates, China Discuss Nuclear Strategy," *Wall Street Journal*, January 12, 2011. <http://online.wsj.com/article/SB10001424052748703947404576076941991898836.html>.
71. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of Andrew Scobell, March 10, 2011; and U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimony of Cortez A. Cooper, January 27, 2011.
72. Yuhua Hayishi and Julian E. Barnes, "Gates Leaves Beijing, Will Press Japan to Expand Its Defense Role," *Wall Street Journal*, January 13, 2011. <http://online.wsj.com/article/SB10001424052748704803604576077412162707724.html>.
73. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of Andrew Scobell, March 10, 2011.
74. Agence France-Presse, "U.S. Rolls Out Red Carpet for China Military Chief," May 14, 2011. <http://www.defensenews.com/story.php?i=6502345>.
75. Yang Liming and Ju Hui, "Three Points of Consensus Reached, Six Specific Achievements in China-US Military Exchanges," *Zhongguo Qingnian Bao [China Youth Daily]*, May 20, 2011, OSC ID: CPP20110520787016.
76. U.S. Department of Defense, "Joint Press Conference with Adm. Mullen and Gen. Chen from the Pentagon" (Washington, DC: May 18, 2011).
77. Bill Gertz, "Chinese to view sensitive U.S. sites," *Washington Times*, May 18, 2011. <http://www.washingtontimes.com/news/2011/may/17/chinese-to-view-sensitive-us-sites/>.
78. Jeremy Page, "China Gives Mullen Rare Look at Jet, Sub," *Wall Street Journal*, July 14, 2011. <http://online.wsj.com/article/SB10001424052702304223804576443932225547482.html>; Li Xiaokun and Li Lianxing, "Warm welcome awaits Mullen," *China Daily*, July 8, 2011.
79. Michael Wines, "Bumps Remain as Military Leaders of U.S. and China Meet," *New York Times*, July 11, 2011. <http://www.nytimes.com/2011/07/12/world/asia/12china.html>.
80. Michael Wines, "Bumps Remain as Military Leaders of U.S. and China Meet," *New York Times*, July 11, 2011. <http://www.nytimes.com/2011/07/12/world/asia/12china.html>.

81. Agence France-Presse, "Mullen Asks China for Help on North Korea," July 10, 2011. <http://www.defensenews.com/story.php?i=7057993>.
82. Tom Cook, "Rising Tensions in the South China Sea: An Interview with Ian Storey" (Seattle, WA: The National Bureau of Asian Research, June 17, 2011). <http://www.nbr.org/research/activity.aspx?id=151>.
83. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimony of Stacy A. Pedrozo, January 27, 2011.
84. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimonies of Balbina Hwang, Stacy A. Pedrozo, and Jim Thomas, January 27, 2011.
85. Ian Storey, "China and the Philippines: Implications of the Reed Bank Incident," *China Brief* (May 16, 2011). [http://www.jamestown.org/single/?no\\_cache=1&tx\\_ttnews\[tt\\_news\]=37902](http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=37902).
86. Agence France-Presse, "Philippines wants UN body to broker China dispute," July 11, 2011. <http://www.asiaone.com/News/Latest+News/Asia/Story/A1Story20110711-288603.html>.
87. *Defense News*, "Philippine-U.S. Navies Unite Amid China Tensions," June 27, 2011. <http://www.defensenews.com/story.php?c=ASI&s=TOP&i=6938404>; Amanda Doronila, "Analysis: On sending Philippine Navy's biggest warship to the Spratlys," *Philippine Daily Inquirer*, June 20, 2011. <http://ph.news.yahoo.com/analysis-sending-philippine-navys-biggest-warship-spratlys-033002016.html>; and Lachlan Carmichael and Shaun Tandon, "U.S. Says it Will Provide Hardware to Philippines," *Defense News*, June 23, 2011. <http://www.defensenews.com/story.php?i=6906530>.
88. Agence France-Presse, "Philippines Ups Spending to Guard South China Sea," September 7, 2011. <http://www.defensenews.com/story.php?i=7610902&c=ASI&s=TOP>; Reuters, "China to set up South China Sea stations," September 8, 2011. <http://www.chinapost.com.tw/asia/philippines/2011/09/08/315998/Philippines-to.htm>.
89. *Defense News*, "Philippine-U.S. Navies Unite Amid China Tensions," June 27, 2011. <http://www.defensenews.com/story.php?c=ASI&s=TOP&i=6938404>.
90. Ben Bland and Kathrin Hill, "Vietnam and China oil clashes intensify," *Financial Times*, May 27, 2011. <http://www.ft.com/cms/s/0/4d3badc0-8867-11e0-a1c3-00144feabdc0.html?ftcamp=rss#axzz1QmAioYo3>.
91. BBC, "China accuses Vietnam in South China Sea row," June 10, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-13723443>.
92. Dang Dinh Quy, "One Axis and Two Wings: An Update" (Diplomatic Academy of Vietnam briefing for USCC Commissioners, Washington, DC, June 26, 2011).
93. Michael Swaine and M. Taylor Fravel, "China's Assertive Behavior, Part Two: The Maritime Periphery," *China Leadership Monitor* 35 (Summer 2011): 6.
94. Andrew Higgins, "In South China Sea, a dispute over energy," *Washington Post*, September 17, 2011. [http://www.washingtonpost.com/world/asia-pacific/in-south-china-sea-a-dispute-over-energy/2011/09/07/gIQA0PrQaK\\_story.html](http://www.washingtonpost.com/world/asia-pacific/in-south-china-sea-a-dispute-over-energy/2011/09/07/gIQA0PrQaK_story.html).
95. Cecil Morela, "Philippines protests to China over oil rig plan," Agence France-Presse, June 1, 2011. [http://old.news.yahoo.com/s/afp/20110601/wl\\_asia\\_afp/philippineschinadiplomacyspratlys\\_20110601160852](http://old.news.yahoo.com/s/afp/20110601/wl_asia_afp/philippineschinadiplomacyspratlys_20110601160852).
96. Michael D. Swaine and M. Taylor Fravel, "China's Assertive Behavior Part Two: The Maritime Periphery," *China Leadership Monitor* 35 (Summer 2011): 6. [http://web.mit.edu/ssp/people/fravel/Swaine\\_Fravel\\_CLM\\_35\\_0624111.pdf](http://web.mit.edu/ssp/people/fravel/Swaine_Fravel_CLM_35_0624111.pdf); and Ben Bland, "Vietnamese fishermen on front line in China clash," *Financial Times*, June 20, 2011. <http://www.ft.com/intl/cms/s/0/0b4e8380-9b52-11e0-bbc6-00144feabdc0.html#axzz1WdFprBsj>.
97. Associated Press, "China to strengthen fisheries management in 'sensitive' waters," December 23, 2011. [http://www.breitbart.com/article.php?id=D9K9I9Q80&show\\_article=1](http://www.breitbart.com/article.php?id=D9K9I9Q80&show_article=1); and Michael D. Swaine and M. Taylor Fravel, "China's Assertive Behavior Part Two: The Maritime Periphery," *China Leadership Monitor* 35 (Summer 2011): 6. [http://web.mit.edu/ssp/people/fravel/Swaine\\_Fravel\\_CLM\\_35\\_0624111.pdf](http://web.mit.edu/ssp/people/fravel/Swaine_Fravel_CLM_35_0624111.pdf).
98. VietnamNet Bridge, "Chinese military ships bully Vietnam's fishing boats," June 3, 2011. <http://www.lookatvietnam.com/2011/06/chinese-military-ships-bully-vietnams-fishing-boats.html>.
99. Associated Press, "Chinese navy confiscated fish from fishermen, Vietnamese claims," July 16, 2011. <http://www.manilastandardtoday.com/insideNews.htm?f=2011/july/16/news7.isx&d=2011/july/16>.
100. Margie Mason, "Vietnamese protest China for 3rd week," Associated Press, June 20, 2011. <http://www.chinapost.com.tw/china/national-news/2011/06/20/306846/Vietnamese-protest.htm>; and Associated Press, "Vietnamese Police Squash Anti-China Protest," August 21, 2011. <http://www.npr.org/2011/08/21/139827365/vietnamese-police-squash-anti-china-protest>.



101. Matthew Pennington, "Amid South China Sea Tensions US Says Committed to Protect Philippines," Associated Press, June 23, 2011. <http://www.660news.com/news/world/article/245086—amid-south-china-sea-tensions-us-says-it-is-committed-to-defence-of-the-philippines>.

102. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimony of Stacy A. Pedrozo, January 27, 2011.

103. Michael D. Swaine and M. Taylor Fravel, "China's Assertive Behavior Part Two: The Maritime Periphery," *China Leadership Monitor* 35 (Summer 2011): 6. [http://web.mit.edu/ssp/people/fravel/Swaine\\_Fravel\\_CLM\\_35\\_0624111.pdf](http://web.mit.edu/ssp/people/fravel/Swaine_Fravel_CLM_35_0624111.pdf).

104. Kyodo News (Japan), "Chinese fishery vessel sets sail for disputed waters," September 2, 2011. <http://english.kyodonews.jp/news/2011/09/112598.html>.

105. Shi Jiangtao, "China charts course to project marine power," *South China Morning Post*, June 9, 2011.

106. *People's Daily*, "China to beef up maritime forces amid disputes," June 17, 2011. <http://english.people.com.cn/90001/90776/90883/7412388.html#>; Grace Ng, "China Beefs Up Maritime Patrol Force," *Straits Times Indonesia*, May 3, 2011. <http://www.thejakartaglobe.com/asia/china-beefs-up-maritime-patrol-force/438869>.

107. Grace Ng, "China Beefs Up Maritime Patrol Force," *Straits Times Indonesia*, May 3, 2011. <http://www.thejakartaglobe.com/asia/china-beefs-up-maritime-patrol-force/438869>.

108. Open Source Center Graphic, "Military-Related Events in South China Sea, 13 to 21 June 2011," June 21, 2011. CPP20110622017001. [www.opensource.gov](http://www.opensource.gov).

109. BBC, "Singapore urges China to clarify South China Sea claim," June 20, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-13838462>.

110. Ben Bland and Girija Shivakumar, "China confronts Indian vessel," August 31, 2011. <http://www.ft.com/cms/s/0/883003ec-d3f6-11e0-b7eb-00144feab49a.html#axzz1WdFprBsj>.

111. James Rupert and Daniel Ten Kate, "China Pushing for Binding S. China Sea Code, Aquino Says," Bloomberg News, September 1, 2011. <http://www.bloomberg.com/news/2011-08-31/china-wants-binding-conduct-code-in-s-china-sea-aquino-says.html>.

112. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimonies of Stacy A. Pedrozo and Jim Thomas, January 27, 2011.

113. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimonies of Stacy A. Pedrozo and Jim Thomas, January 27, 2011.

114. Agence France-Presse, "China Stages Military Drills in South China Sea," June 17, 2011. [http://www.straitstimes.com/BreakingNews/Asia/Story/STIStory\\_680861.html](http://www.straitstimes.com/BreakingNews/Asia/Story/STIStory_680861.html).

115. Xinhua, "PLA's Operation in S China routine drill: Ministry," August 9, 2011. [http://www.chinadaily.com.cn/china/2011-08/09/content\\_13080729.htm](http://www.chinadaily.com.cn/china/2011-08/09/content_13080729.htm).

116. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impact*, written testimony of Jim Thomas, January 27, 2011.

117. *Philippine Star*, "Manila Protests Presence of Chinese Navy Vessels in Philippine Waters," June 2, 2011.

118. Philippines Department of Foreign Affairs, "Statement of the Department of Foreign Affairs on Developments in the West Philippine Sea (South China Sea)" (Pasay City, Philippines: June 1, 2011). <http://www.dfa.gov.ph/main/index.php/office-of-the-undersecretary-for-policy/3111-statement-of-the-department-of-foreign-affairs-on-developments-in-the-west-philippine-sea-south-china-sea>.

119. Association of Southeast Asian Nations, *Declaration on the Conduct of Parties in the South China Sea*, 2002. <http://www.aseansec.org/13163.htm>.

120. Ian Storey, "Recent Developments in the South China Sea" (Center for Strategic and International Studies conference, "Maritime Security in the South China Sea," Washington, DC, June 20–21, 2011).

121. Representatives of the Singaporean Ministry of Foreign Affairs, and Singaporean academics, meetings with Commissioners, Singapore, December 13, 2010; Representatives of the Indonesian Ministry of Foreign Affairs, meetings with Commissioners, Jakarta, Indonesia, December 15, 2010.

122. Representatives of the Singaporean government, meetings with Commissioners, Singapore, December 13, 2010; Representatives of the Indonesian government, meetings with Commissioners, Jakarta, Indonesia, December 15, 2010; U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2010), p. 139.

123. Representatives of the Singaporean government, meeting with Commissioners, Singapore, December 13, 2010; Ian Storey, "China's Missteps in Southeast Asia: Less Charm, More Offensive" *China Brief* 10:25 (December 17, 2010). [http://www.jamestown.org/single/?no\\_cache=1&tx\\_ttnews\[tt\\_news\]=37294](http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=37294).

124. Representatives of the Singaporean government, meeting with Commissioners, Singapore, December 13, 2010.

125. Jim Gomez, "SE Asia risks China's ire to discuss sea dispute," Associated Press, September 22, 2011. <http://my.news.yahoo.com/se-asia-risks-chinas-ire-discuss-sea-dispute-062157276.html>; Xinhua, "China opposes attempts to internationalize South China Sea disputes," September 28, 2011. [http://news.xinhuanet.com/english2010/china/2011-09/28/c\\_131165615.htm](http://news.xinhuanet.com/english2010/china/2011-09/28/c_131165615.htm).

126. Long Tao, "Time to teach those around the South China Sea a lesson," *Global Times*, September 29, 2011. <http://www.globaltimes.cn/NEWS/tabid/99/ID/677717/Time-to-teach-those-around-South-China-Sea-a-lesson.aspx>.

127. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimonies of Jim Thomas, January 27, 2011.

128. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimonies of Stacy A. Pedrozo, January 27, 2011.

129. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimonies of Balbina Hwang, January 27, 2011.

130. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimonies of Stacy A. Pedrozo, January 27, 2011.

131. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimonies of Stacy A. Pedrozo, January 27, 2011; *People's Daily*, "China to strengthen maritime forces amid dispute," June 17, 2011. <http://english.people.com.cn/90001/90776/90883/7412388.html#>.

132. Elinor Mills, "China linked to new breaches tied to RSA," *CNET News Insecurity Complex*, June 6, 2011. [http://news.cnet.com/8301-27080\\_3-20068836-245/china-linked-to-new-breaches-tied-to-rsa/#ixzz1WY7QASTd](http://news.cnet.com/8301-27080_3-20068836-245/china-linked-to-new-breaches-tied-to-rsa/#ixzz1WY7QASTd); and Christopher Drew, "Stolen Data Is Tracked to Hacking at Lockheed," *New York Times*, June 3, 2011. <http://www.nytimes.com/2011/06/04/technology/04security.html>.

133. For example, the "Shadows in the Cloud" case study documented 131 compromised information systems in 31 countries. Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," April 6, 2010, p. 27. <http://shadows-in-the-cloud.net>.

134. Dmitri Alperovitch, *Revealed: Operation Shady RAT* (Santa Clara, CA: McAfee, August 2011), p. 4. <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>.

135. Dmitri Alperovitch, *Revealed: Operation Shady RAT* (Santa Clara, CA: McAfee, August 2011), p. 6. <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>.

136. Zhao Huanxin, "China names key industries for absolute state control," *China Daily*, December 19, 2006. [http://www.chinadaily.com.cn/china/2006-12/19/content\\_762056.htm](http://www.chinadaily.com.cn/china/2006-12/19/content_762056.htm).

137. McAfee Foundstone Professional Services/McAfee Labs, *Global Energy Cyberattacks: 'Night Dragon'* (Santa Clara, CA: McAfee, February 10, 2011). <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>.

138. McAfee Foundstone Professional Services/McAfee Labs, *Global Energy Cyberattacks: 'Night Dragon'* (Santa Clara, CA: McAfee, February 10, 2011). <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>.

139. *The Official Google Blog*, "Ensuring your information is safe online," June 1, 2011. <http://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html>.

140. U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, D.C.: U.S. Government Printing Office, November 2009), p. 172. <http://www.uscc.gov/annual/report/2009/annual/report/full/09.pdf>; and Northrop Grumman Corporation, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" (contracted research paper for the U.S.-China Economic and Security Review Commission, June 2009), p. 32. <http://www.uscc.gov/researchpapers/2009/NorthropGrumman/PRC/Cyber/Paper/FINAL/Approved%20Report/16Oct2009.pdf>.



141. John Markoff and David Barboza, "2 China Schools Said to Be Tied to On-line Attacks," *New York Times*, February 18, 2010. <http://www.nytimes.com/2010/02/19/technology/19china.html>.

142. By comparison, 12 percent of the respondents (the next highest group) viewed the U.S. government as the greatest concern. Stewart Baker et al., *In the Dark: Crucial Industries Confront Cyberattacks* (Santa Clara, CA: McAfee/Center for Strategic and International Studies, April 2011), pp. 20–22. <http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf>.

143. Matthew Robertson and Helena Zhu, "Slip-Up in Chinese Military TV Show Reveals More Than Intended," *Epoch Times*, updated August 28, 2011. <http://www.theepochtimes.com/n2/china-news/slip-up-in-chinese-military-tv-show-reveals-more-than-intended-60619.html>; and Edward Wong, "China State TV Deletes Video Implying Hacking of Western Sites," *New York Times*, August 26, 2011. <http://www.nytimes.com/2011/08/27/world/asia/27china.html>.

144. Andrew Erickson and Gabe Collins, "A Smoking Cursor? New Window Opens on China's Potential Cyberwarfare Development: CCTV 7 program raises new questions about Beijing's support for hacking," *China SignPost*, August 24, 2011. <http://www.chinasignpost.com/2011/08/a-smoking-cursor-new-window-opens-on-china%E2%80%99s-potential-cyberwarfare-development-cctv-7-program-raises-new-questions-about-beijing%E2%80%99s-support-for-hacking/>.

145. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: U.S. Department of Defense, 2011), p. 5.

146. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

147. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

148. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impact*, written testimony of Martin C. Libicki, January 27, 2011.

149. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impact*, written testimony of Martin C. Libicki, January 27, 2011.

150. Michael Wines, "China Creates New Agency for Patrolling the Internet," *New York Times*, May 4, 2011. <http://www.nytimes.com/2011/05/05/world/asia/05china.html>.

151. Josh Chin, "Following Jiang Death Rumors, China's Rivers Go Missing," *Wall Street Journal China Real Time Report*, July 6, 2011. <http://blogs.wsj.com/chinarealtime/2011/07/06/following-jiang-death-rumors-chinas-rivers-go-missing/>.

152. *Financial Times*, "Why China fears the Arab spring," February 28, 2011. <http://www.ft.com/cms/s/0/3442a77c-4377-11e0-8f0d-00144feabdc0.html#ixzz1XIOaqqYu>; Joe McDonald, "China Cracks Down On Internet Content," *Associated Press*, August 24, 2011.

153. Fang Yunyu, "China's Great Firewall Father Speaks Out," *Global Times*, February 18, 2011. <http://special.globaltimes.cn/2011-02/624290.html>. The original source is no longer available. A copy is preserved at <http://cryptome.org/0003/gwf-father.htm>.

154. Richard Lai, "China tightens grip on VPN [virtual private networks] access amid pro-democracy protests, Gmail users also affected," *Engadget*, March 16, 2011. <http://www.engadget.com/2011/03/16/china-tightens-grip-on-vpn-access-amid-pro-democracy-protests-g>; and Oiwan Lam, "China: Cracking down circumvention tools," *Global Voices Online*, May 13, 2011. <http://advocacy.globalvoicesonline.org/2011/05/13/china-cracking-down-circumvention-tools/>.

155. BBC News, "China: 1.3 million websites shut in 2010," July 13, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-14138267>.

156. BGPmon.net, Untitled, March 26, 2011. <http://bgpmon.net/blog/?p=499>; and Fahmida Y. Rashid, "Facebook Traffic Diverted to China Raising Privacy Concerns," *eWeek.com*, March 25, 2011. <http://www.eweek.com/c/a/Security/Facebook-Traffic-Diverted-to-China-Raising-Privacy-Concerns-130825/>.

157. See for example, Roger Cliff et al., *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States* (Arlington, VA: RAND Corporation, 2007); Thomas G. Mahnken, "China's Anti-Access Strategy in Historical and Theoretical Perspective," *Journal of Strategic Studies* 34:3 (June 2011): 299–323; Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: U.S. Department of Defense, 2011); and Bill Gertz, "China 'A2/

AD' [Anti-Access/Area Denial] Threat," *Washington Times*, December 15, 2010. <http://www.washingtontimes.com/news/2010/dec/15/inside-the-ring-251245374/>.

158. U.S.-China Economic and Security Review Commission, *2009 Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), pp. 113–127.

159. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Robert J. Wittman, January 27, 2011.

160. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Daniel K. Inouye, January 27, 2011.

161. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Oriana Skylar Mastro, January 27, 2011; U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Roger Cliff, January 27, 2011; and U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Cortez A. Cooper, January 27, 2011.

162. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Roger Cliff, January 27, 2011.

163. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Cortez A. Cooper, January 27, 2011.

164. Peng Guangqian and Yao Youzhi, eds., *The Science of Military Strategy* (Beijing, China: Military Science Publishing House, 2005), p. 452.

165. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Cortez A. Cooper, January 27, 2011.

166. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Oriana Skylar Mastro, January 27, 2011.

167. Mao Zedong, *Problems of Strategy in China's Revolutionary War* (Peking [Beijing], China: Foreign Languages Press, 1965).

168. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Roger Cliff, January 27, 2011; U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011; and U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Oriana Skylar Mastro, January 27, 2011.

169. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Oriana Skylar Mastro, January 27, 2011.

170. Peng Guangqian and Yao Youzhi, eds., *The Science of Military Strategy* (Beijing, China: Military Science Publishing House, 2005), p. 463.

171. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Roger Cliff, January 27, 2011.

172. Zhang Yuliang, ed., *Zhanyi Xue [The Science of Campaigns]* (Beijing: Guofang Daxue Chubanshe, 2006), p. 89. USCC staff translation.

173. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Roger Cliff, January 27, 2011.

174. Information Office of the State Council, *China's National Defense in 2010* (Beijing, China: March 2011).

175. Information Office of the State Council, *China's National Defense in 2008* (Beijing, China: January 2009).

176. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2010* (Washington, DC: U.S. Department of Defense, 2010), p. 24.

177. Henry Kissinger, *On China* (New York: Penguin Press, 2011), p. 368.

178. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2010* (Washington, DC: U.S. Department of Defense, 2010), p. 24.

179. Andrew Scobell, *China's Use of Military Force: Beyond the Great Wall and the Long March* (New York, New York: Cambridge University Press, 2003), p. 15.

180. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

181. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Roger Cliff, January 27, 2011; U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011; and U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Martin C. Libicki, January 27, 2011.

182. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Roger Cliff, January 27, 2011.

183. Roger Cliff (nonresident senior fellow at the Project 2049 Institute), e-mail correspondence with Commission staff, August 8, 2011.

184. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Roger Cliff, January 27, 2011; and U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

185. Peng Guangqian and Yao Youzhi, eds., *The Science of Military Strategy* (Beijing, China: Military Science Publishing House, 2005), p. 461.

186. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Roger Cliff, January 27, 2011.

187. Zhang Yuliang, ed., *Zhanyi Xue [The Science of Campaigns]* (Beijing, China: Guofang Daxue Chubanshe, 2006), p. 96. USCC staff translation.

188. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2010* (Washington, DC: U.S. Department of Defense, 2010), pp. 22–23; U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Oriana Skylar Mastro, January 27, 2011; U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Cortez A. Cooper, January 27, 2011; U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), pp. 130–34; and Michael J. McDevitt, “The PLA Navy Anti-Access Role in a Taiwan Contingency” (paper presented at the 2010 Pacific Symposium, June 16, 2010, p. 16).

189. Michael J. McDevitt, “The Strategic and Operational Context Driving PLA Navy Building,” in *Right-Sizing the People's Liberation Army: Exploring the Contours of China's Military*, eds. Roy Kamphausen and Andrew Scobell (Carlisle, PA: U.S. Army War College, 2007), pp. 485–486; U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and Its Regional Impact*, written testimony of Cortez A. Cooper, January 27, 2011; and Dean Cheng, “Sea Power and the Chinese State: China's Maritime Ambitions,” *Heritage Backgrounder* 2576 (July 11, 2011). <http://www.heritage.org/research/reports/2011/07/sea-power-and-the-chinese-state-chinas-maritime-ambitions>;

190. Peng Guangqian and Yao Youzhi, eds., *The Science of Military Strategy* (Beijing, China: Military Science Publishing House, 2005), p. 461.

191. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Oriana Skylar Mastro, January 27, 2011; U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Cortez A. Cooper, January 27, 2011; and U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011. See also U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), p. 144.

192. Officials of the Singaporean government, meeting with Commissioners, Singapore, December 13, 2010.

193. U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), p. 147; and U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), p. 91.

194. Information Office of the State Council, *China's National Defense in 2010* (Beijing, China: March 2011); and Information Office of the State Council, *China's National Defense in 2008* (Beijing, China: January 2009).

195. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: U.S. Department of Defense, 2011), p. 32.

196. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Stacy A. Pedrozo, January 27, 2011.

197. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

198. U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), p. 136.

199. Ronald O'Rourke, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress* (Washington, DC: Congressional Research Service, June 8, 2011), pp. 16–22.

200. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), pp. 85–87. The Department of Defense's recent report on China's military power similarly lists between 1,000 and 1,200 short-range ballistic missiles. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: U.S. Department of Defense, 2011), p. 78.

201. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

202. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: U.S. Department of Defense, 2011), p. 3.

203. Jan Van Tol et al., *AirSea Battle: A Point of Departure Operational Concept* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), p. 18.

204. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: U.S. Department of Defense, 2011), p. 78.

205. U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), p. 138.

206. Ronald O'Rourke, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress* (Washington, DC: Congressional Research Service, June 8, 2011), p. 42.

207. Andrew S. Erickson, Lyle J. Goldstein, and William S. Murray, "Chinese Mine Warfare: A PLA Navy 'Assassin's Mace' Capability," *China Maritime Studies* 3 (Newport, RI: U.S. Naval War College, June 2009): 25.

208. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), pp. 73–91.

209. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), p. 80.

210. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

211. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: U.S. Department of Defense, 2011), p. 28.

212. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), pp. 82–83.

213. Information Office of the State Council, *China's National Defense in 2010* (Beijing, China: March 2011).

214. Jan Van Tol et al., *AirSea Battle: A Point of Departure Operational Concept* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), pp. 19 and 21.

215. David D. Chen, "2011 PLA Military Training: Toward Greater Interoperability," *China Brief* 11:2 (January 21, 2011): 10–11.

216. Bryan Krekel, with George Bakos and Christopher Barnett, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA: Northrup Grumman Corporation, October 9, 2009). [http://www.uscc.gov/researchpapers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper](http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper)



*FINAL Approved%20Report 16Oct2009.pdf*. See also U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

217. Jan Van Tol et al., *AirSea Battle: A Point of Departure Operational Concept* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), p. 20.

218. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

219. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Cortez A. Cooper, January 27, 2011.

220. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

221. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Cortez A. Cooper, January 27, 2011.

222. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Dean Cheng, January 27, 2011. See also U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

223. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Dean Cheng, January 27, 2011.

224. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Oriana Skylar Mastro, January 27, 2011.

225. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Cortez A. Cooper, January 27, 2011.

226. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Jim Thomas, January 27, 2011.

227. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), pp. 89–90.

228. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

229. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Martin C. Libicki, January 27, 2011.

230. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of Martin C. Libicki, January 27, 2011.

231. Leo Pigaty and James C. Workman, "Testing the Survivability of Logistics Information Systems," *Army Logistician* (November-December 2004). <http://www.almc.army.mil/alog/issues/novdec04/testing.html>.

232. Bryan Krekel, with George Bakos and Christopher Barnett, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA: Northrup Grumman Corporation, October 9, 2009), p. 25. [http://www.uscc.gov/researchpapers/2009/NorthropGrumman\\_PRC\\_Cyber\\_Paper\\_FINAL\\_Approved%20Report\\_16Oct2009.pdf](http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf).

233. Denny Roy (senior fellow, East-West Center), meeting with Commissioners, Honolulu, HI, May 17, 2011.

234. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

235. Yoichi Kato, "U.S. Commander says China Aims to be a 'Global Military' Power," *Asahi Shimbun* (Tokyo), December 28, 2010. <http://www.asahi.com/english/TKY201012270241.html>.

236. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), p. 9.

237. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

238. Alan B. Romberg, *Rein In at the Brink of the Precipice: American Policy Toward Taiwan and U.S.-PRC Relations* (Washington, DC: Stimson Center, 2003), pp. 171–76; Andrew Scobell, *China's Use of Military Force: Beyond the Great Wall and the Long March* (New York, NY: Cambridge University Press, 2003), pp. 171–191; and Arthur S. Ding, “The Lessons of the 1995–1996 Military Taiwan Strait Crisis: Developing a New Strategy Toward the United States and Taiwan,” in *The Lessons of History: The Chinese People's Liberation Army at 75* (Carlisle, PA: Strategic Studies Institute, July 2003), pp. 379–402.

239. Dean Cheng and Peter Cugley, *The PRC [People's Republic of China] Space Program: An Open Source Examination* (Alexandria, VA: CNA, September 2008), pp. 24–27.

240. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

241. Roger Cliff, Chad J. R. Ohlandt, and David Yang, “Ready for Takeoff: China's Advancing Aerospace Industry” (contracted research paper for the U.S.-China Economic and Security Review Commission, 2011), p. 90. [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf).

242. Roger Cliff, Chad J.R. Ohlandt, and David Yang, “Ready for Takeoff: China's Advancing Aerospace Industry” (contracted research paper for the U.S.-China Economic and Security Review Commission, Washington, DC, 2011), p. 93. [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf).

243. Union of Concerned Scientists, “UCS Satellite Database (through 4/30/11)” (Cambridge, MA: 2011). [http://www.ucsusa.org/nuclear\\_weapons\\_and\\_global\\_security/space\\_weapons/technical\\_issues/ucs-satellite-database.html](http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html).

244. Roger Cliff, Chad J.R. Ohlandt, and David Yang, “Ready for Takeoff: China's Advancing Aerospace Industry” (contracted research paper for the U.S.-China Economic and Security Review Commission, 2011), pp. 107–108. [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf).

245. Roger Cliff, Chad J.R. Ohlandt, and David Yang, “Ready for Takeoff: China's Advancing Aerospace Industry” (contracted research paper for the U.S.-China Economic and Security Review Commission, 2011), p. 102. [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf).

246. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Barry Watts, May 11, 2011.

247. U.S. Department of Defense, *Annual Report on the Military Power of the People's Republic of China* (Washington, DC: July 28, 2003), p. 10. <http://www.defense.gov/pubs/2003chinaex.pdf>.

248. Information Office of the State Council, *China's Space Activities in 2006* (Beijing, China: October 2006), p. 2. [http://news.xinhuanet.com/english/2006-10/12/content\\_5193446.htm](http://news.xinhuanet.com/english/2006-10/12/content_5193446.htm).

249. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

250. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Scott Pace, May 11, 2011.

251. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

252. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

253. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

254. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Scott Pace, May 11, 2011.

255. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

256. Information Office of the State Council, *China's National Defense in 2010* (Beijing, China: 2010), p. 28. [http://merln.ndu.edu/whitepapers/China\\_English\\_2010.pdf](http://merln.ndu.edu/whitepapers/China_English_2010.pdf).

257. Roger Cliff, Chad J.R. Ohlandt, and David Yang, “Ready for Takeoff: China's Advancing Aerospace Industry” (contracted research paper for the U.S.-China Eco-



conomic and Security Review Commission, 2011), pp. 97–98. [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf).

258. For example, see Cheng Guangjin, “China, Russia shake hands in outer space,” *China Daily*, December 25, 2009. [http://www.chinadaily.com.cn/china/2009-12/25/content\\_9227208.htm](http://www.chinadaily.com.cn/china/2009-12/25/content_9227208.htm); Agence France-Presse, “China to explore Mars with Russia this year,” January 1, 2011. [http://www.straitstimes.com/BreakingNews/TechandScience/Story/STISStory\\_619866.html](http://www.straitstimes.com/BreakingNews/TechandScience/Story/STISStory_619866.html); C. Wang et al., “A brief introduction to the SMESE mission [SMall Explorer for Solar Eruptions],” NASA.gov, 2006. [http://cdaw.gsfc.nasa.gov/publications/ilws\\_goa2006/211\\_Wang.pdf](http://cdaw.gsfc.nasa.gov/publications/ilws_goa2006/211_Wang.pdf); Globalsecurity.org, “Sinosat,” undated. <http://www.globalsecurity.org/space/world/china/sinogat.htm>; and Jonathan Amos, “China and UK strike space deal,” BBC, June 29, 2011. <http://www.bbc.co.uk/news/science-environment-13946179>.

259. The White House, Office of the Press Secretary, “U.S.-China Joint Statement” (Washington, DC: November 17, 2009). <http://www.whitehouse.gov/the-press-office/us-china-joint-statement>; David Weaver, “NASA [National Aeronautics and Space Administration] Administrator Statement on China Visit (10–270)” (Washington, DC: NASA Headquarters, October 25, 2010). [http://www.nasa.gov/home/hqnews/2010/oct/HQ\\_10-270\\_Bolden\\_China.html](http://www.nasa.gov/home/hqnews/2010/oct/HQ_10-270_Bolden_China.html); and The White House, Office of the Press Secretary, “U.S.-China Joint Statement” (Washington, DC: January 19, 2011). <http://www.whitehouse.gov/the-press-office/2011/01/19/us-china-joint-statement>.

260. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Scott Pace, May 11, 2011.

261. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

262. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

263. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

264. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

265. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

266. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

267. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Mark Stokes, May 11, 2011.

268. James Mulvenon and Rebecca Samm Tyroler-Cooper, “China’s Defense Industry on the Path to Reform” (prepared by Defense Group Incorporated for the U.S.-China Economic and Security Review Commission, October 2009), p. 19. [http://www.uscc.gov/researchpapers/2009/DGI%20Report%20on%20PRC%20Defense%20Industry%20%20Final%20Version%20with%20USCC%20seal\\_%2002Nov2009%20\\_2\\_.pdf](http://www.uscc.gov/researchpapers/2009/DGI%20Report%20on%20PRC%20Defense%20Industry%20%20Final%20Version%20with%20USCC%20seal_%2002Nov2009%20_2_.pdf).

269. Micah Springut, Stephen Schlaikjer, and David Chen, “China’s Program for Science and Technology Modernization: Implications for American Competitiveness” (prepared by CENTRA, Inc., for the U.S.-China Economic and Security Review Commission, 2011), p. 57. [http://www.uscc.gov/researchpapers/2011/USCC\\_REPORT\\_China%27s\\_Program\\_forScience\\_and\\_Technology\\_Modernization.pdf](http://www.uscc.gov/researchpapers/2011/USCC_REPORT_China%27s_Program_forScience_and_Technology_Modernization.pdf).

270. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

271. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

272. Mark Stokes, “China’s Evolving Conventional Strategic Strike Capability” (Arlington, VA: Project 2049 Institute, September 14, 2009), p. 20. [http://project2049.net/documents/chinese\\_anti\\_ship\\_ballistic\\_missile\\_asbm.pdf](http://project2049.net/documents/chinese_anti_ship_ballistic_missile_asbm.pdf).

273. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), p. 98.

274. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011; for additional background, see Dean Cheng and Peter Cugley, *The PRC [People's Republic of China] Space Program: An Open Source Examination* (Arlington, VA: CNA, September 2008), pp. 18–20.

275. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Scott Pace, May 11, 2011.

276. Michael Sheehan, "Tiangong-1 launch betrays China's earthly ambitions," BBC News, September 29, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-15089720>.

277. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

278. U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China* (Washington, DC: 2010), p. 36. [http://www.defense.gov/pubs/pdfs/2010\\_CMPR\\_Final.pdf](http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf).

279. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

280. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

281. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

282. Eric Hagt, "Emerging Grand Strategy for China's Defense Industry Reform," in Roy Kamphausen, David Lai, and Andrew Scobell, eds., *The PLA at Home and Abroad: Assessing The Operational Capabilities Of China's Military* (Carlisle, PA: U.S. Army War College Strategic Studies Institute, June 2010), p. 522. Cited in U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

283. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

284. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

285. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

286. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

287. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

288. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.

289. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Bruce MacDonald, May 11, 2011.

290. U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2009), p. 115.

291. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impact*, written testimony of Dean Cheng, January 27, 2011.

292. Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005). OSC ID: CPP20091231572001.

293. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impact*, written testimony of Dean Cheng, January 27, 2011.

294. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Mark Stokes, May 11, 2011.

295. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

296. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Mark Stokes, May 11, 2011.

297. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Mark Stokes, May 11, 2011.

298. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Alanna Krolikowski, May 11, 2011.

299. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Mark Stokes, May 11, 2011.

300. U.S.-China Economic and Security Review Commission, *Hearing on China's Emergent Military Aerospace and Commercial Aviation Capabilities*, testimony of Roger Cliff, March 20, 2010.

301. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, testimony of Frank Wolf, May 11, 2011.

302. U.S.-China Economic and Security Review Commission, *Hearing on China's Emergent Military Aerospace and Commercial Aviation Capabilities*, testimony of Wayne Ulman, March 20, 2010.

303. Mark Stokes, "China's Evolving Conventional Strategic Strike Capability" (Arlington, VA: Project 2049 Institute, September 14, 2009), p. 14. [http://project2049.net/documents/chinese\\_anti\\_ship\\_ballistic\\_missile\\_asbm.pdf](http://project2049.net/documents/chinese_anti_ship_ballistic_missile_asbm.pdf).

304. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Barry D. Watts, May 11, 2011.

305. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

306. *Washington Times*, "U.S. deploys warfare unit to jam enemy satellites," September 21, 2005. <http://www.washingtontimes.com/news/2005/sep/21/20050921-102706-1524r/>.

307. *Economist*, "Endangered birds," December 9, 2010. <http://www.economist.com/node/17647639>.

308. Matt Peckham, "Astronauts Safe From Space Debris Threat to International Space Station," *Time*.com, April 5, 2011. <http://techland.time.com/2011/04/05/crew-seeks-cover-as-space-debris-threatens-international-space-station/#ixzz1SfxcMKgv>.

309. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Bruce MacDonald, May 11, 2011.

310. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Dean Cheng, May 11, 2011.

311. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

312. For example, see U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Programs*, written testimony of Dean Cheng, May 11, 2011.

313. Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005), pp. 68–71. OSC ID: CPP20091231572001.

314. Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005), p. 70. OSC ID: CPP20091231572001.

315. Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005), p. 59. OSC ID: CPP20091231572001.

316. Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005), p. 68. OSC ID: CPP20091231572001.

317. Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005), pp. 59, 69. OSC ID: CPP20091231572001.

318. Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005), p. 68. OSC ID: CPP20091231572001.

319. Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005), pp. 69–70. OSC ID: CPP20091231572001.

320. Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005), p. 68. OSC ID: CPP20091231572001.

321. Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing, China: National Defense Industries Press, 2005), p. 59. OSC ID: CPP20091231572001.

322. Roger Cliff, Chad J.R. Ohlandt, and David Yang, “Ready for Takeoff: China’s Advancing Aerospace Industry” (contracted research paper for the U.S.-China Economic and Security Review Commission, 2011), pp. 107–11. [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf).

323. Roger Cliff, Chad J.R. Ohlandt, and David Yang, “Ready for Takeoff: China’s Advancing Aerospace Industry” (contracted research paper for the U.S.-China Economic and Security Review Commission, 2011), p. 111. [http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5B1%5D.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5B1%5D.pdf).

324. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Gregory L. Schulte, May 11, 2011; Office of the Director of National Intelligence, *National Security Space Strategy Unclassified Summary* (Washington, DC: U.S. Department of Defense, January 2011.)

325. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Gregory L. Schulte, May 11, 2011.

326. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Dean Cheng, May 11, 2011.

327. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Mark Stokes, May 11, 2011.

328. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, testimony of Gregory L. Schulte, May 11, 2011.

329. U.S.-China Economic and Security Review Commission, *Hearing on China’s Active Defense Strategy and its Regional Impact*, written testimony of David A. Deptula, January 27, 2011.

330. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Gregory L. Schulte, May 11, 2011.

331. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Scott Pace, May 11, 2011.

332. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China’s Military and Civil Space Programs*, written testimony of Clay Moltz, May 11, 2011.



## **CHAPTER 3**

### **CHINA'S FOREIGN POLICY**

#### **SECTION 1: AN OVERVIEW OF CHINA'S RELATIONS WITH NORTH KOREA AND IRAN**

##### **Introduction**

Despite Beijing's stated claim to be a responsible major power, China continues to place its national interests ahead of regional stability by providing economic and diplomatic support to countries that undermine international security. In particular, China continues to have strong relations with two countries that have the most potential to destabilize their regions of the world, North Korea and Iran. Despite Pyongyang's growing isolation as the result of its recent provocative actions, Beijing continues to defend its long-time ally and provide it with much-needed economic support. China also continues to invest in and trade with Iran, despite Iran's support for international terrorism and pursuit of weapons of mass destruction. China's support for these regimes provides the two countries with resources that could be used to defy international sanctions and threaten the stability of the region. This section of the Annual Report provides an overview of China's relations with these nations in recent years.

##### **China's Support for North Korea**

Over the past year and a half, the Democratic People's Republic of Korea (or North Korea) has acted in a destabilizing fashion, increasing the chances for conflict on the Korean Peninsula. In 2010, North Korea attacked and sank a South Korean naval vessel, revealed a previously unknown uranium enrichment facility, and shelled a South Korean island. In response, most of the international community increasingly distanced itself economically and diplomatically from North Korea. China, however, has taken a different approach and instead continues to support its neighbor and ally, all the while refusing to criticize publicly the North for its actions.\* China's continued support for North Korea reflects Beijing's

---

\*It should be noted that in the past, China has pressured North Korea behind the scenes to refrain from overly destabilizing activities. For example, in 2006, media reports claimed that China shipped no oil to North Korea for an entire month. Although there was no formal announcement that China's action was an attempt to pressure North Korea, the embargo did occur one month after North Korea's October 2006 nuclear test. Although one Japanese expert claimed China cut off oil supplies to North Korea after North Korea shelled a South Korean island, Commission staff were unable to discover any confirmation of the oil embargo. Furthermore, a review of China's exports to North Korea showed that while China's oil exports to North Korea did drop in the third and fourth quarter of 2010, the decline is similar to previous declines in China's oil exports to North Korea in the latter half of 2006 through 2009. Joseph Kahn, "China

Continued



desire to prevent the collapse of the North Korean regime and the negative impact this could have on China's economic and social stability. As a result, China is of its own volition in a "mutual hostage situation" where it feels forced to continue to support North Korea despite, and increasingly due to, the North's destabilizing activities.

### ***China's diplomatic support for North Korea***

Throughout 2010 and into 2011, China continued to support and defend North Korea against international pressure despite North Korean activities that had the potential to cause a war in Northeast Asia. After North Korea torpedoed a South Korean naval vessel in March 2010, killing 46 sailors,\* China refrained from condemning the attack or implicating North Korean involvement.<sup>1</sup> Instead, China waited a month to respond publicly to the sinking, at which time China simply referred to the incident as a "tragedy."<sup>2</sup> When a multinational report concluded a few months later that North Korea was indeed responsible, China refused to accept the findings and instead continued to call the incident a "mysterious naval tragedy."<sup>3</sup> Beijing also used its position as a member of the United Nations (UN) Security Council to dilute a UN statement that would have condemned North Korea for the attack.<sup>4</sup>†

In late 2010, China again defended North Korea from international criticism despite the North's provocative actions. On November 20, 2010, Pyongyang revealed a previously unknown nuclear enrichment facility, developed in defiance of UN sanctions.‡ In response to the revelation, Chinese Foreign Ministry Spokes-

cut off exports of oil to North Korea—Asia—Pacific—International Herald Tribune," *New York Times*, October 30, 2006. <http://www.nytimes.com/2006/10/30/world/asia/30iht-oil.3334398.html>; Sunny Lee, "China cut off oil to stop N. Korea from retaliating against South," *Korea Times*, January 19, 2011. [http://www.koreatimes.co.kr/www/news/nation/2011/01/113\\_79966.html](http://www.koreatimes.co.kr/www/news/nation/2011/01/113_79966.html); and International Trade Centre, "Trade Map" (Geneva, Switzerland: September 30, 2011). [http://www.trademap.org/light/Bilateral\\_TS.aspx](http://www.trademap.org/light/Bilateral_TS.aspx).

\* On March 26, 2010, North Korea torpedoed a South Korean corvette, the *Cheonan*, killing 46 sailors. Although not immediately identified as the perpetrator of the attack, a North Korean minisubmarine was implicated as the attacker by a multinational study released a few months later. International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea," *Asia Report* 200 (Brussels, Belgium: January 21, 2011): 2–5.

† Beijing did protest loudly, however, when the United States and South Korea announced joint naval exercises, partially in response to North Korea's sinking of the *Cheonan*. Reacting to these exercises, China's Ministry of Foreign Affairs stated that "we firmly oppose foreign warships and military aircraft carrying out activities in the Yellow Sea and other Chinese coastal waters that affect China's security interests." China also subsequently held its own military exercises in the Yellow, East China, and South China seas. International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea," *Asia Report* 200 (Brussels, Belgium: January 21, 2011): 1; Qin Gang, spokesperson for the Chinese Ministry of Foreign Affairs, July 9, 2010, cited in Bonnie Glaser and Brittany Billingsley, "US-China Relations: Tensions Rise and Fall, Once Again," *Comparative Connections* 12:3 (October 2010); and Chris Buckley, "China denies military exercise aimed at U.S.," Reuters, June 29, 2010. <http://www.reuters.com/article/2010/06/29/us-china-military-idUSTRE65S1YU20100629>.

‡ On November 20, 2010, North Korea surprised the international community by revealing a previously unknown uranium enrichment facility at the Yongbyon Nuclear Complex. According to North Korean engineers, this facility produces low enriched uranium for fuel in a still-under-construction nuclear power reactor. However, Siegfried S. Hecker, codirector of Stanford University's Center for International Security and Cooperation and the first outsider invited to visit the facility, stated that the facility could produce either fuel for the nuclear reactor or, with modifications, weapons-grade uranium. Both the newly revealed facility and the future nuclear power reactor violate UN sanctions. Siegfried S. Hecker, "A Return Trip to North Korea's Yongbyon Nuclear Complex" (Stanford, CA: Stanford University, Center for International Security and Cooperation, November 20, 2010), p. 1. <http://iis-db.stanford.edu/pubs/23035/HeckerYongbyon.pdf>; International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea," *Asia Report* 200 (Brussels, Belgium: January 21, 2011): 11; and David E. Sanger, "North Koreans Unveil New Plant for Nuclear Use," *New York Times*, November 20, 2011. <http://www.nytimes.com/2010/11/21/world/asia/21intel.html>.

woman Jiang Yu simply expressed “that all sides should exercise calm and restraint, and maintain a responsible attitude to prevent tensions from escalating, playing a positive role in preserving the peace and stability of the peninsula.”<sup>5</sup> China’s first official statement expressing concern over North Korea’s new enrichment facility occurred two months later, during Chinese President and Communist Party Secretary Hu Jintao’s January 2011 visit to the United States. The joint statement from that visit noted that “the United States and China expressed concern regarding the DPRK’s [North Korea’s] claimed uranium enrichment program.”<sup>6</sup> Despite this statement, in the following month China maneuvered within the UN Security Council to block an expert report about the revelation of the new facility.<sup>7</sup> Less than a week after revealing the nuclear enrichment facility, China again blocked international pressure on North Korea when the North Korean military shelled a South Korean island, killing four South Koreans.\* Following the attack, China declined to criticize the North publicly and instead called for “emergency talks” between North Korea and South Korea.<sup>8</sup> China also maneuvered within the UN Security Council to successfully block a statement condemning the shelling.<sup>9</sup>

China has also sought to protect North Korea in light of its continued proliferation attempts over the past year. Over the course of the past year, several accounts of North Korean attempts to defy international sanctions have come to light. According to a 2010 report from an expert panel established by the United Nations, North Korea may be involved in “nuclear and ballistic missile related activities in certain countries including Iran, Syria and Myanmar.”<sup>10</sup> *The New York Times* reported that in defiance of UN Security Council Resolution 1874 North Korea smuggled, possibly through China, at least 19 intermediate-range ballistic missiles to Iran.<sup>11</sup> However, when the United Nations established an expert panel to investigate North Korea’s continued attempts to proliferate weapons of mass destruction, Beijing lobbied to delay the report’s release.<sup>12</sup> Ultimately unsuccessful, Beijing then switched tactics and attacked the authority of the report itself, stating that “[t]his does not represent the position of the Security Council, and nor [sic] does it represent the position of the relevant Security Council sanctions committee.”<sup>13</sup>

Besides defending North Korea against international pressure, Beijing also has sought publicly to portray its relationship with North Korea as strong and getting stronger. According to experts Scott Snyder, director of the Center for U.S.-Korea Policy at the Asia Foundation, and See-won Byun, a research associate at the same institute:

\* On November 23, 2010, the North Korean military shelled South Korea’s Yeonpyeong Island, killing two South Korean civilians and two South Korean marines. This was the first artillery attack on South Korean territory since the end of the Korean War in 1953. On August 10, 2011, North Korea again fired live artillery rounds into South Korea, this time in the maritime territory around the same island. John M. Glionna and Jung-yoon Choi, “North, South Korea Exchange Fire Along Tense Western Sea Border,” *LA Times*, August 10, 2011. <http://articles.latimes.com/2011/aug/10/world/la-fgw-koreas-exchange-fire-20110810>; and Peter Foster, “North Korean attack on Yeonpyeong Island is worst against civilians in 20 years,” *Telegraph* (United Kingdom), November 23, 2010. <http://www.telegraph.co.uk/news/worldnews/asia/southkorea/8153100/North-Korean-attack-on-Yeonpyeong-Island-is-worst-against-civilians-in-20-years.html>.

*China and North Korea took unprecedented steps to consolidate political ties through historic high-level party and military exchanges in October [2010] commemorating the 65th anniversary of the founding of the WPK [the Workers Party of Korea, North Korea's Communist Party] and the 60th anniversary of the entry of the Chinese People's Volunteers (CPV) into the Korean War.*<sup>14</sup>

During the 65th anniversary of the founding of North Korea's Communist Party, Zhou Yongkang, a member of the Standing Committee of the Politburo, led a delegation to China to meet North Korean leader Kim Jong Il.<sup>15</sup> Later that same month, President Hu and Chinese Vice President (and likely future President and Communist Party leader) Xi Jinping celebrated the 60th anniversary of China's entry into the Korean War, noting that "[t]he Chinese people will never forget the friendship—established in battle—with the DPRK's [North Korea] people and army."<sup>16</sup> In July 2011, at the 50th anniversary of the signing of the *Treaty of Friendship, Cooperation and Mutual Assistance between China and North Korea*, President Hu noted that "[i]t is the firm and unwavering strategic policy of the Chinese Party and Government to continue to strengthen and develop the traditional China-DPRK [North Korea] friendly and cooperative relations [and] boost high-level visits and exchanges and expand economic cooperation."<sup>17</sup>

Further demonstrating the heightened relationship despite North Korea's provocative activities is the number of high-level meetings between the two countries. For example, since May 2010, Kim Jong Il has made an unprecedented four trips to China.\* In addition, the past year has seen a large number of exchanges between the Chinese and the North Korean governments. Table 1, below, lists some of the major exchanges.

**Table 1: Timeline of Sino-North Korean Diplomatic Exchanges since the Attack on the Cheonan**

Date	Event
Mar. 30–Apr. 3, 2010	An Yonggi, director of the North Korean military's Foreign Affairs Department, visits Beijing and meets with Xu Caihou, vice chairman of the People's Republic of China (PRC) Central Military Commission
Apr. 29–May 1, 2010	Kim Yong Nam, North Korean legislator and president of the Presidium of the Supreme People's Assembly, visits Shanghai for the World Expo and meets with PRC President Hu Jintao
Aug. 16–18, 2010	Wu Dawei, PRC envoy on Korean Peninsula Affairs, visits North Korea and meets Kim Jong Il and Foreign Minister Pak Ui-chun

\*Mr. Kim's trips to China occurred in May and August 2010 and in May and August 2011. See Se Young Lee, "China Confirms Visit by North Korea's Kim," *Wall Street Journal*, May 22, 2011. <http://online.wsj.com/article/SB10001424052702304520804576339052444645420.html>; Evan Ramstad, "China, North Korea Tout Ties as Kim Exits," *Wall Street Journal*, August 30, 2010. <http://online.wsj.com/article/SB10001424052748703369704575461162930482200.html>; *Chosun Ilbo* (South Korea), "Cracks Open in N. Korea-China Ties," June 7, 2011. [http://english.chosun.com/site/data/html\\_dir/2011/06/07/2011060701031.html](http://english.chosun.com/site/data/html_dir/2011/06/07/2011060701031.html); and Mansur Mirovalev, "Kim Jong Il, North Korea Leader, Visits China," Associated Press, August 25, 2011. [http://www.huffingtonpost.com/2011/08/25/kim-jong-il-china\\_n\\_936054.html](http://www.huffingtonpost.com/2011/08/25/kim-jong-il-china_n_936054.html).

**Table 1: Timeline of Sino-North Korean Diplomatic Exchanges since the Attack on the *Cheonan*—Continued**

<b>Date</b>	<b>Event</b>
Sept. 30–Oct. 2, 2010	Choe Thae Bok, secretary of the Worker's Party of Korea Central Committee and chairman of the Supreme People's Assembly, leads delegation to China and meets with PRC President Hu Jintao
Oct. 9–11, 2010	Zhou Yongkang, member of the Chinese Communist Party's (CCP) Standing Committee, leads a delegation to North Korea and meets with Kim Jong Il
Oct. 14, 2010	Pyon In Son, vice minister of North Korea's People's Armed Forces, leads a military delegation to Beijing and meets with PRC Defense Minister General Liang Guanglie
Oct. 25, 2010	General Guo Boxiang, PRC vice chairman of the Central Military Commission, visits Pyongyang and meets with North Korean Premier Choe Yong-rim
Nov. 30–Dec. 4, 2010	Choe Tae Bok, chairman of the Supreme People's Assembly, visits Beijing and Jilin and holds talks with PRC State Councilors Wu Bangguo and Chen Zhili
Dec. 8–9, 2010	Dai Bingguo, PRC vice minister of foreign affairs, visits North Korea and meets with Kim Jong Il
Feb. 13–14, 2011	Meng Jianzhu, PRC state councilor and minister of Public Security, visits North Korea and meets with Kim Jong Il
Apr. 12, 2011	Zhang Mingqi, vice president of the All-China Federation of Trade Unions, visits North Korea and meets with Choe Ryong Hae, secretary of the Central Committee of the Worker's Party of Korea
Apr. 13, 2011	North Korea's first vice foreign minister, Kim Kye Gwan, visits China and meets with PRC Vice Foreign Minister Zhang Zhijun, Foreign Minister Yang Jiechi, and Special Representative for Korean Peninsula Affairs Wu Dawei
May 16–20, 2011	A delegation of the Chinese People's Political Consultative Conference (CPPCC) led by Chen Zongxing, vice chairman of the CPPCC National Committee, visits North Korea and meets Kim Yong Nam, president of the Presidium of the Supreme People's Assembly
June 9, 2011	Chen Deming, PRC minister of Commerce, visits North Korea and meets with Jang Song Taek, vice chairman of the DPRK National Defense Commission
June 10–14, 2011	A delegation led by Li Yuanchao, head of the CCP Organization Department, visits North Korea for a "strategic dialogue" with DPRK counterparts, meeting Kim Yong Nam, president of the Presidium of the Supreme People's National Assembly; Choe Thae Bok, chairman of the Supreme People's Assembly; and Kim Jong Il
June 24–28, 2011	Chen Zhenggao, deputy secretary of the Liaoning Provincial Party Committee and governor of Liaoning Province, leads a delegation to North Korea and meets North Korean Premier Choe Yong Rim in Pyongyang
July 9–12, 2011	Yang Hyong Sop, vice president of the Presidium of North Korea's Supreme People's Assembly, leads a delegation to China and attends a reception on July 10 hosted by Ji Jae Ryong, North Korea's ambassador to China, and attended by PRC State Councilor Dai Binguo

**Table 1: Timeline of Sino-North Korean Diplomatic Exchanges since the Attack on the *Cheonan*—Continued**

Date	Event
July 11–14, 2011	Zheng Dejiang, PRC politburo member and vice premier, travels to North Korea in celebration of the 50th anniversary of the Sino-North Korean mutual assistance treaty
July 9–12, 2011	Yang Hyong Sop, vice president of the Presidium of North Korea's Supreme People's Assembly, leads a delegation to China and attends a reception on July 10 hosted by Ji Jae Ryong, North Korea's ambassador to China, and attended by PRC State Councilor Dai Bingguo
July 22, 2011	Foreign Minister Yang Jiechi and North Korean counterpart Pak Ui Chun hold talks on the sidelines of the Asian Regional Forum in Bali. The PRC Foreign Ministry spokesperson expresses support for bilateral talks held on the sidelines between ROK (South Korea) and North Korean envoys of the Six-Party Talks Wi Sung-lac and Ri Yong-ho
Aug. 4–7, 2011	Chinese Navy fleet visits Wonsan, North Korea, where Vice Admiral Tian Zong, commander of China's northern fleet, is received by North Korean Rear Admiral Kim Myong Sik
Aug. 25–26, 2011	Jon Chang Bok, chief of the General Logistics Bureau of the Korean People's Army Armed Forces Department, leads a Korean People's Army delegation to China and meets Liao Xilong, chief of the PLA General Logistics Department, and Defense Minister Liang Guanglie

Sources: Scott Snyder and See-won Byun, "China-Korea Relations," *Comparative Connections* 12: 4 (Honolulu, HI: January 2011): 112–16; Scott Snyder and See-won Byun, "China-Korea Relations," *Comparative Connections* 13: 1 (Honolulu, HI: May 2011): 116–18; and Scott Snyder and See-won Byun, "China-Korea Relations: A Fragile China-ROK [Republic of Korea, or South Korea] Strategic Partnership," *Comparative Connections* 13: 2 (Honolulu, HI: September 2011): 106–10.

### ***China's economic support for North Korea***

In addition to diplomatic support, Beijing also continues to provide Pyongyang with economic support that North Korea increasingly needs due to its growing international isolation. As the Congressional Research Service noted, "China, with its huge economy and rapid rate of growth, is the lifeline that keeps [North Korea] alive."<sup>18</sup> Drew Thompson, former director of China Studies at the Center for the National Interest, wrote that:

*Chinese aid, trade, and investment are critical to North Korea's social stability and economic productivity and a key source of technology and hard currency. Presumably, without this trade and investment, Kim Jong Il would lack the means to secure the allegiance of elites that support his rule, making trade and investment with China particularly important for ensuring the regime's survival.*<sup>19</sup>

China is North Korea's largest trading partner.\*<sup>20</sup> Although accurate trade values for Sino-North Korean trade are unavailable,

\*In 2010, the top five importers of North Korean goods were (in order): China, South Korea, Egypt, South Africa, and the Russian Federation. The top five exporters to North Korea in 2010 were China, South Korea, Brazil, the Netherlands, and Egypt. International Trade Centre, "Trade Map" (Geneva, Switzerland: August 12, 2011). <http://www.trademap.org/light/Bilat->



international data estimate bilateral trade between China and North Korea in 2010 reached \$3.46 billion, an increase of 29 percent over 2009.<sup>21</sup> In 2010, China exported to North Korea \$2.3 billion worth of goods and imported \$1.2 billion. China's top five imports from the North in 2010 included coal (33 percent of total imports); mineral ores (21 percent of total imports); apparels (14 percent of total imports); finished iron and steel (9 percent of total imports); and fish and seafood products (5 percent of total imports).<sup>22</sup> China's primary exports to North Korea in 2010 were mineral fuels and oils (21 percent of total exports), followed by machinery (11 percent of total exports); electronics (8 percent of total exports); vehicles (7 percent of total exports); and plastics (4 percent of total exports).<sup>23</sup>

Despite the large trade deficit with China, North Korea gains more from the trade, since it is desperately dependent upon Chinese imports. In 2010, 52 percent of North Korea's imports came from China, more than double the amount imported from South Korea, the North's second-largest import source.<sup>24</sup> Jayshree Bajoria, a senior staff writer at the Council on Foreign Relations, estimated that China may provide an estimated 90 percent of North Korea's energy, 80 percent of its consumer goods, and 40 to 45 percent of its food.<sup>25</sup> In contrast, bilateral trade with North Korea constituted less than 0.2 percent of China's 2010 total global trade.<sup>26</sup> North Korea's dependency on China likely has increased over the past year, since South Korea, the North's other main trade partner, began curtailing trade with the North after last year's sinking of the *Cheonan*.<sup>27</sup> In May 2010, South Korea took the unprecedented step of banning all inter-Korean trade, except for items produced at North Korea's Kaesong Industrial Complex, a North Korean-South Korean joint industrial park. As a result of the partial ban, inter-Korean trade, from imposition of the ban to May 2011, decreased by 54 percent, down to \$118 million (excluding Kaesong Industrial Complex trade).\*

China also provides North Korea with much-needed foreign direct investment. China's investments in North Korea are concentrated in a few sectors. According to the Open Source Center, 43 percent of publicly listed Chinese-North Korean joint ventures were involved in some facet of natural resource production.<sup>28</sup> The two countries have established three joint special economic zones, all located in North Korea near the border with China.<sup>†</sup> <sup>29</sup> Chinese entities have also pledged to invest in several infrastructure projects. China's Shangdi Guanqun Investment Company, for example, is renovating North Korea's Rason port.<sup>30</sup> Of note, the announcement of the port project came just one month after North Korea's shelling of Yeonpyeong Island and the revelation of a sec-

eral TS.aspx; and United Nations, "United Nations Commodity Trade Statistics Database," <http://comtrade.un.org/db/>.

\*Of import, trade through the Kaesong Industrial Complex actually grew for the same period, reaching \$1.44 billion in 2010, a growth of \$103 million (54 percent) over 2009. Evan Ramstad, "Strong Kaesong Boosts Inter-Korean Trade," *Wall Street Journal*, May 27, 2011. <http://blogs.wsj.com/korearealtime/2011/05/27/strong-kaesong-boosts-inter-korean-trade/>.

†The zones are in the North Korean cities of Rason and Sinuiju and on the North Korean islands of Hwanggu'mp'yo'ng and Wihwa. Xinhua, "China, DPRK [Democratic People's Republic of Korea] to develop two economic zones," June 9, 2011. [http://www1.chinadaily.com.cn/china/2011-06/09/content\\_12667570.htm](http://www1.chinadaily.com.cn/china/2011-06/09/content_12667570.htm); and Jay Solomon and Jeremy Page, "Chinese Firm to Invest in North Korea," *Wall Street Journal*, January 19, 2011. <http://online.wsj.com/article/SB10001424052748704678004576090270026745368.html>.



ond uranium enrichment facility. Undisclosed Chinese companies are also investing in the construction of a highway from the port to the border with China and building a new bridge over the Yalu River, which separates China from North Korea.<sup>31</sup> Other Chinese joint venture investments include mineral and metal extraction and processing and low-end manufacturing facilities.<sup>32</sup>

Unlike in many other countries where China invests, the majority of Chinese investors operating in North Korea are not national state-owned enterprises but rather “privately owned companies and provincial, prefecture, and municipal-owned [state-owned enterprises],” according to Mr. Thompson.<sup>33</sup> Only four out of 138 known Chinese companies engaging in joint ventures in North Korea were national-level state-owned enterprises, and only two of the companies rank among China’s top 100.<sup>34</sup> According to an Open Source Center report, of 86 Chinese joint ventures in North Korea, approximately 65 percent originated from China’s northeastern provinces Heilongjiang, Liaoning, and Jilin, which border North Korea.<sup>35</sup> Explanations for the apparent lack of national-level investments are not clear, but it may provide China’s northeast provinces with some influence over China’s foreign policy (see sec. 2 of this chapter for more on provinces as foreign policy actors).

Unfortunately, accurate data on the amount of China’s investments in North Korea are unavailable. According to China’s Ministry of Commerce, China’s officially reported 2010 investments in North Korea totaled \$12.1 million, a 52 percent increase over 2009. China’s total investment in North Korea since 2004 equaled \$109.3 million.<sup>36</sup> Yet recent activities by China cast doubt upon these statistics or point to a recent radical uptick in investments. For example, a Chinese Foreign Ministry spokesperson stated that total investment in one of the special economic zones will be between \$300 million and \$500 million.<sup>37</sup> China’s funding for the Yalu bridge project is estimated at \$260 million.<sup>38</sup> The *Wall Street Journal* reported that China’s investment in the Rason port project is estimated at \$2 billion.<sup>39</sup> If the estimate is accurate, and the project is seen to completion, this will be China’s single largest investment in North Korea and nearly 20 times the size of China’s claimed 2004 to 2009 total investments in North Korea.

Although precise data are unavailable, China’s foreign direct investment in North Korea is substantial and provides the North with vital resources. Currently, excluding South Korea’s investment in the Kaesong Industrial Complex, China is North Korea’s largest foreign direct investor.<sup>40</sup> While figures for 2009 and 2010 are unknown, estimates indicate that in 2008 China provided 94 percent of all investments in North Korea.<sup>41</sup> \* Furthermore, while many nations are decreasing their investments in North Korea on account of its recent provocations,<sup>42</sup> China appears to be increasing its investment in North Korea as the large high-profile projects detailed above demonstrate.

\* By way of comparison, North Korea only receives a miniscule portion of China’s overall foreign direct investments: only .02 percent in 2010, according to China’s official statistics. Ministry of Commerce, People’s Republic of China, “2010 Niandu Zhongguo Duiwai Zhijie Touzi Tongji Gongbao” (Statistical Bulletin on China’s Outward Direct Investment, 2010) (Beijing, China: 2011), p. 82.

China also provides economic support to North Korea by only loosely implementing international sanctions against North Korea. According to a Congressional Research Service study, despite China's publicly strong support for UN sanctions against North Korea for its nuclear program, China takes a "minimalist approach" to enforcing those sanctions. The study continues, noting that China persists in allowing North Korea trade and financial transactions to transit Chinese territory without rigorous inspections, contrary to UN sanctions.<sup>43</sup> According to media reports, China has also been complicit in allowing North Korea's continued support of Iran's nuclear program by permitting cargo to transit through China unchecked and failing to act on U.S.-provided intelligence toward this end.<sup>44</sup> In addition, China continues to allow luxury goods, banned by UN sanctions, to flow unobstructed to North Korea.<sup>45</sup>

#### **UN Sanctions against North Korea**

Currently, the United Nations has two main sets of reinforcing sanctions against North Korea for Pyongyang's illicit weapons of mass destruction programs: UN Security Council Resolution 1718 and UN Security Council Resolution 1874.

*UN Security Council Resolution 1718*: passed in 2006 in response to North Korea's October 9, 2006, nuclear weapons test. This resolution called upon member states to refrain from purchasing or transferring to, or procuring from, North Korea large military platforms (such as tanks and aircraft), nuclear and ballistic missile components, and luxury items (undefined).<sup>46</sup>

*UN Security Council Resolution 1874*: passed in response to North Korea's May 12, 2009, nuclear weapons test, this resolution sought to tighten previous sanctions against North Korea. In particular, it called for expanding the arms embargo to all weapons except small arms, the active inspection of all goods traveling to and from North Korea, and the curtailing of economic transactions with North Korea except when in support of humanitarian or denuclearization purposes. This resolution also established an expert panel to assess current efforts of implementing sanctions on North Korea.<sup>47</sup>

#### ***China's military support for North Korea***

Despite active measures to support the North Korean regime both economically and diplomatically, China appears to be providing North Korea with only minimal military support. David F. Helvey, principal director for East Asia Policy, Office of the Secretary of Defense, described to the Commission how Beijing still has a mutual defense agreement with Pyongyang, the only mutual defense agreement to which China is still obligated.<sup>48</sup> In previous years, Beijing has provided military arms to North Korea but appears to have refrained at least publicly from such activities since

2009, the year of tightened UN sanctions.\* The two countries have also conducted several high-level military exchanges in recent years, including an October 2010 visit to North Korea by General Guo Boxiong, vice chairman of the Central Military Commission.<sup>49</sup> Furthermore, despite the Chinese military's growing international interactions,<sup>†</sup> Commission staff research turned up no confirmed reports of joint military exercises involving Chinese and North Korean troops in the past ten years. A Congressional Research Service report notes that although China supplied ballistic missile components to North Korea in the past, it is unclear whether China continues this support today.<sup>50</sup>

### ***Reasons behind China's support for North Korea***

The overarching goal of China's North Korea policy is to maintain stability in North Korea. A Commission-sponsored research report describes how China's policies toward North Korea revolve around preventing the collapse of the North Korean regime:

*[North Korea's] sinking of the South Korean naval ship Cheonan, the shelling of [South Korea's] Yeonpyeong Island, as well as the seemingly never-ending stand-off over North Korea's nuclear program and proliferation practices provide China with ample opportunity to play a constructive role. But all of China's actions or inactions have served to simply demonstrate that the overriding Chinese interest on the Korean Peninsula is to prevent any increased pressure on the North Korean regime that could potentially lead to an implosion.*<sup>51</sup>

Victor Cha, director of Asian Studies at Georgetown University, testified to the Commission that Beijing has decided to support the North “unconditionally” in order to preserve “a minimum amount of stability in North Korea . . . even if it means acquiescing to North Korean provocation.”<sup>52</sup>

Beijing fears a North Korean collapse for several reasons. Should the regime implode, it is likely that a large number of refugees, possibly in the hundreds of thousands, would attempt to flee the dire situation in North Korea by migrating across the border to China. Regional geography plays a major role in ensuring that any chaos in North Korea is likely to bleed over into China's northeast provinces of Liaoning, Heilongjiang, and Jilin. The China-North Korean border is 1,400 kilometers long, sparsely guarded, and very porous.<sup>53</sup> In contrast, North Korea's border with South Korea is heavily mined on both sides.<sup>54</sup> Furthermore, the majority of North Koreans reside along the border with China.<sup>55</sup> Therefore, according to the International Crisis Group, Beijing fears the “threat of an unsustainable flood of hundreds of thousands of refugees, bringing social, criminal and political problems with them.”<sup>56</sup> The resulting

\* In 2009, the Stockholm International Peace Research Institute reported that China supplied over \$4 million in small arms sales, the last such report. Stockholm International Peace Research Institute, “Arms Transfer Database” (Stockholm, Sweden: September 6, 2011). <http://www.sipri.org/research/armaments/transfers/transparency/databases/armstransfers>.

† For more on the Chinese military's growing international activities, see the Commission's 2009 Annual Report to Congress. U.S.-China Economic and Security Review Commission, 2009 Annual Report to Congress (Washington, DC: U.S. Government Printing Office, November 2009), pp. 113–127. [http://www.uscc.gov/annual\\_report/2009/09\\_annual\\_report.php](http://www.uscc.gov/annual_report/2009/09_annual_report.php).

economic and social strains would seriously impact China's already economically weak northeast, commonly referred to as China's "rust belt."<sup>57</sup>

Beijing also fears that a North Korean political and economic collapse could result in the unification of the peninsula under South Korea, an U.S. ally. Dr. Cha testified that "North Korea is a strategic piece of territory for China, not in the sense that it is intrinsically valuable, but in the sense that Beijing can never allow it to fall in the hands of the South or the U.S."<sup>58</sup> As Selig Harrison, director of the Asia Program at the Center for International Policy, described, "China does not want Korea to be reunified under a South Korean regime allied militarily with the United States, and therefore wants the survival of a pro-Beijing regime in Pyongyang."<sup>59</sup> By keeping a nominally friendly state on its border, China gains the benefit of a buffer state between it and South Korea and, more importantly, U.S. forces stationed in South Korea.<sup>60</sup> Having a buffer state on its borders has been a long-standing interest for Beijing, as demonstrated by its decision to intervene in the Korean War in 1950.<sup>61</sup> China's desire for a buffer state on its borders has grown since the United States declared that it was increasing its focus on East Asia in 2010.<sup>62</sup>

The collapse of the North's government and economy would also negatively impact China's economic interests in North Korea. As mentioned above, North Korea is not a major trade partner of China. However, it does possess natural resources that are valuable to China's continued economic development (see table 2, below). Natural resources accounted for roughly 40 percent (\$465 million) of China's total imports from North Korea in 2010.<sup>63</sup> Chaos within North Korea would inhibit China's ability to extract these resources. In addition, North Korea's collapse would also impact China's goal of developing its economically weak northeast region, which constitutes the bulk of Chinese investment in North Korea.<sup>64</sup> The chaos that would ensue from an implosion of the North Korean regime would also prohibit China from capitalizing on its growing infrastructure investments in North Korea.<sup>65</sup>

**Table 2: North Korea's Estimated Natural Resource Reserves**

<b>Resource</b>	<b>Estimated North Korean Reserves (tons)</b>
Anthracite coal	4,500,000,000
Asbestos	1,300
Barite	210,000
Copper	290,000
Fluorspar	50,000
Gold	200
Iron	5,000,000,000

**Table 2: North Korea's Estimated Natural Resource Reserves—Continued**

<b>Resource</b>	<b>Estimated North Korean Reserves (tons)</b>
Kaolinite	200,000
Lead	1,060,000
Lignite	16,000,000,000
Limestone	100,000,000,000
Magnesite	6,000,000
Molybdenum	5,400
Rosette graphite	200,000
Silver	300–500
Talcum	70,000
Tungsten trioxide	24,600
Uranium ore	400,000
Zinc	2,100,000,000

Source: Adapted from Gooheon Kwon, "A United Korea? Reassessing North Korea Risks (Part I)," (New York, NY: Goldman Sachs and Co., *Global Economics Paper No: 188*, September 21, 2009), p. 10.

Because China's primary goal vis-à-vis North Korea is to prevent North Korea's collapse, coupled with North Korea's need for Chinese support, the two nations find themselves in what Dr. Cha has referred to as a "mutual hostage" situation. Testified Dr. Cha:

*In the end, [China's] support [for North Korea] derives less from some anachronistic communist allegiance, and more from the fact the two are mutual hostages: North Korea needs China to survive. It hates this fact of life and resists all Chinese advice to change its ways. China needs North Korea not to collapse. It hates this fact. And as the only patron supporting the decrepit regime today, it is, ironically, powerless more than it is omnipotent because the regime's livelihood is entirely in Chinese hands. It must therefore countenance [North Korean] bad behavior because any punishment could destabilize the regime.<sup>66</sup>*

### **China's Support for Iran**

China's relationship with Iran is characterized by the prioritization of national interests over international stability. In recent years, while a growing number of states are divesting themselves of investments in Iran's petroleum industry, China has sought to take advantage of these new investment opportunities. China also continues to provide Iran with refined petroleum products, such as gasoline, despite U.S. attempts to embargo this product. Furthermore, open source reporting notes that China may be selling Iran advanced conventional weapons, which would provide Tehran with a growing capacity to threaten U.S. interests in the region.

***U.S. sanctions against third-party involvement in Iran***

Over the past several decades, the United States has imposed a series of sanctions on Iran to deter it from supporting international terrorism, pursuing weapons of mass destruction, and abusing human rights. While most of the laws target U.S. companies interacting with Iran, several U.S. laws specifically target foreign companies dealing with Iran.\* These acts mandate that the U.S. government impose three or more of a possible set of nine sanctions upon a foreign entity that is found to violate one of the provisions of the sanctions. Violations include investing in Iran's petroleum industry, supplying it with refined petroleum products, and providing it with technology or know-how related to weapons of mass destruction or advanced conventional weapons. Corresponding penalties include such actions as denying Export-Import Bank loans and export licenses of U.S. military technology to the offending entity, barring the entity from winning U.S. government procurement contracts, and prohibiting the entity from importing goods to the United States or acquiring any U.S.-based property. The various acts also allow the U.S. president to waive the sanctions should it be in the national interest of the United States, or if the foreign entity's home country is cooperating to prevent Iran from acquiring weapons of mass destruction or destabilizing numbers and types of conventional weapons.<sup>67</sup>

***China's views on U.S. sanctions***

Beijing views Washington's attempts to punish foreign firms dealing with Iran as the extraterritorial application of U.S. domestic law and thus as an infringement of another state's sovereignty. In response to the December 2005 announcement by the Bush Administration that the United States was sanctioning six Chinese firms† under *The Iran Sanctions Act*, China's Ministry of Foreign Affairs quickly noted its disagreement with the legality of the U.S. law:

*The United States has expressed dissatisfaction with the export of certain items by Chinese enterprises, and has implemented sanctions against these Chinese enterprises under [U.S.] domestic law, to which we indicate our opposition. The reason is simple. The U.S.-imposed sanctions on these Chinese enterprises are not in accordance with international law, nor are they in accordance with international requirements on non-proliferation. Instead they are in accordance with their domestic law. We demand that the U.S. stop the relevant sanctions in order to facilitate the healthy development of Sino-U.S. economic and trade relations on the basis of equality and mutual benefit. At the same time*

\*These laws, collectively referred to as *The Iran Sanctions Act*, include the *Iran Sanctions Act of 1996*, the *Iran Nonproliferation Act of 2000*, the *Iran Nonproliferation Amendment Act of 2005*, the *North Korea Nonproliferation Act of 2006*, the *Iran Freedom Support Act of 2006*, and the *Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010*.

†The six companies were China Aero-Technology Import and Export Corporation (CATIC), China North Industries Corporation (Norinco), Hongdu Aviation Industry Group, Limmt Metallurgy and Minerals Company, Ounion (Asia) International Economic and Technical Cooperation Ltd., and Zibo Chemet Equipment Company. David E. Sanger, "U.S. to Punish 9 Companies Said to Help Iran on Arms," *New York Times*, December 28, 2005. <http://www.nytimes.com/2005/12/28/international/asia/28china.html>.



*we also clearly express, that if we find that Chinese enterprises have truly acted in violation of Chinese government laws and regulations, we will earnestly pursue the issue and punish in accordance with the law.*<sup>68</sup>

China also opposed the 2010 passage of *The Comprehensive Iran Sanctions, Accountability, and Divestment Act*. Following this law's enactment, a spokesperson for the Chinese Ministry of Foreign Affairs stated that:

*China has already noted the U.S. and other parties' announcements to implement unilateral sanctions against Iran. Not long ago, the U.N. Security Council approved Resolution 1929 concerning Iran's nuclear issue. China believes that all nations should fully, seriously, and correctly enforce this Security Council resolution, and avoid interpreting it as one pleases in order to expand the Security Council's sanctions.*<sup>69</sup>

Because Beijing disputes the legality of the U.S. laws, China is generally unwilling to comply with U.S. sanctions regarding Iran. According to John W. Garver, professor of International Relations at the Georgia Institute of Technology:

*Beijing was less willing than the European countries and Japan to follow U.S. policy advice on Iran or to bow before U.S. unilateral actions penalizing non-U.S. firms for involvement in Iran's energy sector. Beijing's greater independence from Washington served China's interest in penetrating Iran's energy sector. China's support for Iran over the nuclear issue and against U.S. pressure also inclined Tehran to see China as a relatively reliable and like-minded partner.*<sup>70</sup>

#### ***China's investments in Iran's petroleum industry and provision of refined petroleum products***

While the fear of U.S. sanctions has caused many businesses to limit or cease operations in Iran, Chinese firms have seen these sanctions as an opportunity for expansion. According to a 2011 report by the Government Accountability Office, 20 of the 38 non-Chinese foreign companies with investments in Iran's petroleum industry prior to 2010 have divested (or are in the process of divesting). As these companies leave, however, Chinese (and Indian) companies use the openings to expand their investment in Iran.<sup>71</sup> Dr. Garver testified that by 2009, China and Iran were major energy partners, particularly since 2009, when "Chinese firms entered into eight new energy deals, many of which had been abandoned by Western firms under fear of U.S. sanctions."<sup>72</sup> Robert J. Einhorn, special advisor for nonproliferation and arms control at the U.S. Department of State, referred to China's practice of taking over other countries' contracts when they divest from Iran as "backfilling," which he criticized as "taking advantage of the responsible restraint of other countries."<sup>73</sup> An example of China's backfilling of divested western investments is exemplified by China National Petroleum Corporation, which expanded its investment in

Iran's South Pars Gas Field after several foreign gas companies pulled out of the project.<sup>74</sup>

There is mixed evidence on whether China may be quietly tapering off its investments in Iran's petroleum industry. In April 2011, Mr. Helvey testified to the Commission that the United States had "not seen evidence of new PRC investments in Iran's energy sector." He continued, noting, however, that China still maintains its old investments and that it is continuing to invest in Iran's other extractive resources, such as aluminum, copper, and coal.<sup>75</sup> Erica S. Downs, a fellow at The Brookings Institution, testified to the Commission in April 2011 that "recently, China's national oil companies appear to be following Washington's warning not to backfill projects abandoned by European oil companies and other firms in Iran."<sup>76</sup> According to a September 2011 Reuters article, a Chinese slowdown in further investments in Iran's petroleum industry may reflect "Beijing's efforts to appease Washington and avoid U.S. sanctions on its big energy firms."<sup>77</sup> Table 3, below, lists known Chinese investments in Iran's petroleum industry.

**Table 3: Chinese investments in Iran's Petroleum Industry, 2005-present**

Chinese Company	Activity	Status	Commercial activity
China National Off-shore Oil Cooperation (CNOOC)	Development of the North Pars natural gas field and construction of a liquefied natural gas plant	Initial agreement reached 2006–2007; final agreement signed 2009; expected completion in 2015.	Project valued at \$16 billion; CNOOC to receive 50 percent share of liquid natural gas product
China National Petroleum Corporation (CNPC)	Oil exploration and development project in Masjed-i-Suleiman oil field	Progress stalled since 2010, and the February 2011 deadline was missed	CNPC has a 75 percent holding in project
	Development of Block 3 oil field in the Zagros Basin	Second exploration well started in December 2007	unknown
	Development of the North Azadegan oil field	Equipment procurement problems likely to delay production	Providing 90 percent of the financing under a buyback contract, a \$2+ billion investment
	Development of the South Pars phase 11 natural gas project (replacing France's Total SA)	Contract signed June 2009; deal finalized in February 2010	12.5 percent share of project valued at more than \$4.7 billion
Sinopec	Development of the Yadavaran oil field	Production scheduled to begin in next 1–2 years	Contract valued between \$2 and \$3.6 billion
	Expansion and upgrade of the Arak refinery	As of 2008, estimated completion date was 2011	Contract valued at \$2.8 billion.

**Table 3: Chinese investments in Iran's Petroleum Industry, 2005-present—Continued**

Chinese Company	Activity	Status	Commercial activity
	Development of additional refinery capability	Memorandum of Understanding signed in November 2009; possibly finalized in February 2010	Contract valued at \$6.5 billion

Source: U.S. Government Accountability Office, "Iran's Oil, Gas, and Petrochemical Sectors" (Washington, DC: March 23, 2010), pp. 12–17; U.S. Government Accountability Office, "Firms Reported in Open Sources as Having Commercial Activity in Iran's Oil, Gas, and Petrochemical Sectors" (Washington, DC: August 3, 2011), pp. 16–18; and Foundation for Defense of Democracies, "Iran Energy Project" (Washington, DC: September 7, 2011). <http://www.defend-democracy.org/project/iran-energy-project/>.

However, other reports provide a different picture. In August 2011, a Reuters article noted that Sinopec Engineering Inc., an arm of the state-owned Sinopec, started up a refining unit in Iran's Arak refinery.<sup>78</sup> Although the actual value of this last investment is unknown, an earlier media report noted that Sinopec had signed a Memorandum of Understanding with Iran in November 2009 to invest \$6.5 billion in Iran's oil refineries.<sup>79</sup> In addition, in September 2011, Iran's state-controlled Pars Oil and Gas Company announced that China National Petroleum Company will resume work on Iran's South Pars Gas Field, on hold since 2009.<sup>80</sup> In addition, the U.S. Government Accountability Office in its August 2011 report listed Chinese investment projects in Iran as currently still active.<sup>81</sup>

China is also one of the few countries still willing to sell Iran refined petroleum products.<sup>82</sup> According to the Congressional Research Service, as of mid-2010, China was supplying Iran with about half of Iran's total gasoline imports.<sup>83</sup> Dr. Garver testified that as western companies began tapering off their sales of gasoline to Iran, "China was stepping in to help Iran off-set that Western pressure."<sup>84</sup> Five Chinese companies, each a state-owned enterprise, shipped gasoline to Iran in 2010. ChinaOil, a subsidiary of China National Petroleum Corporation, shipped 600,000 barrels of gasoline to Iran, valued at \$55 million. Sinopec and its subsidiary, Unipet, both shipped a total of 850,000 barrels of gasoline to Iran in 2010 for an undisclosed amount.<sup>85</sup> Two other state-owned enterprises, Zhuhai Zhenrong and Zhenhua Oil, also reportedly supplied Iran with gasoline in 2010.<sup>86</sup>

Despite China's investments in Iran's petroleum industry, and the provision of refined oil products to Iran, the U.S. government has not sanctioned any Chinese state-owned oil company. Noting this fact, Dr. Garver asserted:

*Between 2002 and 2009, nearly 40 Chinese entities were sanctioned 74 times by the United States under U.S. legislation and Executive Orders. Interestingly, however, none of China's oil majors were among the Chinese firms sanctioned in spite of those firms' vigorous entry into Iran's energy sector in the late 2000s and in spite of the apparent applicability of U.S. sanctions laws to those firms' investment in Iran's energy sector.*<sup>87</sup>

When asked by Commissioners about this discrepancy during a hearing in 2011, Daniel Kritenbrink, then acting deputy assistant secretary for East Asian and Pacific Affairs at the U.S. State Department, replied:

*We have made very clear to China that we expect them to show restraint in investments in the energy sector, and this is both in line with U.N. Security resolutions and with U.S. law. China has voted in favor of these Security Council resolutions, and stated that it shares our goal in fully implementing them. And we watch this very carefully and will continue to do so. If we find instances of where Chinese firms have violated those obligations, I can assure you we're going to look at that very carefully and engage with the Chinese very seriously.*<sup>88</sup>

***China's provision of arms and weapons of mass destruction-related materials to Iran***

According to open source reporting, China continues to provide Iran with advanced conventional weapons, an act that could be in violation of U.S. sanctions against Iran.<sup>89</sup> The Stockholm International Peace Research Institute, which tracks open source reporting of international arms sales, notes that over the past five years, China has sold \$312 million worth of arms to Iran, second only to Russia, which supplied Iran with \$684 million worth of arms.<sup>90</sup> Furthermore, since Russia began decreasing its arms sales to Iran in 2008, China has become Iran's largest arms supplier.\*<sup>91</sup> As shown in table 4 below, China's arms sales since 2006 have consisted almost entirely of antiship cruise missiles. In addition to direct sales, there have been media reports that China constructed a missile plant in Iran in 2010 to produce the Nasr-1 antiship cruise missile.<sup>92</sup> In response to a query from the Commission, the U.S. Department of State noted that if these reports are true, the provision of these cruise missiles would be "potentially sanctionable."<sup>93</sup>

**Table 4: Partial List of China's Arms Sales to Iran, 2006–2010**

Item	Quantity	Date Delivered	Range
C-802 antiship cruise missile	340	1994–2010	120 kilometers (km)
FL-6 antiship cruise missile	225	1999–2010	32 km
TL-10/FL-8 antiship cruise missile	120	2004–2010	c. 20 km

\* For example, in September 2010, Russia withdrew from a \$1 billion sale to Iran of Russia's advanced air defense systems, the S-300. United Press International, "Russia ending S-300 Iran deal costs \$1B," September 29, 2010. [http://www.upi.com/Business\\_News/Security-Industry/2010/09/29/Russia-ending-S-300-Iran-deal-costs-1B/UPI-59401285794692/#ixzz1ZLj7ANAk](http://www.upi.com/Business_News/Security-Industry/2010/09/29/Russia-ending-S-300-Iran-deal-costs-1B/UPI-59401285794692/#ixzz1ZLj7ANAk).

**Table 4: Partial List of China's Arms Sales to Iran, 2006–2010—Continued**

Item	Quantity	Date Delivered	Range
C-704 antiship cruise missile	25	2010	c. 35 km
C-801 antiship cruise missile	25	2006–2010	40–80 km
QW-11 man-portable surface-to-air missile	500	2006–2010	5 km

Source: Stockholm International Peace Research Institute, “Arms Transfer Database” (Stockholm, Sweden: September 6, 2011). <http://www.sipri.org/databases/armstransfers>; Global Security.org, “Chinese Missiles.” [www.globalsecurity.org/military/world/china/missile.htm](http://www.globalsecurity.org/military/world/china/missile.htm).

Although officially China ended all assistance for Iran's nuclear program in 1997 due to international pressure, there has been speculation that China, or Chinese entities, have quietly continued to provide some support for Iran's pursuit of weapons of mass destruction and ballistic missile capabilities.<sup>94</sup> Chinese companies were accused in March 2009 and 2010 of providing sensitive materials to Iran for its nuclear program.<sup>95</sup> In April 2009, a New York grand jury indicted the Chinese firm LIMMT Economic and Trade Co. for covertly using U.S. banks to finance the sale of restricted high-strength metals with military applications to subsidiaries of an Iranian military agency, potentially supporting Tehran's ballistic missile and nuclear weapons programs.<sup>96</sup> Secretary of State Hillary Rodham Clinton noted during President Hu's January 2011 visit to the United States that “we think that there are some entities within China that we have brought to the attention of the Chinese leadership that are still not, shall we say, as in compliance as we would like them to be” with international efforts to not provide Iran with nuclear technology and know-how.<sup>97</sup> In late spring 2011, a UN report posited that Iran had acquired ballistic missile technology from North Korea by transshipping the technology through “a neighboring third country,” alleged to be China.<sup>98</sup> In May 2011, the U.S. State Department sanctioned three Chinese companies and one Chinese citizen for their role in weapons proliferation involving Iran under *The Iran, North Korea, and Syria Nonproliferation Act*.<sup>99</sup> It is unclear from reports, however, what items were proliferated and what was sent specifically to Iran, as opposed to Syria or North Korea.

### ***Implications for the United States***

China's continued support for Iran and North Korea have several implications for the United States. By continuing to defend Iran and North Korea in international fora, China undermines international efforts to compel these countries to discontinue pursuing agendas and programs that destabilize their respective regions. China's tactics to weaken and delay international resolutions and reports provide both North Korea and Iran with valuable time to develop their respective nuclear programs. Knowing that they can rely on China to defend them from international criticism creates

\*The individuals and entities sanctioned were Karl Lee, Dalian Sunny Industries, Dalian Zhongbang Chemical Industries Company, and Xian Junyun Electronic.

Office of the Spokesperson, “Fact Sheet: Iran, North Korea and Syria Nonproliferation Act” (Washington, DC: U.S. Department of State, May 24, 2011). <http://www.state.gov/r/pa/prs/ps/2011/05/164129.htm>.

moral hazard in Pyongyang and Tehran where China's support insulates North Korea and, to a lesser extent, Iran, from the risk of their actions. As a consequence, China's diplomatic defense could embolden these nations, particularly North Korea, to undertake further destabilizing actions.

China's economic relationships with North Korea and Iran undermine international attempts to dissuade sanctioned activities by providing these regimes with a means to acquire much-needed capital. Chinese investments and infrastructure deals provide hard currency that can be diverted to finance questionable programs. By providing valuable commodities, such as refined petroleum, to Iran, China allows the North Korean and Iranian elites to maintain their hold on these countries. Furthermore, China's lax implementation of international sanctions allows these countries to continue to both acquire and proliferate sanctioned items.

Finally, if reports of China's arms sales to Iran are true, China's willingness to continue to sell to Iran advanced conventional arms and dual-use technology would enhance Iran's conventional military capabilities, thus providing Iran with a growing capacity to threaten the region. A study from the Center for Strategic and Budgetary Assessments notes that, like China, "Iran seems determined to continue developing more formidable A2/AD [antiaccess and area denial] capabilities." To this end, China-supplied ballistic and cruise missiles "could be used not only to target Persian Gulf shipping, but also to hold at risk the oil and natural gas production facilities (to include overland pipelines) of other Gulf states."<sup>100</sup> Even minimal physical damage, for example, to Saudi Arabian production, refinement, or overland transport capacity would disproportionately affect energy markets and surge prices.<sup>101</sup> With respect to shipping, China's provision of antiship cruise missiles to Iran could allow Iran to target, among other things, oil tankers transiting the Strait of Hormuz. According to one analysis of this threat, "[e]xtended closure of the strait would remove roughly a quarter of the world's oil from the market, causing a supply shock of the type not seen since the glory days of OPEC [Organization of Petroleum Exporting Countries]."\* Even relatively limited or ineffectual attacks could cause tanker operations in the area to cease or would at least increase insurance rates.<sup>102</sup>

## Conclusions

- China has continued over the past year to support North Korea despite North Korea's destabilizing actions. Diplomatically, China shields North Korea from pressure in international fora. China also continues to trade with and invest in North Korea, providing it with an economic lifeline in the face of growing international ostracism. Beijing's continued support for Pyongyang is primarily driven by its fear of a collapse of the North Korean regime and the consequences this would have for

\*This analysis also reviews Iranian mine warfare and missile warfare capabilities. It concludes that, between mines and missiles, "[i]t does not take much imagination to suggest that the traffic in the Strait of Hormuz could be impeded for weeks or longer, with major air and naval operations required to restore the full flow of traffic." See Caitlin Talmadge, "Closing Time: Assessing the Iranian Threat to the Strait of Hormuz," *International Security* 33: 1 (Cambridge, MA: Summer 2008): 82.



China's economic, social, and security interests; as well as the fear of the loss of a buffer state on its border.

- Despite U.S. efforts to sanction Iran for its support of international terrorism and pursuit of weapons of mass destruction, China remains a large investor in Iran's petroleum industry and a major provider of refined oil products. China may also be supplying Iran with advanced conventional weapons, such as cruise missiles. China's investments in Iran's petroleum industry, and its continued provision of gasoline and advanced conventional weapons, may be at odds with U.S. laws.
- Continued Chinese support for North Korea and Iran demonstrates China's willingness to place its national interests ahead of regional stability by providing economic and diplomatic support to countries that undermine international security.

## **SECTION 2: ACTORS IN CHINA'S FOREIGN POLICY**

### **Introduction**

Through a combination of hearings, two fact-finding trips to East Asia, and research over the past year, the Commission investigated the changing dynamics of China's foreign policy-making. Overall, the Chinese Communist Party (CCP) elite, the party's Politburo Standing Committee, continue to exert overarching control of China's foreign policy-making. Other party and government entities, such as the Ministry of Foreign Affairs, the People's Liberation Army (PLA), and provincial actors, influence and implement China's foreign policies. However, as China has expanded its overseas interests, the number of voices affecting Chinese foreign policy also has increased. Chinese state-owned enterprises (SOEs) and banks, and think tanks and academic institutions have increasing influence on China's foreign policies. In addition, private citizens may have a modicum of ability to influence foreign policies through the use of the Internet. As a result of the growing number of players influencing China's foreign policy-making process, coordination among the various actors is more difficult for Beijing. The following section will describe the actors creating, implementing, and influencing Chinese foreign policy and what implications the proliferation of voices could have for the United States.

### **Official Chinese Foreign Policy Actors**

China's official foreign policy actors include individuals and organizations in the CCP apparatus and in the Chinese government under the State Council. The most influential actors are the Politburo Standing Committee, the Foreign Affairs Leading Small Group, the Ministry of Foreign Affairs, the PLA, and on a smaller scale, provincial governments.

#### ***Politburo Standing Committee of the CCP***

Comprising the top nine members of the CCP, the Politburo Standing Committee is the ultimate body that approves foreign policy decisions. Although it does not publicize its agenda, the Politburo Standing Committee reportedly meets every seven to ten days and operates on a consensus basis; no one member has exclusive say over foreign policy decisions.<sup>103</sup> In testimony to the Commission, Susan Lawrence, an analyst at the Congressional Research Service, stated that the two members of the Politburo Standing Committee who have the greatest involvement in foreign policy are current President and Party Chairman Hu Jintao and Vice President Xi Jinping (who is likely to become president and party chairman in 2012).<sup>104</sup> However, as a Commission-sponsored report

noted, 2012 may herald changes to the foreign policy-making dynamics on the Politburo Standing Committee as new leaders attempt to jockey for power during China's leadership transition.<sup>105</sup>

***Foreign Affairs Leading Small Group of the CCP***

The party's Foreign Affairs Leading Small Group\* is a coordinating body comprised of representatives from party leadership organs, the government, and the military. Although China does not publicize the membership of the Foreign Affairs Leading Small Group, reports suggest that its members include the state councilor (see text box below); the head of the CCP's International Department;† the ministers of foreign affairs, commerce, defense, state security, and public security; leading officials in charge of propaganda, Taiwan policy, and Hong Kong and Macau affairs; and a deputy chief of the PLA's General Staff Department.‡<sup>106</sup> The role of the group is to analyze major foreign policy issues and make recommendations to the Politburo Standing Committee on policy decisions. However, Ms. Lawrence testified that several analysts believe that the Foreign Affairs Leading Small Group has not met as a full body for almost two years. She stated that this suggests that President Hu and Vice President Xi "feel comfortable running foreign policy without regular input from the full membership."<sup>107</sup>

\*Leading small groups in China are ad hoc policy and coordination working groups, the membership of which consists of Chinese political elites. The creation of such groups of high-level officials allows the Chinese government to focus efforts and resources from various ministries and departments on issues or projects that the central government feels are important. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), p. 98.

†The International Department is a body within the CCP that maintains and builds links with foreign political parties, including noncommunist parties such as the Democratic and Republican parties in the United States. It also facilitates contacts with think tanks and non-governmental organizations worldwide. David Shambaugh, "China's 'Quiet Diplomacy': The International Department of the CCP," *China: An International Journal* 5:1 (March 2007): 26–54.

‡The PLA General Staff Department is the military command headquarters for the PLA. Its duties include planning, organizing, and directing military operations; and conducting staff work for the top leadership of the PLA to assist them in decision-making. David Finkelstein, "The General Staff Department of the Chinese People's Liberation Army: Organization, Roles and Missions," in James Mulvenon, *The People's Liberation Army as Organization* (Arlington, VA: RAND Corporation, 2002), pp.122–123. [http://www.rand.org/pubs/conf\\_proceedings/CF182/CF182.ch4.pdf](http://www.rand.org/pubs/conf_proceedings/CF182/CF182.ch4.pdf).

***State Councilor Dai Bingguo***

China's State Councilor Dai Bingguo advises the premier and vice premier of the State Council of the Chinese government (currently Wen Jiabao and Li Keqiang, respectively) and outranks the ministers of foreign affairs and commerce. In addition to his position in the Chinese government, State Councilor Dai also has influence among the CCP leadership as a full member of the CCP Central Committee\* and as the former head of the CCP International Department and the former party secretary of the Ministry of Foreign Affairs.<sup>108</sup> In his role as state councilor, State Councilor Dai is often considered China's top diplomat and serves as U.S. Secretary of State Hillary Rodham Clinton's counterpart in important bilateral meetings, such as the annual U.S.-China Strategic and Economic Dialogue.<sup>109</sup>

Unlike the U.S. State Department, which is instrumental in formulating and implementing foreign policy, China's Ministry of Foreign Affairs primarily implements foreign policies that have been approved by the Politburo Standing Committee and the Foreign Affairs Leading Small Group. For example, Chinese ambassadors, who serve under the Ministry of Foreign Affairs, generally neither approve nor direct policy; they can only make recommendations to higher-ups. In states deemed less vital to China's national interests, the ministry enjoys more leeway in determining policies.<sup>110</sup> In testimony to the Commission, Daniel Kritenbrink, then acting deputy assistant secretary of State in the Bureau of East Asian and Pacific Affairs, explained the challenges of liaising with China's Ministry of Foreign Affairs due to its limited role in foreign policy-making:

*The [Chinese] Ministry of Foreign Affairs, while being the [U.S.] State Department's primary counterpart, [is] one of several voices and institutions involved in the making of Chinese foreign policy. . . . Given the structure of the Communist Party and the Chinese government, the ultimate decisions are made at a much higher level.*"<sup>111</sup>

According to several witnesses who testified to the Commission, the role of the Ministry of Foreign Affairs in foreign policy-making has diminished over the past decade.<sup>112</sup> David Lampton, director of China Studies at The Johns Hopkins School of Advanced International Studies, testified that "no longer do [China's Ministry of] Foreign Affairs offices control the gateways to the outside world as they once did."<sup>113</sup> Some analysts assert that the reasons for the decline in influence include the Ministry of Foreign Affairs' increasing reliance on other agencies for expertise and its competition with a multitude of other actors advancing their interests overseas.<sup>114</sup> For

\*The full CCP Central Committee, elected by the National Congress of the Communist Party of China, is composed of 371 top Chinese leaders from the party, state, and army. The body nominally elects members of the Politburo (25 members), which appoints the Politburo Standing Committee (nine members). However, most analysts agree that the Central Committee as a full body does not have much real power in Beijing and merely serves as a rubber stamp for decisions already made by the Politburo and the Politburo Standing Committee. Nevertheless, departments within the body can be very influential. Kenneth Lieberthal, *Governing China: From Revolution Through Reform* (New York, NY: W.W. Norton & Company, Inc., 1995), pp. 78-79; Xinhua, "New CPC [Communist Party of China] central committee elected," October 21, 2007. [http://news.xinhuanet.com/english/2007-10/21/content\\_6917379.htm](http://news.xinhuanet.com/english/2007-10/21/content_6917379.htm).

example, according to Ms. Lawrence, many of the Chinese players in Africa, including SOEs, banks, and private entrepreneurs, do not necessarily feel compelled to coordinate their activities with the Ministry of Foreign Affairs because they have their own connections and expertise on the ground in African countries.<sup>115</sup> In addition, the Ministry of Foreign Affairs must compete for influence with other organizations, such as the Ministry of Commerce, which holds jurisdiction over foreign trade, and the National Development and Reform Commission (NDRC), which has major influence over China's economic development, specifically in the energy sector.<sup>116</sup>

### ***People's Liberation Army***

The PLA historically was much more involved in China's foreign policy-making process, with prominent military officers holding powerful positions on the Politburo Standing Committee. Today, no uniformed member of the PLA sits on the Politburo Standing Committee, and thus the military officially does not have a direct voice in Chinese foreign policy. However, President Hu and Vice President Xi currently preside over the Central Military Commission, the military's supreme decision-making body, ensuring that the interests of the military are represented on the Politburo Standing Committee, albeit unofficially. In addition, because of the PLA's expertise on defense-related issues, it can influence the policy-making process. In testimony to the Commission, David Helvey, principal director for East Asia for Asia Pacific Security Affairs at the Department of Defense, stated, "[a]s China's interests have expanded, there is a greater intersection between China's defense and foreign policies, giving the PLA a greater role in shaping debates—particularly public debate—on foreign and security policy."<sup>117</sup> Linda Jakobson and Dean Knox explain the PLA's foreign policy role in a study by the Stockholm International Peace Research Institute:

*The PLA shares authority with government and commercial entities on decisions pertaining to arms control and non-proliferation—spheres with direct foreign policy implications over which the PLA formerly exercised nearly unquestioned authority. The PLA still holds sway in these and other defence-related foreign policy issues, particularly with respect to policies related to strategic arms, territorial disputes and national security towards countries such as India, Japan, North Korea, Pakistan, Russia and the USA. In particular, the PLA is a staunch advocate of a hard line towards Taiwan and perceived US interference in cross-Strait relations.*<sup>118</sup>

In recent years, the PLA appears to have grown more assertive in expressing its views. Yu-Wen Julie Chen, visiting scholar at the University of Virginia, testified to the Commission that the PLA has apparently "trespassed on the Foreign Ministry's conventional role as the mouthpiece of foreign affairs" and has been more willing to publicly express opinions that differ from those of the senior civilian leadership.<sup>119</sup> A representative from Singapore's Ministry of Defense told the Commission that this shift began to surface immediately following the global financial crisis as many of the PLA's hard-line leaders grew more confident in China's relatively un-

scathed economy relative to its western counterparts.<sup>120</sup> Some of the means that the PLA has used publicly to assert its views on foreign policy are military publications and op-eds penned by senior military officials in prominent newspapers.<sup>121</sup>

This deviation from official policy has led several observers to assert that the PLA is actually becoming more autonomous. They point to the 2007 Chinese antisatellite test\* and the January 2011 test of the J-20 stealth fighter jet during then U.S. Secretary of Defense Robert Gates' visit to Beijing as evidence that the military is acting without approval from President Hu and the rest of the Politburo Standing Committee.<sup>†</sup><sup>122</sup> However, others argue that these incidents merely display a lack of coordination among Chinese foreign policymakers, particularly between the PLA and the Ministry of Foreign Affairs, and do not represent a fundamental change in who creates China's foreign policy.<sup>123</sup> Others believe that the civilian leadership in China strategically allows the PLA publicly to voice more extreme views and then distances itself from those opinions so as to add a degree of uncertainty to its interactions with other countries.<sup>124</sup> Because of the opacity that surrounds civil-military relations in China, it is unclear which of these theories, or combinations of them, are correct. As Alan Wachman, professor at Tufts University, testified to the Commission, "[e]ven though it is a widespread perception that the PLA is resurgent and the Ministry of Foreign Affairs is in a diminished state of influence, I don't think any of us really is in a position to say that we know that to be the case."<sup>125</sup>

### ***Chinese Provinces***<sup>‡</sup>

Although China's management of foreign affairs is highly centralized, Chinese provinces sometimes act as agents of the central government or as partners with the central government in creating and implementing foreign policies related to trade and security.<sup>126</sup> This is especially the case with China's border provinces, which often act as China's "front line" of engagement with its neighbors.<sup>127</sup> The provincial foreign policy-making bureaucracy both reflects and complements that of the central government: Governors and provincial party secretaries are the top decisionmakers and have the same status as ministers in the central government. These individuals usually lead provincial foreign affairs leading

\*On January 11, 2007, China conducted its first successful antisatellite weapon test, during which it shot down an aging weather satellite with a ballistic missile. However, the Ministry of Foreign Affairs did not release an official statement about the test until 12 days later, leading analysts to question whether President Hu Jintao and other leaders in the Chinese government knew about the PLA's intentions prior to conducting the test. Shirley A. Kan, "China's Anti-Satellite Weapon Test" (Washington, DC: Congressional Research Service, April 23, 2007), p. 4. <http://www.fas.org/sgp/crs/row/RS22652.pdf>.

†During Secretary Gates' January 2011 trip to Beijing, the PLA conducted a test of its J-20 stealth fighter jet. When Secretary Gates asked President Hu about the test, the Chinese leader said he was not aware that it had taken place, leading some western analysts to question whether the military deliberately did not inform President Hu. For more information on the J-20 and its test flight, see chapter 2, section 1, of this Report. Jeremy Page and Julian Barnes, "China Shows its Growing Might: Stealth Jet Upstages Gates, Hu," *Wall Street Journal*, January 12, 2011. <http://online.wsj.com/article/SB10001424052748704428004576075042571461586.html>.

‡For the purposes of this section, the term "provinces" will refer to provincial-level entities in China, including provinces, autonomous regions, municipalities, and special administrative regions.



small groups to coordinate and direct local foreign relations.<sup>‡</sup><sup>128</sup> Many provincial leaders also are powerful actors in the central government, and currently provincial leaders hold two of the nine seats on the Politburo Standing Committee and ten of 25 Politburo seats.<sup>§</sup>

Under the stewardship of central government ministries, Chinese provinces are empowered to be economic liaisons and international dealmakers, fulfilling China's "going out" strategy\* and creating economic growth locally. Provincial leaders are responsible for creating and implementing local foreign trade strategies and managing provincial SOEs.<sup>129</sup> Border provinces such as Jilin and Liaoning (opposite North Korea), and Yunnan (opposite Burma, Laos, and Vietnam) create and implement policies to foster economic engagement across their borders, often with heavy political and financial support from the central government. Jilin is a leading actor in support of China's engagement policy toward North Korea. The province invests in open border cities, economic cooperation zones, joint ventures, and cross-border infrastructure and aims to advance national policies to secure resources, create wealth, and promote economic stability across the border.<sup>†</sup><sup>130</sup> Yunnan Province has similar trade-liberalizing policies along its border with Vietnam and Burma.<sup>131</sup> Reflecting on Yunnan's role as an integral link to China's southern neighbors, President Hu toured Yunnan in 2009 and declared the province a "bridgehead" for China's relations with South and Southeast Asia, a pronouncement that inspired widespread investments in infrastructure and commerce under the banner of a new "bridgehead strategy."<sup>132</sup>

The provinces also are agents of China's foreign policies related to security and defense, pursuing regional security goals, and maintaining internal and external stability along China's borders. This is especially the case in regard to North Korea, which could create a problem for China in the event of a human security disaster (including the possibility of refugees flooding into China). In such a case, provincial and local officials would be responsible for the

<sup>‡</sup> Provincial-level management of foreign relations under governors and provincial party secretaries is conducted by provincial Foreign Affairs Offices and Foreign Trade and Economic Cooperation Commissions, which manage foreign diplomatic relations and foreign trade relations, respectively. Chen Zhimin, "Coastal Provinces and China's Foreign Policy-making," in Yifan Hao and Lin Su, eds., *China's Foreign Policy Making: Societal Force and Chinese American Policy* (Aldershot, UK: Ashgate Publishing Limited, 2005), pp. 11–12. <http://www.cewp.fudan.edu.cn/attachments/article/68/Chen%20Zhimin,%20Coastal%20Provinces%20and%20China%27s%20Foreign%20Policy%20Making.pdf>.

<sup>§</sup> Liaoning and Shanghai are represented in the Politburo Standing Committee; Beijing, Tianjin, Jiangsu, Hubei, Guangdong, Xinjiang, and Chongqing are represented in the Politburo. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 32. <http://books.sipri.org/files/PP/SIPRIPP26.pdf>.

\* China's "going out" strategy was formally enunciated in 2002 by then Chinese President Jiang Zemin as a strategy to help China open up to the world, economically and diplomatically. U.S.–China Economic and Security Review Commission, *2008 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2, 2008), p. 236.

<sup>†</sup> Jilin represents 38 percent of China's accumulated foreign direct investment (FDI) to North Korea since 2000, and North Korea is the province's fourth-largest trading partner. While this heavy investment has contributed to economic growth in Jilin, it also makes Jilin particularly vulnerable to North Korea's unpredictable suspensions of cross-border trade. Bloomberg News, "Dead Border' Is Price of China Support for North Korea Regime," June 14, 2010. <http://www.bloomberg.com/news/2010-06-14/dead-border-thwarts-growth-as-chinese-pay-price-for-backing-north-korea.html>; Carla Freeman and Drew Thompson, *China on the Edge: China's Border Provinces and Chinese Security Policy* (Washington, DC: The Center for the National Interest and The Johns Hopkins School for Advanced International Studies, April 2011), pp. 36–39. [http://www.cftni.org/China\\_on\\_the\\_Edge\\_April\\_2011.pdf](http://www.cftni.org/China_on_the_Edge_April_2011.pdf).

management of border control, fire fighting, internal security, managing displaced persons, and operating refugee camps, *inter alia*.<sup>133</sup> (For more information on China's security polices related to North Korea, see chap. 3, sec. 1, of this Report.) Similarly, in China's westernmost province of Xinjiang, the quasi-military Xinjiang Production and Construction Corps plays a multifaceted role in China's political relationship with its Central Asian neighbors by managing border defense and meeting with foreign leaders.<sup>134</sup> Provincial leaders and law enforcement personnel also are the primary actors dealing with transnational threats like human and drug trafficking, the spread of HIV/AIDS, and political crises in bordering countries.\* Coastal provinces also have provincial maritime law enforcement programs, which add to China's already robust maritime presence.<sup>135</sup> (For more information on China's maritime policies in the South China Sea, see chap. 2, sec. 1, of this Report.)

### **Nontraditional Chinese Foreign Policy Actors**

Aside from the official Chinese actors that are responsible for creating and implementing Chinese foreign policy, a number of nontraditional actors are increasing in importance. SOEs and state-owned banks, Chinese academics and think tanks, and a growing number of Internet users are all beginning to have a voice in foreign affairs and are seeking ways to become more influential in the policy-making process.

#### ***State-owned Enterprises***

As China's SOEs have expanded their global reach, their influence in China's foreign policy-making has grown as well. Large SOEs dominate strategic industries, such as the energy and telecommunications sectors, providing them with many connections to Beijing's political elites. These companies influence foreign policy by virtue of their leaders' access to official policy-making bodies, their expertise in national strategic industries, and their employment of Chinese workers and provision of capital for Beijing.<sup>136</sup> (For more information on China's SOEs, see chap. 1, sec. 2, of this Report.)

Executives of SOEs, especially those in strategic sectors like petroleum, minerals, nuclear, and defense, often have membership in or access to official decision-making bodies in China. Heads of all major SOEs under the central government are appointed by the party's Organization Department and Ministry of Personnel, and some of these individuals hold ministerial or vice-ministerial rank or serve as alternate members of the CCP Central Committee (for example, the general managers of China's three largest state-owned oil companies are vice ministers).<sup>137</sup> While these official positions do not give companies power to make important foreign pol-

\* Yunnan and Guangxi provinces also work to resolve transnational security problems through participation in the Greater Mekong Subregion, a cooperation organization in which these provinces and five Southeast Asian nations work with the Asian Development Bank and other partners to enhance cooperation in nine security, economic, cultural, technological, and environmental sectors. Asian Development Bank, "Greater Mekong Subregion" (Manila, Philippines: July 22, 2011). <http://www.adb.org/gms/>; Carla Freeman and Drew Thompson, *China on the Edge: China's Border Provinces and Chinese Security Policy* (Washington, DC: The Center for the National Interest and The Johns Hopkins School for Advanced International Studies, April 2011), pp. 71–73. [http://www.cftni.org/China\\_on\\_the\\_Edge\\_April\\_2011.pdf](http://www.cftni.org/China_on_the_Edge_April_2011.pdf).

icy decisions directly, they enable state-owned company executives to take part in implementing and debating policies that come from higher up.<sup>138</sup> Business executives also maintain close ties to high-ranking officials. According to a Stockholm International Peace Research Institute report, Fu Chengyu, chief executive officer of China National Offshore Oil Corporation, is said to have access to Foreign Minister Yang Jiechi “any time he wants.”<sup>139</sup>

Moreover, there is a “revolving door” of political and industrial appointments through which highly ranked personnel in government bodies and state-owned companies are promoted from one sector to the other, enabling business executives and government officials to take their expertise and professional networks from the government to the business sector, or vice versa. For example, former heads of large companies have become members of the Politburo Standing Committee or the CCP Central Committee or have become governors or provincial party secretaries.<sup>140</sup> This revolving door particularly applies to China’s oil industry, which is known to undergo occasional personnel “shake-ups” during which oil executives are moved from company to company or from a company to a powerful government position.<sup>141</sup> This system facilitates tied interests between the energy sector and the government and ensures that the governing elites always have a hand in this strategic industry.<sup>142</sup> For example, Zhou Yongkang, a current member of the Politburo Standing Committee, is the former head of China National Petroleum Corporation, one of China’s largest state-owned oil companies. Erica Downs, fellow at The Brookings Institution, testified to the Commission that some analysts assert that Mr. Zhou has used his position on the Politburo Standing Committee to liaise with and promote the interests of the national oil companies.<sup>143</sup>

SOEs also provide valuable expertise to policymakers. Dr. Chen testified to the Commission that SOEs are able “to provide ... detailed and expert knowledge on certain vital issues [which] increases their value for decision-makers.” Because these companies have extensive, on-the-ground experience in numerous countries, their managers often are experts on the foreign countries’ government structures and market conditions. Chinese leaders often rely on this knowledge to inform their foreign policy-making decisions.<sup>144</sup>

SOEs operating overseas are important contributors to China’s economic growth and its ability to employ its burgeoning work force. National SOEs provide the government with massive revenues and employ 6.8 million Chinese workers, most of whom work overseas.<sup>145</sup> As more workers go abroad to work for these SOEs, the Chinese government must find ways to protect them if the country in which they are working becomes destabilized or is victim to a terrorist attack or natural disaster. For example, after the turmoil began in Libya this past year, the PLA and the Ministry of Foreign Affairs worked to evacuate almost 36,000 Chinese citizens from the country, making it one of the largest and most complicated overseas evacuations of Chinese citizens in the history of the People’s Republic of China (PRC).<sup>146</sup> (For more information about the Libya evacuation, see chap. 2, sec. 1, of this Report.) Because the decisions taken by these companies can directly affect

China's economic growth and the livelihood of Chinese workers, leaders are apt to incorporate the companies into the policy-making process, whether it be foreign policy or otherwise.<sup>147</sup>

SOEs often advance China's national "going out" policy to secure resources to fuel China's economic growth and broaden China's global footprint. Their myriad global economic interests sometimes can be at odds with China's wider foreign policy goals.<sup>148</sup> For instance, state-owned oil companies operating in unstable or "rogue" countries like Sudan and Iran have attracted the ire of the international community.\*<sup>149</sup> In the case of Sudan, the NDRC removed the country from a list of preferred destinations for Chinese oil investments in 2007, but two state-owned oil companies ignored the NDRC's guidance and continued to purchase Sudanese oil assets.<sup>150</sup> Dr. Downs testified that the state-owned oil companies rarely coordinate their overseas activities with government ministries and that some Chinese scholars think that the national oil companies are "hijacking the foreign policy process" in Sudan and Iran.<sup>151</sup>

#### ***State-owned Banks***

Two of China's state-owned banks are responsible for supporting government policy objectives abroad: China Development Bank and the Export-Import Bank of China. Both banks operate under the State Council, and China Development Bank has full ministerial rank.<sup>152</sup> China Development Bank and the Export-Import Bank of China play a key role in the financing of China's foreign economic activities. China Development Bank has facilitated several billion dollars' worth of Chinese companies' investments abroad, making it a key player in China's "going out" strategy, especially when it comes to acquiring energy resources. The Export-Import Bank of China is responsible for facilitating foreign trade and allocating China's foreign aid.<sup>153</sup>

Many of China Development Bank's loans require a high degree of cooperation between the central government and business, with the bank acting as the main coordinating body between the two.<sup>154</sup> Government entities often are at the forefront of China's high-profile strategic energy deals overseas; however, China Development Bank sometimes plays the leading role in identifying investment opportunities and coordinating deals.<sup>155</sup> Such was the case for a \$10 billion oil-backed loan to Brazil's national oil company, Petrobras, in 2009. China Development Bank, which had been conducting market research in Brazil since 2000, proposed the loan, which Beijing later supported as a diplomatic deliverable for upcoming state visits with Brazil. Dr. Downs writes of the deal in "Inside China Inc.: China Development Bank's Cross-Border Energy Deals":

*The coincidence of the negotiations between [China Development Bank] and Petrobras with the preparation for the two sets of meetings between Chinese and Brazilian leaders prompted the Chinese government to embrace the deal as a*

\*Sudan and Iran constituted the fourth- and fifth-largest sources of China's crude oil imports for January 2011. ChinaOilWeb.com, "China's Crude Oil Imports Data for January 2011." <http://www.chinaoilweb.com/UploadFile/docs/Attachment/2010-3-169132990.pdf>.

*symbol of the growing economic ties between China and Brazil. According to Chen Yuan [governor of China Development Bank], 'once the Ministry of Foreign Affairs, Ministry of Commerce, the National Development and Reform Commission and the State Council realized this coincidence, they provided their active support. As a result, this project became a national project.'*<sup>156</sup>

**Academics and Think Tanks**

As China's foreign policy becomes more complex, its leaders increasingly are turning to academics and think tanks to inform their debates about policies related to international affairs. Think tanks and universities operate under varying degrees of official administration, with many think tanks funded entirely by the government and major universities overseen by party officials. For this reason, some doubt the independence and the reliability of the information these institutions are providing to policymakers. A study by the Brussels Institute of Contemporary China Studies characterizes Chinese think tanks as:

*[P]ermanent, policy oriented structures with their own research staff who regularly publish and communicate the results of their studies to officials and to the public, albeit to a lesser extent than their Western counterparts. They all strive to achieve greater freedom of research and to contribute to the public good, although these orientations are of course bound by the red lines set by the government and by the need to respect the primacy of the CCP in their policy solutions.*<sup>157</sup>

Chinese scholars influence foreign policymakers through formal channels and informal connections to top leaders.<sup>158</sup> For example, think tanks often submit reports to their affiliated government organizations, and academics are sought out by government officials to participate in meetings or conferences on foreign policy issues.<sup>159</sup> Their opinions often differ, and at times debates between scholars are made public in the media. An example of this type of debate took place in December 2009 when the Chinese newspaper *Global Times* published a debate between two scholars about whether China should intervene militarily in Afghanistan.<sup>160</sup> However, on particularly sensitive core issues for the CCP, such as Taiwan and Tibet, leaders allow little leeway for scholarly debate in public fora.<sup>161</sup>

Major Chinese foreign policy research institutions and their affiliations <sup>162</sup>	
Institution	Administering organization
Communist Party International Strategy Research Institute	Central Party School
People's Liberation Army Academy of Military Sciences National Defence University	Central Military Commission Central Military Commission
China Institute for International Strategic Studies	PLA General Staff Department
China Foundation for International Strategic Studies	PLA General Staff Department



**Major Chinese foreign policy research institutions and their affiliations—*Continued***

*Government*

Development Research Centre	State Council
Chinese Academy of Social Sciences	State Council
China Institute of International Studies	Ministry of Foreign Affairs
China Institutes of Contemporary International Relations	Ministry of State Security
China Center for International Economic Exchanges	National Development and Reform Commission

*Local Government*

Shanghai Institutes for International Studies	Shanghai City Government
---	--------------------------

*Academic\**

Institute of International Relations	China Foreign Affairs University
Strategy and Conflict Research Center	China Foreign Affairs University
Institute of International Studies	Fudan University
School of International Studies	Peking University
School of International Studies	Renmin University
Institute of International Studies	Tsinghua University
Institute of International Strategy and Development	Tsinghua University

Chinese leaders often use think tanks and academia not only as a resource but also as a platform for testing potentially controversial foreign policies and gauging the response. Ms. Lawrence testified to the Commission that Beijing uses “semi-official actors” from scholarly institutions to float ideas, and that:

*[There is an] interesting relationship between scholars and the government. On the one hand, they sometimes will present themselves as being independent analysts of the situation, and yet there are classes of scholars who are cleared by the government to essentially speak for it and also to run with certain kinds of ideas and see what kind of response they get from them.<sup>163</sup>*

***Public Opinion and Internet Users***

While not nearly as influential as some of the above-listed groups, public opinion and Internet users are growing increasingly influential in foreign policy-making as Internet use becomes more prevalent in China. There are over 500 million Internet users in China, 195 million of which are active bloggers, many of whom utilize the Internet as a forum for the discussion of politics, governance, and foreign affairs, among other things.<sup>164</sup> The Commission’s 2010 *Annual Report to Congress* notes:

*China’s leadership, at all levels of the government, increasingly uses the Internet to interact with the Chinese people. This practice, interwoven with strict censorship controls, affords the government the ability to allow a controlled online debate about certain issues ... The government then*

\*Most Chinese university-affiliated research institutes are administered by the Ministry of Education and lack substantial links to foreign policymakers in China. However, some experts from these institutions are well known and have influence on foreign policy-making. Thomas J. Bickford and Kristen Gunness, *China’s International Relations Think Tanks: Structure, Roles, and Change* (Alexandria, VA: The CNA Corporation, September 2007), p. 5.



*leverages what it learns from following this debate to construct policies that aim to undercut the most serious irritants to domestic stability.*<sup>165</sup>

In addition to monitoring the debate on domestic issues, the Chinese government uses the Internet and public opinion to gauge the opinions of Internet users on China's foreign policy decisions. While the government largely censors the Internet in China, it also is sensitive to the reactions of the Chinese people. David Shambaugh, professor at The George Washington University, notes:

*The Chinese government is quite sensitive to this body of public opinion, as much of it is hyper-nationalistic and critical of the government for being 'weak' or 'soft' in the face of foreign pressures and indignities. Foreign Ministry officials are quick to point out that this is a constituency they must constantly consider, react to, and attempt to control.*<sup>166</sup>

The ability of Internet users to mobilize en masse around a foreign policy issue was evident in 2005 when 40 million Chinese signed an Internet petition opposing Japanese attempts to become a permanent member of the United Nations (UN) Security Council.<sup>167</sup> In a more current example of Chinese Internet users' influence over the way China relays its foreign policy, Dr. Downs testified about the prominent news and Internet coverage of the recent Chinese evacuation of its citizens from Libya. The Chinese response to the crisis in Libya contrasted greatly with China's response to the kidnapping and murder of Chinese citizens in Ethiopia in 2007, which elicited sharp criticism of the government from Chinese Internet users for not coming to the aid of Chinese citizens. Dr. Downs asserted that the reason for the enhanced coverage of the Libya evacuation was to prevent the same type of backlash from Chinese Internet users that arose in 2007.<sup>168</sup>

Nevertheless, these voices are severely limited by China's propaganda apparatus, which aggressively censors online material that is deemed inappropriate. As a result, often the only voices that are left on the Internet are those that already coincide with the opinions of Beijing's elite. Dr. Chen testified:

*It is hard to establish a link between online pressure and the government's foreign policy. It is more appropriate to say that policymaking elites can entertain online expression of interests, picking and choosing the ones they see as being most beneficial for the execution or conduct of foreign affairs.*<sup>169</sup>

### **Coordination of Foreign Policy Actors under the CCP**

The proliferation of voices in Chinese foreign policy has made coordination among actors difficult in recent years. Often, in any given country, Beijing must manage the activities of the ministries of Foreign Affairs, Commerce, Finance, Agriculture, Health, and the Export Import Bank of China and China Development Bank. On top of that, companies, provincial governments, and research institutions are launching their own relationships with specific nations. Ms. Lawrence noted, "[m]any of the Chinese players ... now

do not answer to the Foreign Ministry, and do not necessarily feel compelled to coordinate their activities with it.”<sup>170</sup> Difficulties can arise when two ministries conflict with one another in carrying out China’s foreign policy, because they are both seated at the same bureaucratic level.<sup>171</sup>

In some cases, a lack of coordination among China’s various foreign policy actors threatens to upset Beijing’s foreign policy goals. For example, in the South and East China Seas, there are at least six distinct official actors operating, including China’s five civilian maritime administration and security agencies and the PLA Navy. In testimony to the Commission, Stacy A. Pedrozo, a U.S. Navy captain and military fellow at the Council on Foreign Relations, noted that China’s various maritime actors are insufficiently coordinated, posing a threat to the peaceful resolution of disputes in the region.<sup>172</sup> Chinese officials acknowledge this problem as well and have announced plans to enhance central coordination of actors in the South China Sea in the future.<sup>173</sup> A lack of coordination between Chinese government ministries and state-owned weapons manufacturers may also have led to a strain in Sino-Libyan relations in 2011. A Canadian newspaper discovered evidence that three Chinese state-owned companies offered to sell \$200 million in weapons to pro-Qaddafi forces in June in violation of a UN embargo on arms sales to Libya. Chinese Ministry of Foreign Affairs officials denied prior knowledge of the negotiations, and some analysts suggested that the state-owned weapons manufacturers may have bypassed the Ministry of Foreign Affairs and instead dealt directly with the Qaddafi government.<sup>174</sup>

Despite problems of coordination, there is little dispute that the CCP still holds firm control over China’s foreign policy. Although many of the groups involved have access to the political elite in the Communist Party, Dr. Chen testified that “[i]n the end, it is [CCP] decision-making elites who can define and determine which groups can exist and enter the foreign policy-making process.” Ultimately, the top leadership, namely President Hu and the Politburo Standing Committee, are the definitive architects of Chinese foreign policy.<sup>175</sup>

### **Implications for the United States**

The increasing number of voices in Chinese foreign policy-making requires U.S. diplomats and leaders to be adept in identifying which individuals and organizations are influential and where they fall in the Chinese foreign policy-making apparatus while ensuring that they are mindful of the opinions of nontraditional actors as well. As China’s foreign policy actors grow in number and diversity, the direction and intention of China’s foreign policies may become more difficult for U.S. policymakers to calculate. Dr. Shambaugh notes, “[t]he fact that China has such a diverse discourse suggests that it possesses multiple international identities and a schizophrenic personality.”<sup>176</sup> This can complicate how the United States formulates its policies vis-à-vis China and can lead to misperceptions of what each country’s true intentions are. For example, if U.S. leaders exclusively paid attention to the hard-line voices coming out of the PLA, they might be inclined to react to what they perceive is a more aggressive China. During the Com-

mission's December 2010 trip to Singapore, Commissioners heard from the Singaporean Ministry of Foreign Affairs about its frustration with the number of different voices coming out of Beijing, making it difficult to know whether specific Chinese officials' opinions are authoritative.

Although the increasing number of players involved in China's foreign policy-making process may make U.S. policy responses more difficult to coordinate, it could provide U.S. diplomats with multiple channels to engage China's policymakers on important issues. While the Ministry of Foreign Affairs remains the primary point of contact for U.S. officials, the proliferation of other foreign policy players in China could expand opportunities for the United States to pursue a more sophisticated understanding of China's foreign policy process.

### **Conclusions**

- As China expands and diversifies its overseas activities, it encounters an increasingly complex environment requiring the input and advice from knowledgeable subject matter experts. As a result, China's foreign policy-making process is changing to accommodate input from actors who previously had little or no say.
- Actors with increasing influence on China's foreign policies include the PLA, large state-owned enterprises, and academics and think tanks. In addition, while still minor compared to other actors, public opinion, expressed primarily online, appears to have a modicum of influence on some Chinese foreign policies.
- The CCP remains firmly in control of China's foreign policies, especially for issues deemed critical, such as China's policies toward the United States, North Korea, and Taiwan. This is despite the increased difficulty Beijing may have in coordinating a coherent policy among a growing number of actors.
- The growing complexity of China's foreign policy-making process has mixed implications for the United States. On the one hand, Washington may find it more difficult to interact with priority counterparts in Beijing as the number of actors in the policy process expands. On the other hand, the plethora of Chinese actors may provide U.S. foreign policymakers with opportunities to understand or influence Beijing.

## SECTION 3: TAIWAN

### Introduction

Continuing to monitor the situation between Taiwan and China in 2011, the Commission notes that overall the relationship across the Taiwan Strait continues to improve, but at a pace slower than in the previous two years. A key reason for the slower pace of improvements across the Taiwan Strait is the upcoming Taiwan presidential and legislative elections on January 14, 2011, as neither China nor the incumbent Taiwan administration desires to have the cross-Strait rapprochement used as a negative issue prior to the elections. In addition, many of the easier negotiations, such as on economic and trade issues, have been discussed, leaving increasingly difficult political discussions remaining. As a result, this year the two sides have focused on implementing already signed agreements. Despite the slowed, but continued, improvement in economic and diplomatic relations between Taipei and Beijing, the cross-Strait military balance continues to tilt in favor of the mainland due to China's growing military capabilities.

This section of the Commission's Report discusses the current situation across the Taiwan Strait and describes any notable changes in the diplomatic, economic, and military aspects of the cross-Strait relationship over the past year.

### Developments in Cross-Strait Diplomatic Relations

Since the Commission's *2010 Annual Report to Congress*, relations between Taiwan and China have continued to improve, although there has been less cross-Strait diplomatic activity in 2011 than in the previous two years. Since November 2010, Taiwan and China have signed only one agreement, as opposed to the 14 previously signed agreements since Taiwan President Ma Ying-jeou's 2008 inauguration. The December 2010 semiannual talks between the Straits Exchange Foundation and the Association for Relations Across the Taiwan Straits\* produced the Cross-Strait Agreement on Medical and Health Cooperation, which will facilitate cooperation on the exchange of information about epidemics, development of vaccines, and clinical drug trials.<sup>177</sup> During the meeting, the two sides also agreed regularly to review the implementation of previous agreements.<sup>178</sup> The only new agreement introduced and being discussed this year has been on nuclear safety in response to Japan's nuclear crisis, which was proposed by Taiwan in March

\*Taipei and Beijing do not have an official bilateral relationship. Instead, cross-Strait negotiations are held under the auspices of two quasi-official organizations. Representing Taiwan is the Straits Exchange Foundation, "a private intermediary body" entrusted to act on behalf of the Taiwan government in cross-Strait matters. The corresponding body in China is the Association for Relations Across the Taiwan Straits. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), p 143.

2011.<sup>179</sup> In July 2011, Taiwan's Mainland Affairs Council Minister Lai Shin-yuan stated that the nuclear agreement would be addressed at the next meeting between the Straits Exchange Foundation and the Association for Relations Across the Taiwan Straits, which was tentatively scheduled for August 2011 but was postponed until late October.<sup>180</sup>

In 2011, Taiwan and China also implemented several unilateral policies that expanded cross-strait relations in the areas of travel and education. In June 2011, China and Taiwan agreed to begin allowing individual Chinese citizens to travel to Taiwan rather than only in preapproved groups. The lifting of the ban, however, applies only to the residents from three mainland cities: Beijing, Shanghai, and Xiamen, and the length of stay is limited to 15 days only.<sup>181</sup> Taiwan expanded upon its direct flight agreement with China by announcing in June 2011 that the number of cross-strait direct flights would increase from 370 to 558.\*<sup>182</sup> As a result, tourism between the two sides has grown significantly. In his meeting with Commissioners in July 2011, President Ma noted that more than 3,000 mainlanders visit Taiwan every day.<sup>183</sup> According to Taiwan's Tourism Bureau, 2.4 million Taiwan residents visited the mainland in 2010, a 37 percent increase over 2009. In 2010, 1.6 million mainlanders visited the island, a 41 percent increase over 2009.<sup>184</sup>

Taiwan and the mainland have also made their educational systems more accessible to one another. Taiwan's Ministry of Education announced in January 2011 that it would recognize Chinese degrees. In April 2011, Taipei announced that it would allow 2,000 Chinese students to study at Taiwan's universities. However, students from the mainland are subject to stipulations that prohibit them from receiving Taiwan government scholarships, applying for jobs in Taiwan, or studying topics sensitive to Taiwan's national security, such as military technology and aeronautics.<sup>185</sup> In a meeting with members of Taiwan's National Security Council, Commissioners were told that these restrictions were important because of the continuing threat the mainland poses to Taiwan.<sup>186</sup>

Over the course of the past year, the two sides failed to conclude several anticipated agreements. These agreements included:

- *Cross-Strait investment protection agreement*: The two sides originally intended to sign in December 2010 an agreement to protect Taiwan investments on the mainland.<sup>187</sup> During a meeting with the Taipei Economic and Cultural Representative Office,<sup>†</sup> the Commission heard that the two sides were in dispute over whether the agreement would be treated as a domestic or inter-

\*The direct flight agreement referred to is the Cross-Strait Air Transport Agreement, which was signed in November 2008 and established direct flights between Taiwan and the mainland. Prior to the implementation of this agreement, direct flights between the island and the mainland first had to transit through a third-party airport. Mainland Affairs Council, "Explanation concerning the Cross-Strait Air Transport Agreement," November 4, 2008. <http://www.mac.gov.tw/public/Data/3962917501071.pdf>.

†The Taipei Economic and Cultural Representative Office is Taiwan's principal representative office in the United States. Because the United States and Taiwan do not engage in official diplomatic relations, the office serves as Taiwan's de facto embassy. For more information, see "Taipei Economic and Cultural Representative Office in the United States, TECRO Profile and Mission" (Washington, DC: November 3, 2010). <http://www.taiwanembassy.org/US/ct.asp?xItem=166566&CtNode=2294&mp=12&xp1>.

national agreement.<sup>188</sup> According to the media, Taiwan is wary of China's legal system and insists on using the International Chamber of Commerce for arbitration. However, China refuses to treat any cross-Strait issue as international.<sup>189</sup> It is unclear when further discussions on this issue will be held.

- *Double taxation agreement:* In June 2011, Taiwan's Finance Minister, Lee Sush-der, stated that the two sides have "largely" reached an agreement on a double-taxation avoidance pact originally expected in 2009. The pact had been set aside due to difficulties in agreeing on the tax rates and categories to be included, and Minister Lee provided no details on the provisions that the agreement would contain or when it would be signed.<sup>190</sup>
- *Currency clearance agreement:* During an April 2011 meeting, Taiwan's and China's financial regulation commissions failed to reach a widely anticipated currency clearance agreement that would allow Taiwan banks operating on the mainland to make loans and accept deposits in China's currency, the renminbi (RMB). An official from the People's Bank of China had originally stated in December 2009 that preparation for the agreement was "80 to 90 percent" complete and that it would be signed within the coming months.<sup>191</sup> After the agreement was stalled for more than a year, reports anticipated that the April 2011 meeting between the banking regulators would result in its successful completion. However, the two sides only agreed upon procedural measures, including the establishment of a mechanism for holding regular meetings.<sup>192</sup>
- *Cultural agreement:* Taiwan and China have also continued to disagree over the possibility of a cultural agreement, which Beijing has persisted in suggesting to an unresponsive Taipei. Proposed by China's Minister of Culture, Cai Wu, the agreement would institutionalize cultural exchanges between the two sides and "bring together both sides' resources, funding and creativity."<sup>193</sup> According to one expert, the Ma Administration is reluctant to sign a cultural agreement for fear that the Democratic Progressive Party would attempt to portray the agreement as showing favor to China's culture.<sup>194</sup>

A key complicating factor in further cross-Strait negotiations is Taiwan's upcoming presidential and legislative elections in January 2012, for which the cross-Strait situation is expected to remain a major issue.\* In July 2011, President Ma announced that he planned to scale back visits from high-level mainland officials to Taiwan "during a certain period of time," which other officials in

\*Currently there are three announced candidates for Taiwan's presidential elections. President Ma Ying-jeou is seeking reelection as the Kuomintang Party candidate. His primary opponent is Chairwoman Tsai Ing-wen of the Democratic Progressive Party. In late September 2011, James Soong, formerly of the Kuomintang Party, announced he was running for president as a candidate of the People's First Party. The addition of Mr. Soong's third-party candidacy will likely make an already close election even more difficult to predict.



Taiwan interpreted as an election strategy motivated by aversion to appearing too conciliatory toward China.<sup>195</sup> According to one expert, President Ma has been under pressure from members of his party to prevent the Kuomintang from gaining a reputation as excessively “pro-China.”<sup>196</sup> Taiwan has also banned the travel of senior-level mainland officials to the island, allegedly in an attempt to prevent the visits from being used against his administration in the presidential campaign.<sup>197</sup>

Beijing may also be a factor in the slower pace of developments in the cross-strait relationship. China has taken a strong interest in the outcome of Taiwan’s election, showing preference for a Kuomintang victory. According to Richard C. Bush, director of the Center for Northeast Asian Policy Studies at The Brookings Institution, Beijing has avoided controversial cross-strait issues and “is not pushing the agenda” before the election because it “understands that it has an interest in keeping President Ma and the KMT [Kuomintang] in power.”<sup>198</sup> China may even become lenient on issues such as participation in international organizations in order to demonstrate the effectiveness of President Ma’s cross-strait policies.<sup>199</sup> However, according to one Washington D.C.-based expert on cross-strait issues, it is possible that if President Ma wins reelection, Beijing could take a harder line with Taipei in order to “secure [China’s President] Hu Jintao’s legacy” before President Hu steps down in the fall of 2012.<sup>200</sup>

### ***Developments in Taiwan’s International Space***

Taiwan has continued to pursue efforts to gain international space through participation in international organizations and negotiating with other countries on visa waiver exemption, extradition, and free trade agreements. Since the publication of the Commission’s *2010 Annual Report to Congress*, Taiwan has experienced both progress and setbacks in its participation in international organizations. In 2011, Taiwan joined one new international organization, the Civil Air Navigation and Services Organization, which is an official observer of the United Nations’ International Civil Aviation Organization.\* It experienced a setback in May 2011, when the World Health Organization used the label, “Taiwan, Province of China,” sparking Taiwan officials formally to assert that it be referred to as “Chinese Taipei.”<sup>201</sup> A similar controversy occurred in July 2011, when Taiwan’s Ministry of Foreign Affairs publicly urged Brazil to make the same change after discovering that the Brazilian government’s website designated Taiwan as a province of China.<sup>202</sup> A report prepared for the Commission by The Economic Strategy Institute discussed similar People’s Republic of China (PRC) indignation expressed when “Taiwan” is used, stating:

\* Rather than joining the organization under a regional name such as the commonly used name “Chinese Taipei,” Taiwan is listed solely as “Air Navigation and Weather Services, Civil Aeronautics Administration,” with no mention of Taiwan. Full membership is open to any organization providing air navigation services, as opposed to the International Civil Aviation Organization, which only admits states. Taiwan is not a member of this latter organization. Shelly Shan, “Taiwan joins CANSO [Civil Air Navigation Services Organization] aviation organization,” *Taipei Times*, January 15, 2011. <http://www.taipetimes.com/News/taiwan/archives/2011/01/15/2003493568>; and Civil Air Navigation Services Organization, “Joining CANSO.” <http://www.canso.org/cms/showpage.aspx?id=329>.

*Any person who has participated in the deliberations of international organizations with China can undoubtedly describe the palpable tension which is created when one delegate makes the mistake of referring to 'Taiwan' rather than by the officially approved nomenclature within that organization. First of all, the room will be quiet enough to hear a pin drop. Then there will be a strong and immediate request by the Chinese representative for a 'correction' to the record. Anyone who makes such a mistake once is unlikely to make it twice. In fact, at Board meetings within the Asian Development Bank, if a delegate does make an erroneous reference to 'Taiwan,' the meeting must be formally stopped, and an official statement clarifying the exact political status of 'Taiwan' is read out. Only when this formal clarification and correction is complete can the Board meeting recommence.*<sup>203</sup>

In another sign of Taiwan's success in expanding its international space, it has made substantial gains in joining visa waiver programs. It currently belongs to 124 visa waiver programs around the world, surpassing its original goal of joining 100 programs by 2011.<sup>204</sup> Taiwan has yet to join the U.S. program, although President Ma noted to Commissioners in August 2011 that this is an important goal of his administration.<sup>205</sup> Taiwan's prospects for joining improved this year due to its declining visa refusal rate, a key obstacle to joining the program.\*<sup>206</sup> Taiwan and the United States have also made progress on an extradition agreement,<sup>207</sup> although a representative from the Taipei Economic and Cultural Representative Office noted to the Commission that obstacles still remain to the agreement's successful conclusion.<sup>208</sup>

Taipei continues to pursue free trade agreements with other nations. According to some Taiwan experts, "The Ma administration hopes that the ECFA [Economic Cooperation Framework Agreement] would serve as a model framework for Taiwan's trade negotiation with the rest of the world so that other FTA [free trade agreement]-like agreements could be reached without Beijing's obstruction."<sup>209</sup> During a meeting with Taiwan's Ministry of Economic Affairs, Commissioners heard how Taiwan is currently negotiating a trade agreement with Singapore.<sup>210</sup> In addition, Taiwan is conducting feasibility studies for possible free trade agreements with India and the Philippines.<sup>211</sup> Several experts have stated that Taiwan's ability to sign free trade agreements with other nations is contingent upon Beijing's approval, but Taipei disagrees with this assertion.<sup>212</sup> Commenting on negotiations with Singapore, Minister Lai stated that "China has no say" over whether Taiwan and Singapore come to an agreement, and in the case of India and

---

\*According to section 217 of the Immigration and Naturalization Act, in order to be eligible for participation in the U.S. visa waiver program, countries must have a tourist visa refusal rate for the most recent fiscal year of less than 2.5 percent and an average visa refusal rate for the past two fiscal years of less than 2 percent, or a visa refusal rate of less than 3 percent for just the previous full fiscal year. According to the U.S. State Department, Taiwan's visa refusal rate for fiscal years 2010 and 2009 were 2.2 percent and 4.4 percent. "Immigration and Nationality Act," Title 8, *U.S. Code 1187*, Sec. 217, 2010 edition; U.S. Department of State, "Adjusted Refusal Rate—B-Visas Only by Nationality, Fiscal Year 2009." <http://www.travel.state.gov/pdf/FY09.pdf>; and U.S. Department of State, "Adjusted Refusal Rate—B-Visas Only by Nationality, Fiscal Year 2010." <http://www.travel.state.gov/PDF/FY10.pdf>

the Philippines, “we have made it clear to the other side that this is our right.”<sup>213</sup>

Although the United States remains Taiwan’s third-largest trading partner after China and Japan, negotiations on a U.S.-Taiwan trade agreement, officially titled the U.S.-Taiwan Trade and Investment Framework Agreement,\* have been on hold since 2007. The current obstacle to resumption of the talks is a disagreement about Taiwan’s partial ban on U.S. beef imports.<sup>214</sup> Despite a November 2009 bilateral agreement between Taipei and Washington to allow the import of U.S. beef products into Taiwan, in January 2010 the Taiwan legislature amended a Taiwan food safety law to impose a partial ban on U.S. beef products.<sup>215</sup> In response to the ban, the Office of the U.S. Trade Representative and the U.S. Department of Agriculture issued a joint statement, noting that:

*The decision by Taiwan authorities to place domestic politics over science raises serious concerns. This action will also undermine Taiwan’s credibility as a responsible trading partner and will make it more challenging for us to conclude future agreements to expand and strengthen bilateral trade and economic ties.*<sup>216</sup>

Since the passage of this law, no further official negotiations have been held on the Trade and Investment Framework Agreement with Taiwan.<sup>217</sup>

### **Developments in Cross-Strait Economic Relations**

Despite the absence of a large number of new agreements, cross-strait economic relations in 2011 have been characterized by strong growth in bilateral trade and steady progress in implementing the agreements already signed. The most prominent accord is the 2010 Economic Cooperation Framework Agreement, which included the establishment of the Cross-Strait Economic Cooperation Committee and tariff cuts on more than 800 items on the agreement’s “early harvest” list.<sup>218</sup>

The Cross-Strait Economic Cooperation Committee is a platform for implementing the provisions of the Economic Cooperation Framework Agreement. The committee is responsible for negotiating agreements on trade in commodities and services, investment protection, and conducting dispute resolution between the two sides. It met for the first time in February 2011, and, according to one expert, is “the most senior forum for direct contact between officials from the two sides and represents a significant step forward in cross-strait cooperation.”<sup>219</sup> At the meeting, the committee established six working groups on merchandise trade, services trade, investment, dispute settlement, industry cooperation, and customs. In addition, the members agreed to launch in mid-April 2011 three agreement-authorized negotiations on merchandise trade, services

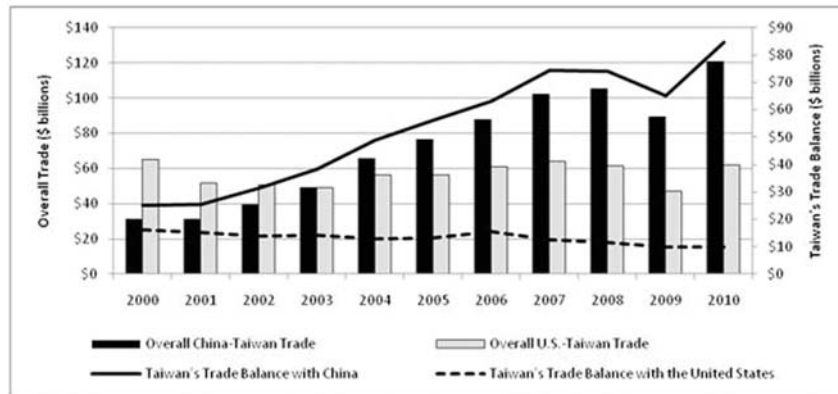
\* According to the Office of the U.S. Trade Representative, “Trade and Investment Framework Agreements (TIFAs) provide strategic frameworks and principles for dialogue on trade and investment issues between the United States and the other parties to the TIFA. . . . [T]hese agreements all serve as a forum for the United States and other governments to meet and discuss issues of mutual interest with the objective of improving cooperation and enhancing opportunities for trade and investment.” Office of the U.S. Trade Representative, “Trade & Investment Framework Agreements” (Washington, DC). <http://www.ustr.gov/trade-agreements/trade-investment-framework-agreements>.

trade, and dispute settlement.<sup>220</sup> Working group talks on merchandise and services trade were held in the beginning of August.<sup>221</sup>

Although Taiwan and China signed no new bilateral economic agreements in 2011, they both continued to pursue individual policies that will improve cross-Strait economic exchange. Taipei has continued to ease restrictions on Chinese investments in Taiwan, although restrictions still remain. According to Taiwan's Ministry of Economic Affairs, investment from the mainland must first undergo a review process to ensure that it does not harm Taiwan's national security or Taiwan industries.<sup>222</sup> As of February 2011, Chinese total investment in Taiwan since mainland investment on the island was first allowed equaled \$139 million.<sup>223</sup> This amount is substantially lower than Taiwan's direct investment in China, which equaled \$14.62 billion in 2010 alone. According to Taiwan's Mainland Affairs Council, Taiwan's direct investment in China has increased from 70 percent of Taiwan's total direct foreign investment in 2009 to 84 percent in 2010.<sup>224</sup> China's comparatively low amount of direct investment in Taiwan is attributed to Taiwan's restrictions, which gradually have been easing.<sup>225</sup> In March 2011, Taiwan's Ministry of Economic Affairs announced it would open 42 additional sectors to Chinese investors, including the strategically important flat panel and computer chip industries.<sup>226</sup> China also is considering reducing tariffs on rare-earth minerals to Taiwan.<sup>227</sup>

Partially as a result of the Economic Cooperation Framework Agreement, cross-Strait trade has continued to expand rapidly. Taiwan's share of China's imports increased in 2011 as a result of the agreement, changing a trend in which its share had been decreasing.<sup>228</sup> According to Taiwan's Mainland Affairs Council, in 2010, total cross-Strait trade increased by 40 percent over the 2009 level, to \$120.8 billion.<sup>229</sup> The import-export balance continues to favor Taiwan, which in the first quarter of 2011 exported to China \$30.1 billion in goods, a 13 percent increase from the same period in the previous year. In contrast, Taiwan imported from China \$14.2 billion in the first half of 2011, a 40 percent increase from the same period last year.<sup>230</sup> By way of comparison, in the first quarter of 2011, U.S. total trade with Taiwan was \$22.1 billion, a 17 percent increase from the same period in 2010. Overall, the United States suffers a trade deficit with Taiwan. In the first half of 2011, the United States imported 35 percent more (\$24.3 billion) from Taiwan than it exported (\$15.7 billion).<sup>231</sup> Figure 1, below, provides a comparison of Taiwan's trade with the United States and China between 2000 and 2010.

**Figure 1: Comparison of Taiwan's Overall Trade Balance with China and the United States (2000-2010)**



Source: Mainland Affairs Council, *Cross-Strait Economic Statistics Monthly* No. 221 (Taipei, Taiwan: August 29, 2011), p. 23. <http://www.mac.gov.tw/public/Attachment/182914593257.pdf>; and U.S. Census Bureau, "Trade in Goods with Taiwan" (Washington, DC: U.S. Department of Commerce). <http://www.census.gov/foreign-trade/balance/c5830.html>.

### Developments in the Cross-Strait Military Balance

Despite a third year of improved economic and diplomatic ties, military tension across the Taiwan Strait remains. Beijing's public statements reflect an effort to downplay the threat that China poses to the island, but Taipei maintains that China's military expansion and recent espionage controversies prove otherwise. Taiwan officials continue to emphasize that it is imperative that the island remain militarily competitive with China in order to maintain an equal hand in cross-Strait negotiations.<sup>232</sup> Taipei has made efforts to demonstrate to the United States that it is in need of additional military technology and equipment and to China that it is still capable of defending itself against an invasion.

Over the past year, Beijing has attempted to make reassuring rather than threatening statements about the cross-Strait military situation. China's 2010 defense white paper, for example, highlighted the progress made in the relationship and downplayed any tension. According to this document:

*The Chinese government has formulated and implemented principles and policies for advancing peaceful development of cross-Strait relations in the new situation, promoted and maintained peace and stability in the area. Significant and positive progress has been achieved in cross-Strait relations.*<sup>233</sup>

The white paper also expressed openness to pursuing confidence-building measures with the Taiwan military, something Taiwan so far has declined.<sup>234</sup> According to Taiwan Military Spokesman Lo Shao-ho, "The proposed confidence-building measures would involve national security and the Ministry of National Defense will follow the government's established policy on China in pushing forward such a mechanism gradually, steadily and practically if necessary."<sup>235</sup> On a May 2011 visit to the United States, People's Liberation Army (PLA) Chief of the General Staff Chen Bingde stated



during a joint press conference that the PLA does not have any missiles stationed “across from Taiwan.”<sup>236</sup> However, the U.S. Department of Defense in its congressionally mandated report on China’s military capabilities noted that “the PLA had deployed between 1,000 and 1,200 short-range ballistic missiles to units opposite Taiwan.”<sup>237</sup>

Several espionage cases alleging the transfer of Taiwan’s military secrets to China have reinforced Taipei’s suspicion of the mainland. In early February 2011, Taiwan Army Major General Lo Hsien-che was arrested on charges of spying for Beijing since 2004.<sup>238</sup> This case is considered by some to be Taiwan’s worst espionage case in 50 years and raised concerns among U.S. officials when it was revealed that details of sensitive U.S. technologies may have been compromised. Documents found in Major General Lo’s office detailed information about Lockheed Martin’s Po Sheng command, control, and communications network being purchased by Taiwan, as well as the procurement details of 30 Boeing AH-64D Longbow Apache attack helicopters.<sup>239</sup> In a second espionage case, a Taiwan businessman was arrested for allegedly trying to steal military secrets for China, but Taiwan’s Ministry of National Defense denied that any national security information was lost.<sup>240</sup> These cases may not be the end of Chinese espionage on the island, as an anonymous Taiwan source told the media that Taiwan knew of at least ten additional spies who had infiltrated Taipei’s national security units and that “[m]any more spies for the Chinese mainland might have gone undetected. . . . The extent of the infiltration into Taiwan’s government units may be worse than imagined.”<sup>241</sup>

In order to show to both China and its own populace that it is capable of defending the island against a mainland attack if necessary, the Taiwan military conducted several high-profile military demonstrations over the past year. These demonstrations included:

- *Military exercises:* In April 2011, Taiwan’s Air Force conducted a high-profile highway landing drill of its fighter jets in a simulation of a surprise attack on Taiwan’s air bases. This was the first highway landing exercise that had been conducted since 2007.<sup>242</sup> Analysts believe that this exercise was meant to send several signals: the first to China in a display of its ability to improvise if its airfields are destroyed, the second to the United States in an attempt to convey to Washington the efficacy with which it would use requested fighter jets, and the third to Taiwan’s public in order to convince them of the Ma Administration’s commitment to defense.<sup>243</sup>
- *Cruise missile developments:* Over the past year, Taiwan announced that it had begun producing two new cruise missiles. In December 2010, Taiwan’s Deputy Defense Minister Chao Shih-chang stated that Taiwan was mass producing the Hsiung Feng IIE, a land-attack cruise missile under development since the late 1990s.<sup>244</sup> With an estimated range between 500 and 650 kilometers, the Hsiung Feng IIE is capable of hitting targets on China’s mainland.<sup>245</sup> Deputy Defense Minister Chao also confirmed that Taiwan had begun producing the Hsiung Feng III, a supersonic antiship cruise missile.<sup>246</sup> In May



2011, an official government statement declared that the Hsiung Feng III will be outfitted on over a dozen navy vessels and patrol boats.<sup>247</sup> However, the accuracy of the Hsiung Feng III was called into question when, during a June 2011 routine test, the missile failed to reach its target, reportedly due to a computer glitch.<sup>248</sup>

- *New missile boats*: In April 2011, President Ma inaugurated a fleet of ten missile boats equipped with stealth capabilities and antiship cruise missiles. These boats, the *Kuang Hua* VI-class missile boat, joined a group of ten already in service in Taiwan's northeastern naval base in Suao and will be followed by another ten by the end of the year. The 171-ton *Kuang Hua* boats will replace Taiwan's aging 50-ton *Seagull*-class missile boats.<sup>249</sup>
- *Naval stealth capabilities*: In July 2011, Taiwan's Navy revealed that it had developed a radar-absorbing stealth coating that makes it significantly harder for radar to detect naval vessels coated with the substance.<sup>250</sup>
- *F-CK-1 fighter upgrade*: In an effort to improve its deteriorating air defense capabilities,\* Taiwan has sought to upgrade its indigenously developed fighter aircraft, the F-CK-1A/B Indigenous Defense Fighters. In June 2011, Taiwan's Air Force took delivery of the first six upgraded fighters. Sixty-five more fighters, out of a total of 125, are set to be upgraded by the end of 2012. The upgrades included enhanced radar, electronic warfare systems, and cockpit computers, as well as the ability to double the payload to four air-to-air missiles.<sup>251</sup>
- *Missile tests*: Taiwan also conducted two missile tests this past year in an effort to demonstrate its defensive capabilities, but during both tests a substantial portion of the missiles failed. In January 2011, six of 19 surface-to-air and air-to-air missiles failed to reach their targets, prompting President Ma to express public dissatisfaction with the results.<sup>252</sup> In a March 2011 test, two out of four surface-to-air missiles again missed their targets. Taiwan's Defense Minister Kao Hua-chu stated that problems with the tests could be due to both human and mechanical errors, and a Democratic Progressive Party spokesman criticized the Ministry of Defense for not solving the problem after the first unsuccessful test.<sup>253</sup>

Further progress in developing Taiwan's indigenous defense capabilities may be hampered by budgetary constraints. Taiwan's 2011 defense budget reached a five-year low of \$9.2 billion, or approximately 2.2 percent of Taiwan's gross domestic product (GDP). In a meeting in Taiwan, Taiwan's Ministry of Defense described to Commissioners how, although the Ma Administration desired a target of 3 percent of GDP for the defense budget, this was unattainable due to economic constraints stemming from the 2010 typhoon recovery and the global financial crisis.<sup>254</sup> Budget cuts have already impacted President Ma's plan to convert the military from a

\*For more on Taiwan's deteriorating air capabilities, see the U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), pp. 149–152.

conscript-based force to an all-volunteer force.<sup>255</sup> Budget constraints may also have postponed the purchase of U.S. Patriot missiles and Black Hawk helicopters, contained in the Obama Administration's January 2010 arms sale notification to Congress.<sup>256</sup> While Kuomintang legislator Lin Yu-fang asserted that the reason for the postponement was a budget shortfall, Taiwan Defense Ministry spokesman Luo Shou-he blamed production delays.<sup>257</sup> Because of the complexity of the U.S. foreign military sales process, it is unclear whether either reason is true, and to date only four of the 60 Black Hawk helicopters contained in the January 2010 notification are under contract.<sup>258 \*</sup>

In accordance with the Taiwan Relations Act of 1979<sup>†</sup> and Taiwan's designation as "a major non-NATO [North American Treaty Organization] ally" for the provision of defensive arms,<sup>‡</sup> on September 21, 2011, the Obama Administration notified Congress of a potential arms sale to Taiwan for almost \$5.9 billion. The notification contained three separate components: an upgrade to Taiwan's current inventory of 145 F-16A/B fighters (\$5.3 billion), a continuation of the F-16 training program in the United States for Taiwan F-16 pilots (\$500 million), and spare parts for Taiwan's fighter and transport aircraft (\$52 million). The proposed upgrade to Taiwan's F-16A/B fighter fleet includes the following:<sup>259</sup>

- Active electronically scanned array radars
- Global Positioning System navigation equipment
- Improved electronic warfare systems
- Updated cockpit computer systems
- Engineering and design study for engine upgrade
- Improved communication equipment
- Data link terminals
- Helmet targeting systems
- Night vision systems
- Laser-guided munitions
- Spare parts
- Logistical support

\*Part of the difficulty in determining the status of Taiwan arms sales is the large gap between when the administration notifies Congress about a possible arms sale and when the actual item in question is transferred to Taiwan. For example, in October 2008, the Bush Administration notified Congress of the possible arms sale of 30 Apache attack helicopters to Taiwan. According to U.S. government website USASpending.gov, a preliminary "long lead contract" for the production of these helicopters was issued on July 30, 2009, and to date, only 9 percent of the total \$2.5 billion has been obligated by the Taiwan government. Delivery for these helicopters is not expected to begin until at least 2014. USASpending.gov, "Prime Award Spending Data: W58RGZ09C0147," September 23, 2011. [http://www.usaspending.gov/search?query=&search\\_type=&formFields=eyJtZWFiY2hUZXJtIjpblc1OFJHwJA5QzAxNDciX X0%3D#](http://www.usaspending.gov/search?query=&search_type=&formFields=eyJtZWFiY2hUZXJtIjpblc1OFJHwJA5QzAxNDciX X0%3D#); Defense Security Cooperation Agency, "Boeing Co., W58RGZ-09-G-0147: \$141,701,518" (Washington, DC: U.S. Department of Defense, November 8, 2010). <http://air-attack.com/contracts/date/2010-11-08>; and China News Agency (Taiwan), "Boeing Gets Taiwan Apache Helicopter Contract," November 9, 2010. <http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20101109000044&cid=1102>. NOTE: The Boeing contract number contains a typo and should actually be W58RGZ-09-C-0147.

†The Taiwan Relations Act (TRA) of 1979 (Public Law 96-8) helps govern the U.S. relationship with Taiwan in the absence of formal diplomatic recognition. "The TRA specifies that it is U.S. policy, among the stipulations: to consider any non-peaceful means to determine Taiwan's future 'a threat' to the peace and security of the Western Pacific and of 'grave concern' to the United States; 'to provide Taiwan with arms of a defense character,' and 'to maintain the capacity of the United States to resist any resort to force or other forms of coercion' jeopardizing the security, or social or economic system of Taiwan's people." Shirley A. Kan, "China/Taiwan: Evolution of the 'One China' Policy—Key Statements from Washington, Beijing, and Taipei" (Washington, DC: Congressional Research Service, July 9, 2007), summary page. A full text of the act is available at <http://www.ait.org.tw/en/taiwan-relations-act.html>.

‡According to Public Law 107-228, "for purposes of the transfer or possible transfer of defense articles or defense services under the Arms Export Control Act (22 U.S.C. 2751 et seq.), the Foreign Assistance Act of 1961 (22 U.S.C. 2151 et seq.), or any other provision of law, Taiwan shall be treated as though it were designated a major non-NATO [North American Treaty Organization] ally (as defined in 644(q) of the Foreign Assistance Act of 1961 (22 U.S.C. 2403(q))." The Foreign Relations Authorization Act of Fiscal Year 2003, Public Law 107-228, 107th Cong., 1st sess., September 30, 2002.

According to the announcement of the possible sale, “the improved capability, survivability, and reliability of newly retrofitted F-16A/B aircraft will greatly enhance the recipient’s ability to defend its borders.”<sup>260</sup>

In response to the arms sale announcement, Beijing quickly followed up on its previous warnings to the United States. Prior to the announcement, China repeatedly expressed its opposition to the sale in several official venues, such as during Secretary Gates’ January 2011 trip to China and during the May 2011 trip of Chen Bingde, chief of the PLA General Staff, to the United States.<sup>261</sup> Immediately following the announcement, China’s Ministry of Foreign Affairs spokesperson noted that:

*Paying no heed to China’s repeated solemn representations, the US side keeps selling advanced arms to Taiwan under the pretext of the Taiwan Relations Act. Its action has grossly violated the three China-US joint communiqués, especially the principles enshrined in the August 17 Communiqué. It constitutes a serious interference in China’s internal affairs and severely undermines China’s national security and reunification. It also impairs China-US relations and the peace and stability across the Taiwan Straits. The Chinese Government and people will by no means accept it. The erroneous practice of the US will inevitably cause damage to China-US relations and bilateral exchanges and cooperation in the military, security and other fields, and the responsibility completely rests with the US side. [emphasis added].*<sup>262</sup>

A day after the arms sales announcement, China’s foreign minister, Yang Jiechi, gave a speech in New York to the National Committee on U.S.-China Relations and the U.S.-China Business Council, stating that:

*The Chinese side urges the U.S. side to fully recognize that U.S. arms sales to Taiwan is a highly sensitive and harmful issue. The Chinese side urges the U.S. side to take China’s solemn position very seriously, correct the mistake of selling weapons to Taiwan, immediately revoke the above-mentioned wrong decision, stop arms sales to Taiwan and U.S.-Taiwan military contacts, and take real actions to uphold the larger interest of China-U.S. relations and peace and stability in the Taiwan Straits.*<sup>263</sup>

A few days later, a senior State Department official provided details about a September 26 meeting between Secretary of State Hillary Rodham Clinton and Foreign Minister Yang. According to the State Department official, Foreign Minister Yang indicated to Secretary Clinton that China was “going to suspend or cancel or postpone a series of military-to-military engagements” with the U.S. military, just restarted back in January 2011. The official also warned that more, unspecified retaliations may be forthcoming from China.<sup>264</sup>

With the Obama Administration’s announcement of the possible sale of F-16A/B retrofits to Taiwan, Taiwan has two arms sales requests still outstanding: F-16C/D fighter jets and diesel-electric submarines. Since 2006, Taiwan has attempted to submit a Letter

of Request to the United States for the purchase of 66 F-16C/D fighters from the United States to replace Taiwan's aging aircraft, especially its 1960s-era F-5 fighters. However, to date, neither the Bush Administration nor the Obama Administration has accepted Taiwan's Letter of Request, the first step in the foreign military sales process.<sup>265</sup> Over the past year, Taiwan officials have repeatedly called for the United States to approve the sale of F-16C/D fighters to Taiwan. During the Commission's trip to Taiwan, for example, President Ma described how the sale of the F-16C/D fighters is critical in order to offset the shifting of the cross-Strait military balance in China's favor.<sup>266</sup> Despite Taiwan's repeated attempts to submit a Letter of Request for the F-16C/D, its inability to submit the letter prevents any deliberation of an arms sale from going forward and keeps Taiwan defense planners in suspense over the possibility of a future sale of the F-16C/D. Immediately after the announcement of the potential sale of the F-16A/B upgrade package, President Ma noted that his administration, while appreciative of the F-16A/B upgrade, would continue to press for the sale of the 66 F-16C/D fighters.<sup>267</sup>

#### **Recent Congressional Actions Related to Taiwan Arms Sales**

Over the last year, Members of the U.S. Congress have expressed concern regarding Taiwan's ability to defend itself from a Chinese attack. In addition to a number of public statements, Members of Congress have taken the following steps in support of U.S. arms sales to Taiwan:

- On April 13, 2011, Representative Robert Andrews (D-NJ) introduced H.Cong.Res.39, which expresses the sense of Congress that the president should move forward with the sale to Taiwan of new and upgraded F-16s.
- On May 26, Senate Taiwan Caucus Co-Chairmen Robert Menendez (D-NJ) and James Inhofe (R-OK) sent a letter to President Obama urging the administration to approve the sale of F-16C/D fighters to Taiwan. The letter was signed by 45 senators.
- On July 20, the House Committee on Foreign Affairs passed H.R. 2583, *The Foreign Relations Authorization Act for Fiscal Year 2012*. The bill contains language that would require the president to take immediate steps to sell to Taiwan both the 66 F-16C/D fighters and the upgrade package for Taiwan's F-16A/B fighters. The bill also requires the sale of the eight diesel-electric submarines once Taiwan has budgeted for them. This language was included in the bill through amendments offered by Representatives Howard Berman (D-CA), Dan Burton (R-IN), and Gerry Connolly (D-VA) and passed by voice votes.

**Recent Congressional Actions Related to Taiwan  
Arms Sales—Continued**

- On August 1, the House Taiwan Caucus, led by Representatives Shelley Berkley (D–NV), Gerry Connolly (D–VA), Mario Diaz-Balart (R–FL), and Phil Gingrey (R–GA), sent a letter with 181 House cosigners to President Obama urging the administration to approve the sale of F–16 C/D fighters to Taiwan.
- On September 12, Senators John Cornyn (R–TX) and Robert Menendez (D–NJ) introduced S.1539, *The Taiwan Airpower Modernization Act of 2011*, which would require the president to sell to Taiwan the requested 66 F–16C/D fighters.
- On September 21, Representative Kay Granger (R–TX) introduced the House version of *The Taiwan Airpower Modernization Act of 2011*, H.R. 2992.
- On September 21, the Senate voted on an amendment offered by Senator John Cornyn (R–TX) S.Amdt.634 to H.R.2832, which would have required the president to sell to Taiwan no fewer than 66 F–16C/D fighters. The amendment failed in the Senate by a vote of 48–48.
- On September 23, Representative Ileana Ros-Lehtinen (R–FL) introduced H.R.2918, *The Taiwan Policy Act of 2011*, which, among other things, would make it the policy of the United States to accept Taiwan’s Letter of Request for the F–16C/D fighters or to provide Taiwan with a formal sales offer for the aircraft. The legislation also would require the administration to consult with Congress regarding Taiwan arms sales and to provide an annual report to Congress detailing Taiwan’s requests for purchase of defense articles; the defense needs asserted by Taiwan; and the decision-making process used to reject, postpone, or modify any such request.

A second outstanding arms sales request by Taiwan is for diesel-electric submarines. First requested in 1995, Taiwan’s request for eight diesel-electric submarines was approved by the Bush Administration in 2001. However, subsequent disputes over the price and funding of the submarines held up the actual sale. In 2002, Taiwan amended its original request for the purchase of the submarines to include a requirement for some of the submarines to be produced in Taiwan with U.S. assistance, further hindering Taiwan’s procurement of the submarines. In 2006, Taiwan submitted a formal Letter of Request for a two-phased approach to the procurement: an initial submarine design phase, followed by possible submarine construction. In January 2008, the Bush Administration accepted Taiwan’s Letter of Request for the submarine design phase. However, neither the Bush Administration nor the Obama Administration has notified Congress of any pending submarine design program. Taiwan continues to reiterate its need for new submarines.<sup>268</sup> In August 2011, President Ma expressed to the Commissioners his desire to purchase the submarines.<sup>269</sup> Later in that trip, the Commissioners heard from Taiwan’s Minister of Defense Kao Hua-chu that these submarines are critical to Taiwan’s de-



fense, since its current fleet of two 1970s-era submarines is ineffective against China's improving naval capabilities.<sup>270</sup> \*

### **Implications for the United States**

Improvements in the diplomatic and economic realm benefit the United States by noticeably reducing tension across the Taiwan Strait. Growing trade between the two sides decreases the likelihood of a conflict in the near future. Similarly, an increase in people-to-people and government relations across the Taiwan Strait helps to prevent misunderstanding. The overall effect of improved cross-Strait relations helps to safeguard the stability of the region.

At the same time, the continued cross-Strait military standoff tempers the positive developments and potentially endangers U.S. interests in the region. As China continues to increase its military capabilities while Taiwan's ability to defend itself is increasingly in question, the peaceful resolution of the cross-Strait situation is less likely. A gross military imbalance could also lead Beijing to resolve the cross-Strait problem through the use of military force, possibly resulting in U.S. military involvement.

### **Conclusions**

- In 2011, Taiwan and China have continued to strengthen their economic and diplomatic relations by focusing on implementing previous agreements rather than signing new agreements.
- A major factor leading to the slower pace of reduced tensions across the Taiwan Strait is Taiwan's upcoming presidential and legislative elections. Seeking to prevent improving cross-Strait ties from being used against the incumbent Kuomintang Party, both Taiwan and China have moved away from pressing for rapid negotiations and developments as in previous years.
- The cross-Strait military balance continues increasingly to favor China, making it less likely that a peaceful resolution to the Taiwan issue will occur. Despite attempts to improve its capacity to defend the island against a potential attack from the mainland, Taiwan continues publicly to call for additional U.S. arms sales to augment its defense needs.

---

\*For more on China's growing naval capabilities, see chapter 2, section 2, of the Commission's *2009 Annual Report to Congress*. U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009).



## SECTION 4: HONG KONG

### Introduction

Hong Kong's relationship with mainland China is characterized in Hong Kong's constitution by the phrase "one country, two systems," whereby Hong Kong enjoys "a high degree of autonomy" in governing itself while still being an "unalienable" part of China.<sup>271</sup> Some developments in Hong Kong over the past year suggest that Beijing's influence in the city's affairs is growing. In the past year, Beijing enhanced its focus on Hong Kong's economy, utilizing it as a vehicle for the internationalization of China's currency, the renminbi (RMB). Mainland involvement in Hong Kong's political affairs was an issue of contention among Hong Kong policymakers and citizens throughout 2011. Furthermore, while Hong Kong citizens and press largely continue to enjoy freedom of expression and assembly, these rights were challenged at times by Hong Kong authorities, who are perceived to be acting out of deference to Beijing. On its trip to mainland China, the Commission stopped in Hong Kong to gain insight into these developments and their implications.

### The Role of Hong Kong in China's Economic Policies

Hong Kong's unique status as an international financial center and trading hub affords it importance in China's economic policies. This was affirmed in 2011 when China released its 12th Five-Year Plan (2011–2015), which was the first five-year plan to include a chapter devoted specifically to Hong Kong and Macau.<sup>272</sup> The components of the 12th Five-Year Plan related to Hong Kong were laid out in a much-vaunted visit by China's Vice Premier Li Keqiang to Hong Kong in August 2011.\* In his visit, the vice premier described Beijing's new policies and measures "designed to deepen the economic and financial cooperation between the mainland and Hong Kong": developing Hong Kong into an offshore RMB center, expanding access to China's markets, enhancing Hong Kong's standing as an international financial center, supporting Hong Kong's participation in international and regional economic cooperation, helping Hong Kong companies "go global," and enhancing Guangdong-Hong Kong-Macau economic cooperation, among other things.<sup>273</sup>

The most visible of these efforts, even before it was reiterated in the five-year plan, has been China's development of Hong Kong as a center for offshore RMB transactions and a launch pad for the

---

\* Vice Premier Li will likely succeed current Premier Wen Jiabao in 2013. His visit was seen as an indication of this, because only the most senior officials get to make such high-profile trips to Hong Kong. Willy Lam, "Li Keqiang Meets Hong Kong," *Wall Street Journal*, August 15, 2011, <http://online.wsj.com/article/SB10001424053111903918104576503311098645364.html>; Goldman Sachs representative, meeting with the U.S.-China Economic and Security Review Commission, Hong Kong, August 15, 2011.

internationalization of China's currency. China has designated Hong Kong as a platform to conduct a limited amount of trading, investing, and lending in RMB as part of a national strategy gradually to internationalize its currency.<sup>274</sup> (For more information on Beijing's currency globalization efforts, see chap. 1, sec. 1, of this Report.) Hong Kong's unique status as a global trade and finance center and the "freest economy in the world"<sup>275</sup> makes it a useful vehicle for China to carry out this strategy. Moreover, Hong Kong provides a controlled setting for China to test out its policies, thanks to its economic and political ties to the mainland. Goldman Sachs representatives in Hong Kong told Commissioners that the city had been chosen to be China's offshore RMB market because Beijing would be able to fully control the terms of the market.<sup>276</sup>

To promote demand for the RMB as a currency for international transactions, China in 2011 announced a number of incentivizing policies in both the mainland and Hong Kong. According to Vice Premier Li, the mainland will expand RMB circulation channels between Hong Kong and the mainland, eventually allowing all provinces to conduct trade in Hong Kong using RMB; Hong Kong companies making direct investments on the mainland in RMB will be given additional support from the Chinese government; and more mainland-based financial institutions will be able to issue RMB-denominated bonds in Hong Kong. For example, in conjunction with Vice Premier Li's Hong Kong visit, China's Ministry of Finance issued 20 billion RMB (\$3.1 billion) in treasury bonds in Hong Kong, five billion RMB (\$786 million) of which were targeted at individuals, "giving more investment opportunities for Hong Kong residents," according to the vice premier. Larger RMB bond issuances are to follow in the future.<sup>277</sup>

Hong Kong business representatives, government officials, and journalists told Commissioners during several meetings in Hong Kong that the city's role as a vehicle for China's currency internationalization has been expanding and will expand in the future.<sup>278</sup> One official noted that 550 billion RMB (\$86 billion) had accumulated in Hong Kong's bond markets by August 2011;<sup>279</sup> RMB bank deposits in Hong Kong increased more than six-fold from May 2010 to August 2011.<sup>280</sup>

The emphasis on Hong Kong's economic development in the 12th Five-Year Plan, coupled with attention from high-level mainland officials on the city's economic issues, indicates that Beijing is sensitive to popular discontent over the city's growing economic woes.<sup>281</sup> Citizen discontent over economic management was widespread in 2011, with complaints focused on skyrocketing housing prices (and assumed collusion between political leaders and property tycoons in mainland China), rising unemployment, growing poverty, a widening wealth gap, and unpopular tax reforms, among other things.<sup>282</sup> During his August visit, the vice premier acknowledged some of these economic challenges but emphasized that China was committed to Hong Kong's development and expressed that he was "fully confident" about Hong Kong's economic future.<sup>283</sup> A few months earlier, the head of the central government's Hong Kong and Macau Affairs Office visited Hong Kong and sounded a warning note on the city's economic management. He remarked that the city's government should allocate more resources

for low-cost housing in order to alleviate discontent over growing poverty and high housing costs. He warned that “housing [in Hong Kong] is both a social and economic issue, and if it’s not handled well, it becomes a political issue.”<sup>284</sup>

### **Beijing’s Influence in Hong Kong’s Political Affairs**

Beijing’s creeping influence in Hong Kong’s political affairs continued to be a contentious issue in 2011. For instance, Beijing attained an unprecedented amount of influence in the city’s independent judicial system when Hong Kong’s highest court appealed to China’s National People’s Congress to interpret Hong Kong’s constitution, the Basic Law.<sup>285</sup> This was the first time that Hong Kong courts had requested that Beijing interpret Hong Kong law, and some policymakers and outside analysts feared that this action would set a precedent for greater mainland influence in Hong Kong’s judiciary.<sup>286</sup> The case, in which a Delaware investment fund filed a lawsuit against the Democratic Republic of Congo, hinged on the contested issue of whether sovereign states can be sued in Hong Kong’s courts. The case was referred by Hong Kong’s Court of Final Appeal to the National People’s Congress because it concerned foreign and diplomatic affairs, which, according to the Basic Law, are the responsibility of the central government. In August, the National People’s Congress ruled that Hong Kong law would follow the central government’s position of granting sovereign states immunity from being sued.<sup>287</sup>

Another high-profile example of growing mainland influence was a Hong Kong government proposal to introduce compulsory “moral and national education” for Hong Kong schoolchildren. The proposal was met with staunch opposition by citizens, educators, and some leaders, who denounced it as “political brainwashing” by Beijing, which had advocated patriotic education in Hong Kong since 2007.<sup>288</sup> A public consultation period for the proposal lasted from May until August 2011, and a final curriculum guide is expected to be released by the Hong Kong Ministry of Education in February 2012.<sup>289</sup>

The divisive nature of Beijing’s influence in Hong Kong politics was highlighted following closed-door negotiations over Hong Kong’s electoral reforms between Beijing officials and Hong Kong’s Democratic Party in 2010. The reform amendments highlighted Beijing’s reluctance to allow significant democratic reforms to Hong Kong’s electoral process and exposed conflict within Hong Kong’s prodemocracy camp.<sup>290</sup> The Basic Law states that the “ultimate aim” of Hong Kong’s leadership selection process is “universal suffrage.”<sup>291</sup> However, the city’s top political leaders, the chief executive and the Legislative Council, are currently selected by a largely undemocratic combination of government appointments, popular voting, and functional constituency voting.\*<sup>292</sup> In response to ever-growing demands for universal suffrage from democratic groups, the People’s Republic of China (PRC) Standing Committee of the National People’s Congress in 2007 ruled that Hong Kong’s chief

\*Functional constituencies are interest group voting blocs, mainly comprised of business and industry leaders. These groups, deemed vital to Hong Kong’s economic growth, are reliably pro-Beijing and generally support and reinforce the policy priorities of mainland China. Ngok Ma, “Hong Kong’s Democrats Divide,” *Journal of Democracy* 22:1 (January 2011): 55.

executive and Legislative Council could be elected by universal suffrage *at the earliest* in 2017 and 2020, respectively. The Standing Committee indicated that only minimal changes to electoral law could be made in the meantime.<sup>293</sup>

The administration of Hong Kong Chief Executive Donald Tsang (who was selected by a pro-Beijing election committee in Hong Kong) followed up on the Standing Committee's decision and offered amendments that Chief Executive Tsang said would democratize the electoral process. Prodemocracy members of the Legislative Council planned to veto the amendments, claiming they did not move swiftly enough toward universal suffrage. However, shortly before the July 2010 vote on the amendments, legislators from the Democratic Party, the flagship party of the democratic camp, completed closed-door negotiations with the Liaison Office of the Central People's Government\* and arrived at a compromise: the Election Committee for selecting the chief executive would increase from 800 to 1,200 members, and ten directly elected seats would be added to the 60-member Legislative Council (previously, there had been 30 functional constituency seats and 30 directly elected seats).<sup>294</sup> The amendments were approved by Hong Kong's Legislative Council and administration and will be in effect for the 2012 elections of Hong Kong's next chief executive and Legislative Council.

Hong Kong's administration hailed the deal between the Democratic Party and Beijing as "a victory of reason" and "a milestone in the city's democratic development."<sup>295</sup> However, some within the democratic camp disapproved of the deal and criticized the Democratic Party for collaborating with Beijing to pass what they saw as a weak, pro-Beijing law that did not take sufficient steps toward universal suffrage.<sup>296</sup> One founding Democratic Party legislator quit in protest immediately after the vote, and 30 party members resigned en masse just hours before a Democratic Party annual meeting in December 2010.<sup>297</sup> Included were seven of the Democratic Party's 60 representatives in the District Councils, Hong Kong's "neighborhood" consultative bodies that have a role in choosing the chief executive and the Legislative Council.<sup>298</sup>

Divisions in the democratic camp became more evident as the various democratic groups prepared for November 2011 District Council elections. In past District Council elections, the democratic camp often coordinated its campaigns to ensure that multiple democratic candidates would not compete against each other for any single seat, in an effort to counter overwhelming numbers of pro-Beijing candidates.<sup>299</sup> For the November 2011 elections, however, at least 36 candidates from other democratic groups registered to run against Democratic Party candidates as a punishment for the party's "betrayal" and cooperation with Beijing officials in 2010.<sup>300</sup>

Hong Kong's democratic camp has a history of being disenfranchised by pro-Beijing interests both in the mainland and

\*The Liaison Office of the Central People's Government in the Hong Kong Special Administrative Region acts as the central government's primary liaison with Hong Kong. The office facilitates economic, security, cultural, technological, and educational exchanges between Hong Kong and the mainland. Michael F. Martin, *Prospects for Democracy in Hong Kong: The 2012 Election Reforms* (Washington, DC: Congressional Research Service, February 2011), pp. 9–10. [http://assets.opencrs.com/rpts/R40992\\_20110201.pdf](http://assets.opencrs.com/rpts/R40992_20110201.pdf).

in Hong Kong.<sup>301</sup> Interparty conflict could exacerbate the democrats' already limited influence to the benefit of pro-Beijing parties and their supporters in mainland China.<sup>302</sup> According to Chan Kin Man, director for the Centre for Civil Society Studies at the Chinese University of Hong Kong, the Chinese Communist Party (CCP) "would love to see a divided pro-democracy camp in Hong Kong so that it will not be forced to speed up constitutional reform in the SAR [Hong Kong Special Administrative Region], a process that might destabilize the political equilibrium on the mainland."<sup>303</sup>

### **Rights to Freedom of Expression and Assembly Challenged**

Journalists, activists, and human rights lawyers reported that Hong Kong citizens' efforts to assert their rights to freedom of expression and association were met with increasing intolerance by Hong Kong authorities in 2011.\*<sup>304</sup> The Hong Kong Journalists Association noted in its 2011 Annual Report that freedom of expression and assembly established in the "one country, two systems" policy was often challenged by Hong Kong authorities who appeared to be undermining Hong Kong citizens' democratic rights in deference to mainland political sensitivities:

*There are now growing and disturbing signs that the one-country element is over-riding two-systems, and that could have far-reaching implications on Hong Kong's autonomy and one of its most fundamental rights—freedom of expression and press freedom.*<sup>305</sup>

### **Freedom of Press**

Media organizations in Hong Kong issued complaints of interference in their reporting by Hong Kong authorities, especially in cases when they were covering politically sensitive topics related to mainland China.<sup>306</sup> Police actively prevented reporters from covering large events and political protests and, in some cases, harmed journalists. During Hong Kong's annual July 1 protest,† police used pepper spray on 19 journalists covering the event, including three who were sprayed directly in the eyes.<sup>307</sup> During Vice Premier Li's August visit, police blocked camera lenses and stationed the press area too far away to observe events.<sup>308</sup> Such actions are violations of Hong Kong Police General Orders, which require officers to facilitate the work of news media as much as possible.<sup>309</sup> Press restrictions during Vice Premier Li's visit prompted an outcry among media and citizens, including a protest of 300 journalists condemning police heavy-handedness and harassment of media.<sup>310</sup> A representative of the International Federation of Jour-

\* Article 27 of Hong Kong's Basic Law guarantees Hong Kong citizens "freedom of speech, of the press, and of publication; freedom of association, of assembly, of procession and of demonstration." National People's Congress of the People's Republic of China, *The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China* (Beijing, China: April 4, 1990). [http://www.basiclaw.gov.hk/en/basiclawtext/images/basiclaw\\_full\\_text.pdf](http://www.basiclaw.gov.hk/en/basiclawtext/images/basiclaw_full_text.pdf).

† Every year, on the anniversary of Hong Kong's handover to China from Britain on July 1, 1997, Hong Kong citizens participate in marches and demonstrations. The marches are often used as opportunities for citizens to voice grievances against the government, with participants numbering in the hundreds of thousands in some years. Kevin Drew, "Growing Discontent Seen In Annual Hong Kong Protest," *New York Times*, July 1, 2011. <http://www.nytimes.com/2011/07/02/world/asia/02iht-hong02.html?pagewanted=all>.



nalists told a Legislative Council panel that Hong Kong police were becoming more like China's police, who are known to routinely hassle journalists.<sup>311</sup>

Hong Kong's Basic Law guarantees freedom of the press and encourages independent reporting, but personnel changes in two Hong Kong news stations in 2011 prompted concerns over the editorial independence of the organizations. The government appointment of a veteran civil servant with no experience in public broadcasting as the chief editor of Radio Television Hong Kong was received with skepticism and concern by the station's staff and two journalism associations. These organizations pointed to potential conflicts between the new chief editor's government background and the role of the station in acting as a check on the government.<sup>312</sup> In a similar situation at Hong Kong's Asia Television Limited station, a newly appointed news chief instructed journalists to "tune down" coverage of a Democratic Party protest over the resignation of the news chief's predecessors, which ostensibly occurred over an erroneous report on the death of former Chinese President Jiang Zemin. There was some speculation that the resignations were encouraged for political reasons.<sup>313</sup> The Hong Kong News Executives' Association as well as Democratic Party Vice Chairwoman Emily Lau were among the individuals and organizations expressing concern over the incident.<sup>314</sup>

Self-censorship was reported to be a growing problem in 2011 as well. An annual Hong Kong University survey of the general population showed that a record number of Hong Kong citizens (over half of survey respondents) believe that Hong Kong's media practices self-censorship.<sup>315</sup> The survey also reported that the general credibility rating of the news media had dropped to its lowest level since 2003.<sup>316</sup> In a July 2011 meeting between Commissioners and Alan Leong, Hong Kong legislator and leader of the democratic Civic Party, Mr. Leong acknowledged that self-censorship, while difficult to measure, is a part of the history of Hong Kong's media and exists in Hong Kong reporting today as well.<sup>317</sup>

One positive recent development in Hong Kong's media field has been the rise of social media and citizen reporting. According to the Hong Kong Journalists Association, such informal news outlets are useful in identifying and monitoring local corruption, especially in cases when representatives of the mass media are prevented from gaining access to sites or information.<sup>318</sup> In one case, a citizen media website reported extensively on an urban development project that residents of a nearby housing estate opposed, fearing that the project would stifle ventilation in the neighborhood. The website published an in-depth report detailing public records going back 30 years and chronicling how developers had exploited loopholes in urban planning laws to advance their projects.<sup>319</sup> In another case, more than 40,000 Hong Kong citizens used Facebook to report and protest the construction of a sprawling private estate on protected government land.<sup>320</sup> The Hong Kong Journalists Association deemed these cases of citizen reporting encouraging, noting that "[w]hile the mainstream media face problems such as patriotic pressure and obstruction of government information, the new media are playing an increasingly important role in monitoring the government."<sup>321</sup>



Publications from Hong Kong that Beijing might consider politically sensitive sometimes can be found in mainland China. In meetings with business leaders in Hong Kong, Commissioners were told that some editorially independent newspapers from Hong Kong have limited circulation in China, enabling independent reports on big events such as the fatal high-speed rail train crash in Wenzhou to be picked up in China.<sup>322</sup> Mr. Leong told Commissioners that a critical book about Premier Wen Jiabao, *China's Best Actor: Wen Jiabao*, is widely available at points of exit and entry in Hong Kong and that many mainland Chinese who visit Hong Kong purchase the book.<sup>323</sup>

### ***Freedom of Assembly***

In 2011, Hong Kong citizens continued their tradition of exercising their right to free assembly. The annual July 1 march, attended by 200,000 people, was the second-largest Hong Kong protest since the city was returned to China in 1997.<sup>324</sup> An annual June 4 candlelight vigil in remembrance of the 1989 Tiananmen Square massacre also drew a near-record amount of participants. Police estimated that 77,000 attended the 2011 candlelight vigil, but event organizers estimated over 150,000 participants, which would make it the one of the city's largest June 4 vigils in 22 years.<sup>325</sup> Large demonstrations against local and national government policies took place in March and June as well, with smaller protests occurring throughout the year.<sup>326</sup> Mr. Leong told Commissioners that some participants at the larger events were visiting mainland Chinese, some of whom expressed that they wanted to participate in a "free society demonstration."<sup>327</sup>

Citizens, activists, and journalists reported several instances of police interference in protest activities in 2011. According to the Civil Human Rights Front, 179 people were arrested in Hong Kong protests in the first half of 2011, compared to just 53 arrests in 2010.<sup>328</sup> The Hong Kong Journalists Association reported that police were particularly intolerant of protests staged near Beijing's Liaison Office.<sup>329</sup> Police excess was also reported during Vice Premier Li's visit, when protesters gathered to voice concerns about human rights, among other things.<sup>330</sup> At a Hong Kong University event attended by Vice Premier Li, police detained three protesting students, which may have constituted false imprisonment, according to Johannes Chan Man-mun, a dean at the university.<sup>331</sup> Hong Kong police have asserted that this claim is unfounded.<sup>332</sup> At another event associated with Vice Premier Li's visit, security officers reportedly dragged away and arrested a man wearing a shirt with the slogan "Vindicate June 4," a reference to the Tiananmen Square massacre.\* According to Legislative Council member James To Kun-sun, police on duty during these demonstrations were trying to prevent Vice Premier Li from being embarrassed.<sup>333</sup> After the incident, several lawmakers requested an investigation into police tactics during the visit, and Hong Kong Police Commissioner Andy Tsang was questioned in a Legislative Council session. Some

\* Discussion of the June 4, 1989, Tiananmen Square massacre is prohibited on the mainland, but in Hong Kong the event is generally freely discussed and commemorated. BBC, "Tiananmen: Thousands in Hong Kong mark crackdown," June 4, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-13658037>.

lawmakers and at least 1,000 citizens called for his resignation.<sup>334</sup> A police review of security arrangements during the vice premier's visit was ongoing at the time of the publication of this Report.

Hong Kong police also have taken more subtle measures to obstruct protest activities. In an April protest opposing the arrest and detention of mainland dissident artist Ai Weiwei,\* and again during the annual July 1 protest, police restricted access to protest venues.<sup>335</sup> Mr. Leong indicated in his meeting with the Commission that police directed participants in the June 4 candlelight vigil to walk an unnecessarily long distance to reach the venue. Mr. Leong characterized this excessive police requirement as "sending a message to the Hong Kong public."<sup>336</sup>

Restriction of travel to Hong Kong was also a growing problem in 2011. The Hong Kong government was accused of catering to mainland political sensitivities when it denied visas to two prominent mainland dissidents ostensibly to prevent them from attending the funeral of Szeto Wah, a founder of Hong Kong's democracy movement.<sup>337</sup> The two dissidents, Wang Dan and Wu'er Kaixi, live in exile in Taiwan. A democratic member of the Legislative Council lamented this action as indicative of the erosion of the "one country, two systems" policy.<sup>338</sup>

Travel from Hong Kong to the mainland continued to be restricted in 2011 as well. In an August 2011 letter to Vice Premier Li from Hong Kong's Democratic Party, Chairman Alfred Ho wrote, "For more than 20 years, many members of the Hong Kong pro-democracy movement have been banned from traveling to [the] Mainland. The freedom of travel to the Mainland is a fundamental right of all Chinese citizens and should not be deprived of."<sup>339</sup>

### **Implications for the United States**

Chinese and Hong Kong policies to promote the gradual internationalization of the RMB are intended, among other things, to allow the RMB to develop into an alternate reserve currency to the U.S. dollar, which is currently the internationally preferred reserve currency. After the global financial crisis, Chinese policymakers indicated a desire to reduce reliance on the dollar and diversify away from U.S. Treasuries.<sup>340</sup>

Hong Kong law, especially as it relates to commercial activity, impacts U.S. and foreign interests operating in Hong Kong. In the case of the abovementioned court decision referred by Hong Kong's Court of Final Appeal to Beijing, a U.S. investment fund's lawsuit filed in Hong Kong was decided by China's National People's Congress. If Beijing becomes more active in Hong Kong's judicial affairs, cases like this may occur again.<sup>341</sup>

Restrictions on Hong Kong's administrative autonomy and freedom of expression and assembly run counter to Hong Kong's Basic Law, as memorialized in the U.S. Hong Kong Policy Act of 1992, which expresses U.S. support for the maintenance of a "high degree

\*Ai Weiwei, a mainland Chinese artist and political dissident, was arrested in April 2011 for suspected "economic crimes," although it is widely assumed that the government targeted him for political, not economic, reasons. He was detained for almost three months before being released on June 22, 2011. Edward Wong, "Dissident Chinese Artist is Released," *New York Times*, June 22, 2011. <http://www.nytimes.com/2011/06/23/world/asia/23artist.html?pagewanted=all>.

of autonomy” in Hong Kong’s self-governance and for human rights development and democratization in Hong Kong.<sup>342</sup>

### **Conclusions**

- Hong Kong plays a central role in China’s policy goal of internationalizing its currency. In 2011, China introduced substantial new measures supporting Hong Kong’s status as China’s primary platform for RMB offshoring.
- Mainland involvement in Hong Kong’s political affairs was evident in 2011, prompting citizen discontent and conflict within Hong Kong’s democratic groups.
- Hong Kong continued to have a vibrant protest culture in 2011, with record amounts of participants in some annual protests. However, there were reports that police sometimes challenged Hong Kong citizens’ rights during protests, especially when protests targeted mainland China.
- Hong Kong’s mass media reported increased interference in their activities by Hong Kong authorities in 2011. Public perception of self-censorship in Hong Kong’s press peaked in 2011, and public opinion of press credibility fell to its lowest level in eight years.

## **RECOMMENDATIONS**

### ***An Overview of China's Relations with North Korea and Iran***

The Commission recommends that:

- Congress investigate whether U.S. sanctions have been imposed on all Chinese firms that have violated the sanction laws by investing in Iran's petroleum industry or providing Iran with refined petroleum products or advanced conventional weapons.
- Congress, in light of China's continued investments in North Korea, hold hearings to evaluate the effectiveness of expanding North Korean sanctions to cover foreign firms investing in North Korea's natural resource industry.

### ***Actors in China's Foreign Policy***

The Commission recommends that:

- Congress investigate the extent to which the People's Liberation Army is becoming a more influential actor in China's foreign policy-making.
- Members of Congress make an effort to engage with multiple official and unofficial foreign policy actors during their trips to China in order to better understand and establish channels of communication with these actors.

### ***Taiwan***

The Commission recommends that:

- Congress urge the administration to sell Taiwan the additional fighter aircraft it needs to recapitalize its aging and retiring fleet.
- Congress request from the administration an update on the Taiwan submarine program that was approved for sale by the U.S. government in 2001.
- Congress explore in hearings the implications for the United States and the region of closer China-Taiwan relations.

### ***Hong Kong***

The Commission recommends that:

- Congress reauthorize Section 301 of the Hong Kong Policy Act of 1992, which requires the U.S. secretary of State to submit an annual report to Congress on political, social, and economic developments in Hong Kong as they relate to the United States. This

should include reporting on China's measures to use Hong Kong as a platform for the internationalization of the renminbi.

- Members of Congress, when visiting mainland China, also visit Hong Kong and that Congress encourage senior administration officials, including the secretary of State, to make visits to Hong Kong part of their travel.
- Congress encourage its Members to raise the issue of preserving Hong Kong's special status when meeting with members of China's National People's Congress.

## ENDNOTES FOR CHAPTER 3

1. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of David Helvey, April 13, 2011; Christopher Bodeen, "China not assigning blame in South Korea sinking," Associated Press, May 27, 2010. <http://www.usatoday.com/news/world/2010-05-27-china-southkorea-N.htm>; and International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea," *Asia Report* 200 (Brussels, Belgium: January 21, 2011): 2.
2. Yoo Jee-ho and Kang Chan-ho, "After Delay, China calls Cheonan a tragedy," *Korea Joongang Daily*, April 23, 2010. <http://joongangdaily.joins.com/article/view.asp?aid=2919581>.
3. Open Source Center, "Analysis: Chinese Reaction to Ch'o'nan Investigation Focuses on Stability," May 20, 2010. OSC ID: FEA20100520005214. <http://www.opensource.gov>; and International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea," *Asia Report* 200 (Brussels, Belgium: January 21, 2011): 3.
4. Colum Lynch, "Security Council draft statement condemns sinking of S. Korean vessel, skirts blame," *Washington Post*, July 9, 2010. <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/08/AR2010070805068.html>; and International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea," *Asia Report* 200 (Brussels, Belgium: January 21, 2011): i.
5. Jack Kim and Chris Buckley, "South Korea suspects North has more uranium sites," Reuters, December 14, 2010. <http://www.reuters.com/article/2010/12/14/us-korea-north-uranium-idUSTRE6BD0CE20101214>.
6. Office of the Press Secretary, "U.S.-China Joint Statement" (Washington, DC: The White House, January 19, 2011). <http://www.whitehouse.gov/the-press-office/2011/01/19/us-china-joint-statement>.
7. Chosun Ilbo (South Korea), "China Blocks UN Warning over N. Korea's Uranium Program," February 25, 2011. [http://english.chosun.com/site/data/html\\_dir/2011/02/25/2011022500432.html](http://english.chosun.com/site/data/html_dir/2011/02/25/2011022500432.html).
8. Ian Johnson and Helen Cooper, "China Seeks Talks to Ease Korean Tension," *New York Times*, November 28, 2010. <http://www.nytimes.com/2010/11/29/world/asia/29korea.html>.
9. Agence France-Presse, "China blocks UN action against N Korea," December 1, 2010. <http://news.smh.com.au/breaking-news-world/china-blocks-un-action-against-n-korea-20101201-18fz3.html>; and International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea," *Asia Report* 200 (Brussels, Belgium: January 21, 2011): i.
10. United Nations, "Report to the Security Council from the Panel of Experts established Pursuant to Resolution 1874 (2009)" (New York, NY: 2010), p. 1; and Chris Buckley, "China plays down U.N. report on North Korea, Iran proliferation," Reuters, May 17, 2011. <http://www.reuters.com/article/2011/05/17/us-china-korea-north-idUSTRE74G0GY20110517>.
11. William J. Broad, James Glanz, and David E. Sanger, "Iran Fortifies its Arsenal with the Aid of North Korea," *New York Times*, November 28, 2010. <http://www.nytimes.com/2010/11/29/world/middleeast/29missiles.html>.
12. Richard Weitz, "China's Proliferation Problem," *Diplomat* (Tokyo, Japan), May 24, 2011. <http://the-diplomat.com/2011/05/24/china%E2%80%99s-proliferation-problem/>; and Chris Buckley, "China plays down U.N. report on North Korea, Iran proliferation," Reuters, May 17, 2011. <http://www.reuters.com/article/2011/05/17/us-china-korea-north-idUSTRE74G0GY20110517>.
13. Chris Buckley, "China plays down U.N. report on North Korea, Iran proliferation," Reuters, May 17, 2011. <http://www.reuters.com/article/2011/05/17/us-china-korea-north-idUSTRE74G0GY20110517>.
14. Scott Snyder and See-won Byun, "China-Korea Relations," *Comparative Connections* 12: 4 (January 2011): 105.
15. Scott Snyder and See-won Byun, "China-Korea Relations," *Comparative Connections* 12: 4 (January 2011): 105.
16. Xinhua, "China commemorates 60th anniversary of participation in Korean War," October 26, 2010. [http://news.xinhuanet.com/english/2010/china/2010-10/26/c\\_13574898.htm](http://news.xinhuanet.com/english/2010/china/2010-10/26/c_13574898.htm).
17. Korean Central Broadcasting Station, "PRC [People's Republic of China] President Receives Visiting DPRK [Democratic People's Republic of Korea] Friendship Delegation," July 11, 2011. OSC ID: KPP20110713045001. <http://www.opensource.gov>.
18. Dick K. Nanto and Mark E. Manyin, *China-North Korea Relations* (Washington, DC: Congressional Research Service, December 28, 2010), p. 13.



19. Drew Thompson, *Silent Partners: Chinese Joint Ventures in North Korea* (Washington, DC: U.S.-Korea Institute at the School for Advanced International Studies, February 2011), p. 3.
20. Dick K. Nanto and Mark E. Manyin, "China-North Korea Relations" (Washington, DC: Congressional Research Service, December 28, 2010), p. 14.
21. International Trade Centre, "Trade Map" (Geneva, Switzerland: August 12, 2011). [http://www.trademap.org/light/Bilateral\\_TS.aspx](http://www.trademap.org/light/Bilateral_TS.aspx); Namsub Shim, "2010 South-North Trade, North-China Trade Tendency Comparison," *Special Reports* (Seoul, South Korea: Korea International Trade Association, March 30, 2011). [http://global.kita.net/engapp/board\\_view.jsp?no=807&code=S4001](http://global.kita.net/engapp/board_view.jsp?no=807&code=S4001); and Dick K. Nanto and Mark E. Manyin, "China-North Korea Relations" (Washington, DC: Congressional Research Service, December 28, 2010), p. 15.
22. International Trade Centre, "Trade Map" (Geneva, Switzerland: August 12, 2011). [http://www.trademap.org/light/Bilateral\\_TS.aspx](http://www.trademap.org/light/Bilateral_TS.aspx); and Dick K. Nanto and Mark E. Manyin, "China-North Korea Relations" (Washington, DC: Congressional Research Service, December 28, 2010), p. 16.
23. International Trade Centre, "Trade Map" (Geneva, Switzerland: August 12, 2011). [http://www.trademap.org/light/Bilateral\\_TS.aspx](http://www.trademap.org/light/Bilateral_TS.aspx); and Dick K. Nanto and Mark E. Manyin, "China-North Korea Relations" (Washington, DC: Congressional Research Service, December 28, 2010), p. 16.
24. Dick K. Nanto, "Increasing Dependency: North Korea's Economic Relations with China," *Korea's Economy 2011*, 27 (Washington, DC: Korea Economic Institute, 2011), p. 77.
25. Jayshree Bajoria, "The China-North Korea Relationship" (Washington, DC: Council on Foreign Relations, October 7, 2010). <http://www.cfr.org/china/china-north-korea-relationship/p11097m>.
26. U.S.-China Business Council, "US-China Trade Statistics and China's World Trade Statistics." <https://www.uschina.org/statistics/tradetable.html>.
27. Dick K. Nanto and Mark E. Manyin, "China-North Korea Relations" (Washington, DC: Congressional Research Service, December 28, 2010), p. 13; and Bureau of East Asian and Pacific Affairs, "Background Note: North Korea" (Washington, DC: U.S. Department of State, April 29, 2011). <http://www.state.gov/r/pa/ei/bgn/2792.htm>.
28. Open Source Center, "OSC Report: China—Directory of PRC Enterprises in North Korea," April 19, 2011. OSC ID: KPP20110419032002. <http://www.opensource.gov>.
29. Korean Central News Agency, "KCNA: DPRK [Democratic People's Republic of Korea], PRC Hold Ground-breaking Ceremonies for Joint Projects in Islands, Naso'n," June 9, 2011. OSC ID: KPP20110609971156. <http://www.opensource.gov>; and Daniel Gearin, "Chinese Infrastructure and Natural Resources Investments in North Korea" (Washington, DC: U.S.-China Economic and Security Review Commission, *Staff Background*, October 20, 2010).
30. Jay Solomon and Jeremy Page, "Chinese Firm to Invest in North Korea," *Wall Street Journal*, January 19, 2011. [http://online.wsj.com/article/SB1001424052748704678004576090270026745\\_368.html](http://online.wsj.com/article/SB1001424052748704678004576090270026745_368.html).
31. *Chosun Ilbo* (South Korea), "Construction of N. Korea-China Bridge to Start in October," February 26, 2010. [http://english.chosun.com/site/data/html\\_dir/2010/02/26/2010022601081.html](http://english.chosun.com/site/data/html_dir/2010/02/26/2010022601081.html); Jay Solomon and Jeremy Page, "Chinese Firm to Invest in North Korea," *Wall Street Journal*, January 19, 2011. [http://online.wsj.com/article/SB1000142405274870467800457609027002674\\_5368.html](http://online.wsj.com/article/SB1000142405274870467800457609027002674_5368.html); and Park Jun Hyeong, "New Bridge Rising from the Yalu," *Daily NK* (South Korea), August 30, 2011. <http://www.dailynk.com/english/read.php?cataId=nk00100&num=8115>.
32. Open Source Center, "OSC Report: China—Directory of PRC Enterprises in North Korea," April 19, 2011. OSC ID: KPP20110419032002. <http://www.opensource.gov>; and United Nations, "Report to the Security Council from the Panel of Experts established Pursuant to Resolution 1874 (2009)" (New York, NY: 2010), p. 36. <http://www.fas.org/irp/eprint/ser1874.pdf>.
33. Drew Thompson, *Silent Partners: Chinese Joint Ventures in North Korea* (Washington, DC: U.S.-Korea Institute at the School for Advanced International Studies, February 2011), p. 4.
34. Drew Thompson, *Silent Partners: Chinese Joint Ventures in North Korea* (Washington, DC: U.S.-Korea Institute at the School for Advanced International Studies, February 2011), p. 4. Unfortunately, the report does not specify which companies, in particular.
35. Open Source Center, "OSC Report: China—Directory of PRC Enterprises in North Korea," April 19, 2011. OSC ID: KPP20110419032002. <http://www.opensource.gov>.

36. Ministry of Commerce, People's Republic of China, "2010 Niandu Zhongguo Duiwai Zhijie Touzi Tongji Gongbao" (Statistical Bulletin on China's Outward Direct Investment, 2010) (Beijing, China: 2011), p. 82.

37. *Huanqiu Shibao* (China), "Wai Jiaobu: Chaoxian Kaifang Liangdao Zuo Ziyou Maoyiqu Bu Weifan Lianheguo Guoding," (Foreign Ministry: North Korea's Opening of Two Islands for Special Economic Zone Don't Violate U.N. Stipulations), February 25, 2010. <http://china.huanqiu.com/roll/2010-02/726837.html>.

38. Park Jun Hyeong, "New Bridge Rising from the Yalu," *Daily NK* (South Korea), August 30, 2011. <http://www.dailynk.com/english/read.php?cataId=nk00100&num=8115>.

39. Jay Solomon and Jeremy Page, "Chinese Firm to Invest in North Korea," *Wall Street Journal*, January 19, 2011. <http://online.wsj.com/article/SB10001424052748704678004576090270026745368.html>.

40. Dick K. Nanto and Mark E. Manyin, "China-North Korea Relations" (Washington, DC: Congressional Research Service, December 28, 2010), p. 17.

41. Dick Nanto and Emma Chanlett-Avery, "North Korea: Economic Leverage and Policy Analysis" (Washington, DC: Congressional Research Service, January 22, 2010), p. 34; and Bates Gill, "China's North Korea Policy: Assessing Interests and Influences" (Washington, DC: United States Institute of Peace, July 2011), p. 5.

42. United Nations, "Report to the Security Council from the Panel of Experts established Pursuant to Resolution 1874 (2009)" (New York, NY: 2010), p. 36. <http://www.fas.org/irp/eprint/scr1874.pdf>.

43. Mary Beth Nikitin et al., "Implementation of U.N. Security Council Resolution 1874" (Washington, DC: Congressional Research Service, October 8, 2010), p. 4.

44. Mary Beth Nikitin et al., "Implementation of U.N. Security Council Resolution 1874" (Washington, DC: Congressional Research Service, October 8, 2010), p. 4; International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea" *Asia Report* 200 (Brussels, Belgium: January 21, 2011): 12; and Tania Branigan, "China denies role in North Korea-Iran missile trade," *Guardian* (United Kingdom), May 18, 2011. <http://www.guardian.co.uk/world/2011/may/18/china-denies-role-north-korea-iran-missile-trade>.

45. Dick K. Nanto and Mark E. Manyin, "China-North Korea Relations" (Washington, DC: Congressional Research Service, December 28, 2010), pp. 18–19.

46. United Nations Security Council, *Resolution 1718* (New York, NY: United Nations, October 14, 2006).

47. United Nations Security Council, *Resolution 1874* (New York, NY: United Nations, June 12, 2009).

48. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of David Helvey, April 13, 2011.

49. Bloomberg News, "China Sends General Guo to Mark North Korea's 'Historical Great Victory,'" October 25, 2010. <http://www.bloomberg.com/news/2010-10-25/china-sends-general-guo-to-mark-north-korea-s-historical-great-victory.html>.

50. Shirley A. Kan, "China and Proliferation of Weapons of Mass Destruction and Missiles: Policy Issues" (Washington, DC: Congressional Research Service, May 26, 2011), p. 26.

51. Stephen Olson and Clyde Prestowitz, *The Evolving Role of China in International Institutions* (Washington, DC: The Economic Strategy Institute, January 2011), p. 73. <http://www.uscc.gov/researchpapers/2011/TheEvolvingRoleofChinainInternationalInstitutions.pdf>. See also Dick K. Nanto and Mark E. Manyin, "China-North Korea Relations" (Washington, DC: Congressional Research Service, December 28, 2010), p. 4.

52. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Victor Cha, April 13, 2011.

53. International Crisis Group, "China and North Korea: Comrades Forever?" *Asia Report* 112 (Brussels, Belgium: February 1, 2006): 10.

54. International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea," *Asia Report* 200 (Brussels, Belgium: January 21, 2011): 8.

55. Bruce W. Bennett, cited in Robert D. Kaplan and Abraham M. Denmark, "The Long Goodbye: The Future of North Korea," *World Affairs Journal* (May-June, 2011). <http://www.worldaffairsjournal.org/articles/2011-MayJun/full-Kaplan-Denmark-MJ-2011.html>; Minxin Pei, "Get Ready for DPRK [Democratic People's Republic of Korea] Collapse," *Diplomat* (Tokyo, Japan), May 12, 2010. <http://the-diplomat.com/2010/05/12/get-ready-for-dprk-collapse/2/>; and John Pomfret, "Why China Won't Do More with North Korea," *WashingtonPost*, May 27, 2009. [http://newsweek.washingtonpost.com/postglobal/pomfretschina/2009/05/can\\_china\\_really\\_do\\_more\\_with.html](http://newsweek.washingtonpost.com/postglobal/pomfretschina/2009/05/can_china_really_do_more_with.html).

56. International Crisis Group, "China and North Korea: Comrades Forever?" *Asia Report* 112 (Brussels, Belgium: February 1, 2006): 11.
57. Patrick Chovanec, "The Nine Nations of China," *Atlantic* (November 2009). <http://www.theatlantic.com/magazine/archive/2009/11/the-nine-nations-of-china/7769/>; and Bruce W. Bennett, "Uncertainties in the North Korean Nuclear Threat," *Documented Briefing* (Arlington, VA: RAND Corporation, 2010): vii.
58. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Victor Cha, April 13, 2011.
59. Selig S. Harrison, "China's North Korean Calculations," *New York Times*, January 6, 2011. <http://www.nytimes.com/2011/01/07/opinion/07iht-edharrison07.html>.
60. Dick K. Nanto and Mark E. Manyin, "China-North Korea Relations" (Washington, DC: Congressional Research Service, December 28, 2010), p. 6; and International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea" *Asia Report* 200 (Brussels, Belgium: January 21, 2011): i.
61. Chen Jian, *China's Road to the Korean War* (New York, NY: Columbia University Press, 1994), pp. 158–160; and Richard W. Stewart, "The Korean War: The Chinese Intervention, 3 November 1950–24 January 1951" (Washington, DC: Department of the Army, *Center for Military History Publication* 19–8, 2000). <http://www.history.army.mil/brochures/kw-chinter/chinter.htm>.
62. International Crisis Group, "China and Inter-Korean Clashes in the Yellow Sea," *Asia Report* 200 (Brussels, Belgium: January 21, 2011): 12.
63. International Trade Centre, "Trade Map" (Geneva, Switzerland: September 29, 2011). [http://www.trademap.org/light/Bilateral\\_TS.aspx](http://www.trademap.org/light/Bilateral_TS.aspx).
64. International Crisis Group, "China and North Korea: Comrades Forever?" *Asia Report* 112 (Brussels, Belgium: February 1, 2006): i; and Drew Thompson, *Silent Partners: Chinese Joint Ventures in North Korea* (Washington, DC: U.S.-Korea Institute at the School for Advanced International Studies, February 2011), p. 4.
65. Selig S. Harrison, "China's North Korean Calculations," *New York Times*, January 6, 2011. <http://www.nytimes.com/2011/01/07/opinion/07iht-edharrison07.html>.
66. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Victor Cha, April 13, 2011.
67. For more details on the violations and list of possible sanctions, see *The Iran and Libya Sanctions Act*, Public Law 104–172, 104th Cong., 2nd sess. (August 5, 1996); *The Iran Nonproliferation Act*, Public Law 106–178, 106th Cong., 2nd sess. (March 14, 2000); *The Iran Nonproliferation Amendments Act of 2005*, Public Law 109–112, 109th Cong., 1st sess. (November 22, 2005); *The North Korea Nonproliferation Act*, Public Law 109–353, 109th Cong., 2nd sess. (October 13, 2006); *The Iran Freedom Support Act*, Public Law 109–293, 109th Cong., 2nd sess. (September 30, 2006); and *The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010*, Public Law 111–195, 111th Cong., 2nd sess. (July 1, 2010).
68. Xinhua, "Waijiaobu: Zhongfang Jianjue Fandui Meiguo Zhicai Zhongguo Gongci" (Foreign Ministry: China Firmly Opposes U.S. Sanctions Against Chinese Companies), December 29, 2005. [http://news.xinhuanet.com/world/2005-12/29/content\\_3982636.htm](http://news.xinhuanet.com/world/2005-12/29/content_3982636.htm). USCC staff translation.
69. Ministry of Foreign Affairs of the People's Republic of China, "2010 Nian 7 Yue 6 Ri Waijiaobu Fayananren Qin Gang Juxing Lixing Jizhehui" (Ministry of Foreign Affairs Spokesperson Qin Gang Holds a Regular Press Conference, July 6, 2010), July 6, 2010. <http://www.mfa.gov.cn/chn/gxh/tyb/fyrbt/jzhsl/t714332.htm>. USCC Staff translation.
70. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of John W. Garver, April 13, 2011.
71. U.S. Government Accountability Office, "Firms Reported in Open Sources as Having Commercial Activity in Iran's Oil, Gas, and Petrochemical Sectors" (Washington, DC: August 3, 2011), p. 3.
72. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of John W. Garver, April 13, 2011.
73. Christian Oliver, "US tells China not to exploit sanctions on Iran," *Financial Times*, August 2, 2010. <http://www.ft.com/cms/s/0/0253d046-9e28-11df-b377-00144feab49a.html>.
74. The companies listed as pulling out of projects there included Royal Dutch Shell, Repsol, OMV, and Total. Christian Oliver, "US tells China not to exploit sanc-

tions on Iran,” *Financial Times*, August 2, 2010. <http://www.ft.com/cms/s/0/0253d046-9e28-11df-b377-00144feab49a.html>.

75. U.S.-China Economic and Security Review Commission, *Hearing on China’s Foreign Policy: Challenges and Players*, written testimony of David A. Helvey, April 13, 2011.

76. U.S.-China Economic and Security Review Commission, *Hearing on China’s Foreign Policy: Challenges and Players*, written testimony of Erica S. Downs, April 13, 2011.

77. Chen Aizhu and Chris Buckley, “Exclusive: China curbs Iran energy work,” Reuters, September 2, 2011. <http://www.huffingtonpost.com/2011/09/02/exclusive-china-curbs-iran-946099.html?view=screen>.

78. Chen Aizhu, “Sinopec Starts up Refining Unit in Iran’s Arak Plant,” Reuters, August 19, 2011. <http://www.iranenergyproject.org/3708/sinopec-starts-up-refining-unit-in-iran-arak-plant>.

79. United Press International Energy, “Sinopec Signs MOU [Memorandum of Understanding] for Iran’s Oil Sector,” November 25, 2009. [http://www.upi.com/Business\\_News/Energy-Resources/2009/11/25/Sinopec-signs-MOU-for-Irans-oil-sector/UPI-26891259164301/](http://www.upi.com/Business_News/Energy-Resources/2009/11/25/Sinopec-signs-MOU-for-Irans-oil-sector/UPI-26891259164301/).

80. Platts (McGraw-Hill), “China to speed up work on delayed Iranian gas project: report,” September 28, 2011. <http://www.platts.com/RSSFeedDetailedNews/RSSFeed/NaturalGas/8393825>.

81. U.S. Government Accountability Office, “Firms Reported in Open Sources as Having Commercial Activity in Iran’s Oil, Gas, and Petrochemical Sectors” (Washington, DC: August 3, 2011), pp. 5–6.

82. Erica S. Downs and Suzanna Maloney, “Getting China to Sanction Iran: The Chinese-Iranian Oil Connection,” *Foreign Affairs* (April 2011).

83. Shirley A. Kan, “China and Proliferation of Weapons of Mass Destruction and Missiles: Policy Issues” (Washington, DC: Congressional Research Service, March 3, 2011), p. 14.

84. U.S.-China Economic and Security Review Commission, *Hearing on China’s Foreign Policy: Challenges and Players*, written testimony of John W. Garver, April 13, 2011; and Laurent Maillard, “China Takes Over From West as Iran’s Main Economic Partner,” *Agence France-Presse*, March 15, 2010. <http://www.google.com/hostednews/afp/article/ALeqM5h1elRZcX3uwz8Zc7Ez7SFDR6X4cg>.

85. U.S. Government Accountability Office, “Exporters of Refined Petroleum Products to Iran” (Washington DC: September 3, 2010), p. 4; and Stratfor, “China Boosts Gas Sales to Iran, Irks US,” *Forbes*, April 16, 2010. <http://www.forbes.com/sites/energysource/2010/04/16/china-boosting-gas-sales-to-iran/>.

86. Shirley A. Kan, “China and Proliferation of Weapons of Mass Destruction and Missiles: Policy Issues” (Washington, DC: Congressional Research Service, March 3, 2011), p. 14.

87. U.S.-China Economic and Security Review Commission, *Hearing on China’s Foreign Policy: Challenges and Players*, written testimony of John W. Garver, April 13, 2011.

88. U.S.-China Economic and Security Review Commission, *Hearing on China’s Foreign Policy: Challenges and Players*, testimony of Daniel Kritenbrink, April 13, 2011.

89. See, for example, *The Iran Nonproliferation Act*, Public Law 106–178, 106th Cong., 2nd sess. (March 14, 2000); *The Iran Nonproliferation Amendments Act of 2005*, Public Law 109–112, 109th Cong., 1st sess. (November 22, 2005); *The North Korea Nonproliferation Act*, Public Law 109–353, 109th Cong., 2nd sess. (October 13, 2006); *The Iran Freedom Support Act*, Public Law 109–293, 109th Cong., 2nd sess. (September 30, 2006); and *The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010*, Public Law 111–195, 111th Cong., 2nd sess. (July 1, 2010).

90. Stockholm International Peace Research Institute, “Arms Transfer Database” (Stockholm, Sweden: September 6, 2011). <http://www.sipri.org/databases/armstransfers>.

91. U.S.-China Economic and Security Review Commission, *Hearing on China’s Foreign Policy: Challenges and Players*, written testimony of John W. Garver, April 13, 2011.

92. United Press International, “China opens missile plant in Iran,” April 23, 2010. [http://www.upi.com/Business\\_News/Security-Industry/2010/04/23/China-opens-missile-plant-in-Iran/UPI-82791272037022/](http://www.upi.com/Business_News/Security-Industry/2010/04/23/China-opens-missile-plant-in-Iran/UPI-82791272037022/).

93. Official at the U.S. Department of State, e-mail exchange with Commission staff, October 31, 2011.

94. Jon B. Alterman and John W. Garver, *The Vital Triangle: China, The United States, and the Middle East* (Washington, D.C.: Center for Strategic and International Studies, 2008).



95. The companies in question were Roc-Master manufacturer and Supply Company and Zhejiang Ouhai Trade Corporation. Shirley A. Kan, "China and Proliferation of Weapons of Mass Destruction and Missiles: Policy Issues" (Washington, DC: Congressional Research Service, March 3, 2011), p. 12.

96. Colum Lynch, "Chinese Firm Indicted in Sales to Iran," *Washington Post*, April 9, 2009. <http://www.washingtonpost.com/wp-dyn/content/article/2009/04/07/AR2009040704010.html?hpid=sec-world>; see also Bill Gertz, "Inside the Ring: China Missile Sales," *Washington Times*, July 13, 2011. <http://www.washingtontimes.com/news/2011/jul/13/inside-the-ring-482504507/>.

97. David Morgan, "US: China entities not complying with Iran sanctions," Reuters, January 19, 2011. <http://www.reuters.com/article/2011/01/19/usa-china-iran-idUSNN1921059820110119>.

98. The report did not name China specifically, but unidentified UN officials involved in the report's production stated that it was indeed China. Tania Branigan, "China denies role in North Korea-Iran missile trade," *Guardian* (United Kingdom), May 18, 2011. <http://www.guardian.co.uk/world/2011/may/18/china-denies-role-north-korea-iran-missile-trade>. See also Louis Charbonneau, "North Korea, Iran trade missile technology: U.N.," Reuters, May 14, 2011. <http://www.reuters.com/article/2011/05/14/us-korea-north-iran-un-idUSTRE74D18Z20110514>.

99. Office of the Spokesperson, "Fact Sheet: Iran, North Korea and Syria Non-proliferation Act" (Washington, DC: U.S. Department of State, May 24, 2011). <http://www.state.gov/r/pa/prs/ps/2011/05/164129.htm>.

100. Andrew F. Krepinevich, "Why AirSea Battle?" (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), p. 27.

101. Joshua R. Itzkowitz Shiffrin and Miranda Priebe, "A Crude Threat: The Limits of an Iranian Missile Campaign against Saudi Arabian Oil," *International Security* 36: 1 (Cambridge, MA: Summer 2011): 199.

102. Joshua R. Itzkowitz Shiffrin and Miranda Priebe, "A Crude Threat: The Limits of an Iranian Missile Campaign against Saudi Arabian Oil," *International Security* 36: 1 (Cambridge, MA: Summer 2011): 199.

103. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 4. <http://books.sipri.org/files/PP/SIPRIPP26.pdf>.

104. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Susan Lawrence, April 13, 2011.

105. Stephen Olson and Clyde Prestowitz, *The Evolving Role of China in International Institutions* (Washington, DC: The Economic Strategy Institute, January 2011), pp. 86–87. This report was sponsored by the U.S.-China Economic and Security Review Commission. <http://www.uscc.gov/researchpapers/2011/TheEvolvingRoleofChinainInternationalInstitutions.pdf>.

106. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Susan Lawrence, April 13, 2011.

107. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Susan Lawrence, April 13, 2011.

108. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 7. <http://books.sipri.org/files/PP/SIPRIPP26.pdf>.

109. China Vitae, "Dai Bingguo." [http://www.chinavitae.com/biography/Dai\\_Bingguo/full](http://www.chinavitae.com/biography/Dai_Bingguo/full).

110. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), pp. 8–10. <http://books.sipri.org/files/PP/SIPRIPP26.pdf>.

111. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Daniel Kritenbrink, April 13, 2011.

112. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Susan Lawrence, April 13, 2011; U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Alan Wachman, April 13, 2011; and U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of David M. Lampton, March 10, 2011.

113. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of David M. Lampton, March 10, 2011.

114. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Erica Downs, April 13, 2011; U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Susan Lawrence, April 13, 2011; U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Yu-Wen Julie Chen, April 13, 2011; and Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 8. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

115. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Susan Lawrence, April 13, 2011.

116. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Susan Lawrence, April 13, 2011; Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 8. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

117. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of David Helvey, April 13, 2011.

118. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 12. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

119. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Yu-Wen Julie Chen, April 13, 2011.

120. See also David Shambaugh, "Coping with a Conflicted China," *Washington Quarterly* 34:1 (Winter 2011): 7–27.

121. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Yu-Wen Julie Chen, April 13, 2011; Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 12. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

122. Andrew Scobell, "Is There a Civil-Military Gap in China's Peaceful Rise?" *Parameters* 39:2 (Summer 2009): 4–22; U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of Andrew Scobell, March 10, 2011.

123. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Yu-Wen Julie Chen, April 13, 2011; U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of Andrew Scobell, March 10, 2011.

124. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of Andrew Scobell, March 10, 2011.

125. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Alan Wachman, April 13, 2011.

126. Chen Zhimin and Jian Junbo, *Chinese Provinces as Foreign Policy Actors in Africa* (Cape Town, South Africa: South African Institute of International Affairs, January 2009), pp. 6–7. [http://www.saiia.org.za/images/stories/pubs/occasional\\_papers/saia\\_sop\\_22\\_zhimin\\_and\\_junbo\\_20090218\\_en.pdf](http://www.saiia.org.za/images/stories/pubs/occasional_papers/saia_sop_22_zhimin_and_junbo_20090218_en.pdf).

127. Carla Freeman and Drew Thompson, *China on the Edge: China's Border Provinces and Chinese Security Policy* (Washington, DC: The Center for the National Interest and The Johns Hopkins School for Advanced International Studies, April 2011), p. 26, 73. [http://www.cftni.org/China\\_on\\_the\\_Edge\\_April\\_2011.pdf](http://www.cftni.org/China_on_the_Edge_April_2011.pdf).

128. Chen Zhimin and Jian Junbo, *Chinese Provinces as Foreign Policy Actors in Africa* (Cape Town, South Africa: South African Institute of International Affairs, January 2009), p. 5. [http://www.saiia.org.za/images/stories/pubs/occasional\\_papers/saia\\_sop\\_22\\_zhimin\\_and\\_junbo\\_20090218\\_en.pdf](http://www.saiia.org.za/images/stories/pubs/occasional_papers/saia_sop_22_zhimin_and_junbo_20090218_en.pdf).

129. Chen Zhimin, "Coastal Provinces and China's Foreign Policy-making," in Yifan Hao and Lin Su, eds., *China's Foreign Policy Making: Societal Force and Chinese American Policy* (Aldershot, UK: Ashgate Publishing Limited, 2005), p.5. [http://www.saiia.org.za/images/stories/pubs/occasional\\_papers/saia\\_sop\\_22\\_zhimin\\_and\\_junbo\\_20090218\\_en.pdf](http://www.saiia.org.za/images/stories/pubs/occasional_papers/saia_sop_22_zhimin_and_junbo_20090218_en.pdf).

130. Carla Freeman and Drew Thompson, *China on the Edge: China's Border Provinces and Chinese Security Policy* (Washington, DC: The Center for the National Interest and The Johns Hopkins School for Advanced International Studies, April 2011), pp. 33–39. [http://www.cftni.org/China\\_on\\_the\\_Edge\\_April\\_2011.pdf](http://www.cftni.org/China_on_the_Edge_April_2011.pdf).



131. Carla Freeman and Drew Thompson, *China on the Edge: China's Border Provinces and Chinese Security Policy* (Washington, DC: The Center for the National Interest and The Johns Hopkins School for Advanced International Studies, April 2011), p. 79. [http://www.cftni.org/China\\_on\\_the\\_Edge\\_April\\_2011.pdf](http://www.cftni.org/China_on_the_Edge_April_2011.pdf).

132. British Consulate General Chongqing, *China's Southwest Frontier: Understanding China's Bridgehead Strategy* (Chongqing, China: June 2011).

133. Carla Freeman and Drew Thompson, *China on the Edge: China's Border Provinces and Chinese Security Policy* (Washington, DC: The Center for the National Interest and The Johns Hopkins School for Advanced International Studies, April 2011), p. 42. [http://www.cftni.org/China\\_on\\_the\\_Edge\\_April\\_2011.pdf](http://www.cftni.org/China_on_the_Edge_April_2011.pdf).

134. *Express Tribune (Pakistan)*, "Pakistan committed to uprooting terror: Zadari," August 30, 2011. <http://tribune.com.pk/story/243150/pakistan-committed-to-uprooting-terror-zadari>; *China Daily*, "Xinjiang Production and Construction Corps," September 29, 2011. <http://www.chinadaily.com.cn/regional/xinjiang.html>; and Xinhua, "Role of Xinjiang Production, Construction Corps important: white paper," May 26, 2003. [http://news.xinhuanet.com/english/2003-05/26/content\\_887338.htm](http://news.xinhuanet.com/english/2003-05/26/content_887338.htm).

135. U.S. China and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impact*, written testimony of Stacy A. Pedrozo, January 27, 2011.

136. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), pp. 24–31. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

137. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Erica Downs, April 13, 2011; Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 25. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

138. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 26. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

139. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 25. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

140. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Erica Downs, April 13, 2011; Cheng Li, *China's Midterm Jockeying: Gearing Up for 2012 (Part 4: Top Leaders of Major State-Owned Enterprises)* (Stanford, CA: *China Leadership Monitor* 43 (February 2011)): 1–3. [http://www.brookings.edu/~media/Files/rc/papers/2011/02\\_china\\_leadership\\_li/02\\_china\\_leadership\\_li.pdf](http://www.brookings.edu/~media/Files/rc/papers/2011/02_china_leadership_li/02_china_leadership_li.pdf).

141. Leslie Hook, "Sinopec chief tipped for political post," *Financial Times*, March 22, 2011. <http://www.ft.com/intl/cms/s/0/29e13b50-5465-11e0-979a-00144feab49a.html>.

142. Leslie Hook, "Sinopec chief tipped for political post," *Financial Times*, March 22, 2011. <http://www.ft.com/intl/cms/s/0/29e13b50-5465-11e0-979a-00144feab49a.html>; Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 26. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

143. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Erica Downs, April 13, 2011.

144. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Yu-Wen Julie Chen, April 13, 2011.

145. Bao Chang, "SASAC [State-owned Assets Supervision and Administration Commission] urges greater safety for workers," *China Daily*, February 26, 2011. [http://www.chinadaily.com.cn/bizchina/2011-02/26/content\\_12082212.htm](http://www.chinadaily.com.cn/bizchina/2011-02/26/content_12082212.htm);

Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 25. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

146. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Erica Downs, April 13, 2011.

147. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Erica Downs, April 13, 2011.

148. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), pp. 26–29. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

149. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Erica Downs, April 13, 2011; Erica Downs, "Business Interest Groups in Chinese Politics: The Case of the Oil Companies," in Cheng Li, *China's Changing Political Landscape: Prospects for Democracy* (Washington, DC: Brookings Institution Press, 2008). [http://www.brookings.edu/media/Files/rc/papers/2010/07\\_china\\_oil\\_companies\\_downs/07\\_china\\_oil\\_companies\\_downs.pdf](http://www.brookings.edu/media/Files/rc/papers/2010/07_china_oil_companies_downs/07_china_oil_companies_downs.pdf).

150. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), pp. 29–30. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

151. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Erica Downs, April 13, 2011.

152. Erica Downs, "Inside China Inc: China Development Bank's Cross-Border Energy Deals" (Washington, DC: The John L. Thornton China Center at The Brookings Institution, March 2011), p. 6. [http://www.brookings.edu/~media/Files/rc/papers/2011/0321\\_china\\_energy\\_downs/0321\\_china\\_energy\\_downs.pdf](http://www.brookings.edu/~media/Files/rc/papers/2011/0321_china_energy_downs/0321_china_energy_downs.pdf).

153. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 28. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

154. Erica Downs, "Inside China Inc: China Development Bank's Cross-Border Energy Deals" (Washington, DC: The John L. Thornton China Center at The Brookings Institution, March 2011), p. 58. [http://www.brookings.edu/~media/Files/rc/papers/2011/0321\\_china\\_energy\\_downs/0321\\_china\\_energy\\_downs.pdf](http://www.brookings.edu/~media/Files/rc/papers/2011/0321_china_energy_downs/0321_china_energy_downs.pdf).

155. Erica Downs, "Inside China Inc: China Development Bank's Cross-Border Energy Deals" (Washington, DC: The John L. Thornton China Center at The Brookings Institution, March 2011), pp. 79–86. [http://www.brookings.edu/~media/Files/rc/papers/2011/0321\\_china\\_energy\\_downs/0321\\_china\\_energy\\_downs.pdf](http://www.brookings.edu/~media/Files/rc/papers/2011/0321_china_energy_downs/0321_china_energy_downs.pdf).

156. Erica Downs, "Inside China Inc: China Development Bank's Cross-Border Energy Deals" (Washington, DC: The John L. Thornton China Center at The Brookings Institution, March 2011), pp. 80–82. [http://www.brookings.edu/~media/Files/rc/papers/2011/0321\\_china\\_energy\\_downs/0321\\_china\\_energy\\_downs.pdf](http://www.brookings.edu/~media/Files/rc/papers/2011/0321_china_energy_downs/0321_china_energy_downs.pdf).

157. Thomas Bondiguel and Thierry Kellner, "The Impact of China's Foreign Policy Think Tanks," *Brussels Institute of Contemporary China Studies (BICCS) Asia Paper* 5:5 (2010): 14. <http://www.vub.ac.be/biccs/site/assets/files/apapers/Asia%20papers/20100405%20-%20Bondiguel%20Kellner.pdf>.

158. Thomas Bondiguel and Thierry Kellner, "The Impact of China's Foreign Policy Think Tanks," *Brussels Institute of Contemporary China Studies (BICCS) Asia Paper* 5:5 (2010): 19–24. <http://www.vub.ac.be/biccs/site/assets/files/apapers/Asia%20papers/20100405%20-%20Bondiguel%20Kellner.pdf>; Thomas G. Moore and Dixia Yang, "Empowered and Restrained: Chinese Foreign Policy in the Age of Economic Interdependence," in David M. Lampton, *The Making of Chinese Foreign and Security Policy in the Age of Reform* (Stanford, CA: Stanford University Press, 2001), pp. 207–208; and Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), pp. 35–40. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

159. Thomas G. Moore and Dixia Yang, "Empowered and Restrained: Chinese Foreign Policy in the Age of Economic Interdependence," in David M. Lampton, *The Making of Chinese Foreign and Security Policy in the Age of Reform* (Stanford, CA: Stanford University Press, 2001), pp. 207–208.

160. Liu Xiao, "China Can Make Arrangements for the Future by Sending Troops to Afghanistan," *Huanqiu Shibao (Global Times)*, December 8, 2009. OSC ID: CPP20091217710003. <http://www.opensource.gov>; Li Daguang, "Sending Troops to Afghanistan Will Cause Trouble for China," *Huanqiu Shibao (Global Times)*, December 8, 2009. OSC ID: CPP20091217710004. <http://www.opensource.gov>.

161. Thomas Bondiguel and Thierry Kellner, "The Impact of China's Foreign Policy Think Tanks," *Brussels Institute of Contemporary China Studies (BICCS) Asia Paper* 5:5 (2010): 14. <http://www.vub.ac.be/biccs/site/assets/files/apapers/Asia%20papers/20100405%20-%20Bondiguel%20Kellner.pdf>.

162. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute (SIPRI), Policy Paper 26, September 2010), p. 38. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

163. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Susan Lawrence, April 13, 2011.

164. Xinhua, "China Internet users exceed 500 million," September 29, 2011. [http://www.chinadaily.com.cn/china/2011-09/29/content\\_13821641.htm](http://www.chinadaily.com.cn/china/2011-09/29/content_13821641.htm).

165. U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2010), p. 222.
166. David Shambaugh, "Coping with a Conflicted China," *Washington Quarterly* 34:1 (Winter 2011): 21–22.
167. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Yu-Wen Julie Chen, April 13, 2011.
168. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Erica Downs, April 13, 2011.
169. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Yu-Wen Julie Chen, April 13, 2011.
170. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, testimony of Susan Lawrence, April 13, 2011.
171. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Erica Downs, April 13, 2011.
172. U.S.-China Economic and Security Review Commission, *Hearing on China's Active Defense Strategy and its Regional Impacts*, written testimony of Stacy A. Pedrozo, January 27, 2011.
173. *People's Daily Online*, "China to strengthen maritime forces amid disputes," June 17, 2011. <http://english.people.com.cn/90001/90776/90883/7412388.html>.
174. Michael Wines, "Secret Bid to Arm Qaddafi Sheds Light on Tensions in China Government," September 11, 2011. <http://www.nytimes.com/2011/09/12/world/asia/12china.html?pagewanted=all>.
175. U.S.-China Economic and Security Review Commission, *Hearing on China's Foreign Policy: Challenges and Players*, written testimony of Yu-Wen Julie Chen, April 13, 2011.
176. David Shambaugh, "Coping with a Conflicted China," *Washington Quarterly* 34:1 (Winter 2011): 21.
177. Taiwan Department of Health, "Background Material on the 'Cross-Strait Agreement on Medical and Health Cooperation,'" (Taipei, Taiwan: December 15, 2010.) <http://www.mac.gov.tw/ct.asp?xItem=91465&ctNode=6256&mp=3>.
178. Associated Press, "Chinese envoy arrives in Taiwan for talks," December 20, 2010. <http://www.washingtontimes.com/news/2010/dec/20/chinese-envoy-arrives-in-taiwan-for-talks/>.
179. *China Post (Taiwan)*, "Cross-strait nuclear safety system to be built: MOEA [Minister of Economic Affairs]," March 18, 2011. <http://www.chinapost.com.tw/taiwan/china-taiwan-relations/011/03/18/295081/Cross-strait-nuclear.htm>.
180. Agence France-Presse, "Taipei, Beijing sign Nuclear Safety Pact," October 12, 2011. [http://focustaiwan.tw/ShowNews/WebNews\\_Detail.aspx?Type=aIPL&ID=201107220007](http://focustaiwan.tw/ShowNews/WebNews_Detail.aspx?Type=aIPL&ID=201107220007); and Lin Shu-yuan and Sofia Wu, "Three Core Issues Stall Investment Pact Talks with China: Minister," Central News Agency (Taiwan), September 29, 2011.05[http://www.taiwannews.com.tw/etn/news\\_content.php?id=1720995](http://www.taiwannews.com.tw/etn/news_content.php?id=1720995).
181. Andrew Jacobs, "As Chinese Visit Taiwan, the Cultural Influence Is Subdued," *New York Times*, August 10, 2011. <http://www.nytimes.com/2011/08/11/world/asia/11taiwan.html>; Xinhua, "Taiwan gears up as mainland tourists arrive," June 28, 2011. [http://www.chinadaily.com.cn/china/2011-06/28/content\\_12795004.htm](http://www.chinadaily.com.cn/china/2011-06/28/content_12795004.htm); and Taiwan Mainland Affairs Council, "Significance of the Policy to Allow Independent Travel to Taiwan by Mainland Tourists," August 18, 2011. <http://www.mac.gov.tw/ct.asp?xItem=97085&ctNode=6337&mp=3>.
182. Agence France-Presse, "China to allow individual travel to Taiwan," June 12, 2011. [http://www.google.com/hostednews/afp/article/ALeqM5ijyF6jjuLEZvIFBm7\\_wZQegagrcw?docId=CNG.cd4577a43425ef99e756265e3cb55023.901](http://www.google.com/hostednews/afp/article/ALeqM5ijyF6jjuLEZvIFBm7_wZQegagrcw?docId=CNG.cd4577a43425ef99e756265e3cb55023.901).
183. Ma Ying-jeou (president of Taiwan), meeting with Commissioners, August 17, 2011, Taipei, Taiwan.
184. Tourism Bureau, "Outbound Departures of Nationals of the Republic of China by Destination, 2005–2010" (Taipei, Taiwan: Ministry of Transportation and Communications). [http://admin.taiwan.net.tw/statistics/File/201012/table25\\_2010.pdf](http://admin.taiwan.net.tw/statistics/File/201012/table25_2010.pdf); Tourism Bureau, "Visitor Arrivals by Residence, 2010" (Taipei, Taiwan: Ministry of

Transportation and Communications). [http://admin.taiwan.net.tw/statistics/File/201012/table02\\_010.pdf](http://admin.taiwan.net.tw/statistics/File/201012/table02_010.pdf).

185. Cindy Sui, "Taiwan universities accept Chinese mainland students," BBC, April 14, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-13076233>. Taiwan students studying on the mainland are not subject to similar stipulations. Xinhua, "Official urges Taiwan to treat mainland students equally," January 12, 2011. [http://chinadaily.com.cn/china/2011-01/12/content\\_11839241.htm](http://chinadaily.com.cn/china/2011-01/12/content_11839241.htm).

186. Members of Taiwan's National Security Council, meeting with Commissioners, Taipei, Taiwan, August 17, 2011.

187. U.S.-Taiwan Business Council, *Defense and Security Report Annual Review 2010* (Arlington, VA: January 2011), p. 10; and Philip Liu, "Talk on Cross-Strait Investment Protection Agreement Runs Aground," CENS (Taiwan), December 7, 2010. [http://cens.com/cens/html/en/news/news\\_inner\\_34545.html](http://cens.com/cens/html/en/news/news_inner_34545.html).

188. U.S.-China Economic and Security Review Commission, luncheon with Taipei Economic and Cultural Representative Office, Washington, DC, June 14, 2011.

189. Lin Shu-yuan and S.C. Chang, "Cross-strait investment protection pact stuck on two issues," China News Agency (Taiwan), August 7, 2011. [http://focustaiwan.tw/ShowNews/WebNews\\_Detail.aspx?Type=aECO&ID=201108070021](http://focustaiwan.tw/ShowNews/WebNews_Detail.aspx?Type=aECO&ID=201108070021); and China Post (Taiwan), "Taipei, Beijing seek consensus on investment protection pact," July 4, 2011. <http://www.chinapost.com.tw/taiwan/china-taiwan-relations/2011/07/04/308499/Taipei-Beijing.htm>.

190. Jenny W. Hsu and Fanny Liu, "Taiwan Finance Minister: 'Largely' Agreed With China On Double Tax Avoidance," Dow Jones Newswires, June 29, 2011. <http://www.nasdaq.com/aspx/stock-market-news-story.aspx?storyid=201106290646dowjonesdjonline000265&title=taiwan-finance-ministerlargelyagreed-with-china-on-double-tax-avoidance>.

191. China Post (Taiwan), "NT\$-Yuan Pact Soon," December 2, 2011. [http://www.chinapost.com.tw/taiwan/national/national-news/2009/T312/02/234921/NT\\$-YUAN-PACT.htm](http://www.chinapost.com.tw/taiwan/national/national-news/2009/T312/02/234921/NT$-YUAN-PACT.htm).

192. China Times, "Cross-Strait banking regulators fail to reach accord," April 26, 2011. <http://www.wantchinatimes.com/news-subclass-cnt.aspx?cid=1102&MainCatID=&id=20110426000055>.

193. Ko Shu-ling, "Officials propose Taiwan, China cultural exchanges," Taipei Times, September 7, 2010. <http://www.taipetimes.com/News/front/archives/2010/09/07/2003482290/1>.

194. David Brown, "China-Taiwan Relations: Steady As She Goes," *Comparative Connections* (Washington, DC: Center for Strategic and International Studies, May 2011), p. 2.

195. Liu Jung, Wang Yu-chung, and Shih Hsiao-kuang, "Ma Wants Fewer Visits by PRC [People's Republic of China] officials," Taipei Times, July 9, 2011. <http://www.taipetimes.com/News/front/archives/2011/07/09/2003507767>.

196. Carnegie Endowment for International Peace, *Challenges to Cross-Strait Relations in 2012*, statement by Arthur S. Ding, July 7, 2011.

197. Wu Ming-jie, "Close elections in Taiwan cause concern in Beijing," China News Agency (Taiwan), September 5, 2011. [http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=201109050000\\_67&cid=1501](http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=201109050000_67&cid=1501).

198. Richard C. Bush III, "Taiwan and East Asian Security," *Orbis* 2:55 (Spring 2011): 275.

199. Bonnie Glaser, "U.S.-China-Taiwan Relations in the Run-up to 2012 Elections in Taiwan and the U.S. and Leadership Transition in China," *Facing the Challenges of Cross-Strait Relations in 2012* (Washington, DC: Carnegie Endowment for International Peace, July 7, 2011), p. 4.

200. Washington-based specialist on cross-Strait relations, e-mail exchange with Commission staff, September 22, 2011. Name withheld at the request of the individual.

201. Agence France-Presse, "Taiwan protests 'province of China' WHO [World Health Organization] label," May 16, 2011. <http://www.google.com/hostednews/afp/article/ALeqM5gDMie64TBpLIE4KRQn8k4z8sc1Cg?docId=CNG.0e7ec9d4e09bee530653022ee578dcc1.621>.

202. Nancy Liu, "Brazil urged to use Taiwan's proper name on website," Central News Agency (Taiwan), July 7, 2011. [http://focustaiwan.tw/ShowNews/WebNews\\_Detail.aspx?Type=aIPL&ID=201107070012](http://focustaiwan.tw/ShowNews/WebNews_Detail.aspx?Type=aIPL&ID=201107070012).

203. Stephen Olson and Clyde Prestowitz, *The Evolving Role of China in International Institutions* (Washington, DC: The Economic Strategy Institute, January 2011), pp.15–16. <http://www.uscc.gov/researchpapers/2011/TheEvolvingRoleofChinainInternationalInstitutions.pdf>.

204. Mo Yan-chih, "Burkina Faso Grants Visa Waiver," Taipei Times (Taiwan), October 9, 2011. <http://www.taipetimes.com/news/taiwan/archives/2011/10/09/>



2003515299; and Nancy Liu, "Taiwan 'optimistic' over U.S. visa waiver prospects," Central News Agency (Taiwan), July 6, 2011. [http://focustaiwan.tw/ShowNews/WebNews\\_Detail.aspx?Type=aIPL&ID=201107060008](http://focustaiwan.tw/ShowNews/WebNews_Detail.aspx?Type=aIPL&ID=201107060008).

205. Ma Ying-jeou (president of Taiwan), meeting with Commissioners, August 17, 2011, Taipei, Taiwan.

206. Jorge Liu and Pin-yu Chen, "U.S. visa waiver talks on course: National Immigration Agency," *Focus Taiwan News Channel*, June 21, 2011. <http://www.wantchinatimes.com/news-subclass-cnt.aspx?cid=1101&MainCatID=&id=20110621000118>.

207. Shih Hsiu-chuan, "US-Taiwan draft treaty proposed," *Taipei Times*, January 8, 2011. <http://www.taipeitimes.com/News/taiwan/archives/2011/01/08/2003492980>; and *Taipei Times*, "US extradition treaty a priority: Shen," May 26, 2011. <http://www.taipeitimes.com/News/taiwan/archives/2011/05/26/2003504193u>.

208. U.S.-China Economic and Security Review Commission, luncheon with Taipei Economic and Cultural Representative Office representatives, Washington, DC, June 14, 2011. See also Shih Hsiu-chuan, "US-Taiwan draft treaty proposed," *Taipei Times*, January 8, 2011. <http://www.taipeitimes.com/News/taiwan/archives/2011/01/08/2003492980>; and *Taipei Times*, "US extradition treaty a priority: Shen," May 26, 2011. <http://www.taipeitimes.com/News/taiwan/archives/2011/05/26/2003504193>.

209. T. Y. Wang, Wei-Chin Lee, and Ching-Hsin Yu, "Taiwan's Expansion of International Space: Opportunities and Challenges," *Journal of Contemporary China* 20:69 (March 2011): 255.

210. Officials of Taiwan's Ministry of Economic Affairs, meeting with Commissioners, Taipei, Taiwan, August 17, 2011.

211. *China Post (Taiwan)*, "Taiwan, Singapore begin free trade agreement discussions," May 23, 2011. <http://www.chinapost.com.tw/taiwan/national/national-news/2011/05/23/303403/Taiwan-Singapore.htm>; David Brown, "China-Taiwan Relations: Steady as She Goes," *Comparative Connections* (Washington, DC: Center for Strategic and International Studies, May 2011), p. 9; and Carnegie Endowment for International Peace, *Challenges to Cross-Strait Relations in 2012*, keynote address by Lai Shin-yuan, July 7, 2011.

212. Richard Bush, "Taiwan and East Asian Security," *Orbis* 2:55 (Spring 2011): 276; T. Y. Wang, Wei-Chin Lee, and Ching-Hsin Yu, "Taiwan's Expansion of International Space: opportunities and challenges," *Journal of Contemporary China* 20:69 (March 2011): 255; and Center for National Policy, *The Future of the US-Taiwan Relationship*, statement by Robert Sutter, August 3, 2011.

213. Carnegie Endowment for International Peace, *Challenges to Cross-Strait Relations in 2012*, keynote address by Lai Shin-yuan, July 7, 2011.

214. Central News Agency (Taiwan), "Beef issues are affecting TIFA [Trade and Investment Framework Agreement] talks: US official," April 13, 2011. <http://www.chinapost.com.tw/taiwan/foreign-affairs/2011/04/13/298427/Beef-issues.htm>; *Inside U.S.-China Trade*, "Hill Trade Leaders Slam Taiwan on New Barrier to U.S. Beef Exports," February 18, 2011; and House Committee on Foreign Affairs, *Hearing on Why Taiwan Matters*, testimony of Rupert Hammond-Chambers, 112th Cong., 1st sess., June 16, 2011.

215. *Inside U.S.-China Trade*, "Hill Trade Leaders Slam Taiwan on New Barrier to U.S. Beef Exports," February 18, 2011; House Committee on Foreign Affairs, *Hearing on Why Taiwan Matters*, testimony of Rupert Hammond-Chambers, 112th Cong., 1st sess., June 16, 2011; U. S. Senate Committee on Finance, Press Release, "Baucus, Hatch, Camp, Levin Urge Taiwan to End Unscientific Restriction on American Beef Exports," February 17, 2011. <http://finance.senate.gov/newsroom/chairman/release/?id=67af6705-9378-4602-bb69-1733c2a20ef5>; and Shih Hsiu-chuan, "Officials indicate ractopamine ban remains in place," *Taipei Times*, July 10, 2011. <http://taipeitimes.com/News/front/archives/2011/07/10/2003507849>.

216. Office of the U.S. Trade Representative, "Joint Statement from USTR, USDA [U.S. Department of Agriculture] on Taiwan's Actions to Unjustifiably Restrict U.S. Beef Imports in Violation of Our Bilateral Agreement," January 2011. <http://www.ustr.gov/about-us/press-office/press-releases/2010/january/joint-statement-ustr-usda-taiwan%e2%80%99s-actions-unjusti>.

217. Rachel Chan, "Ma Calls for Enhancement of Taiwan-US Ties," *Taiwan Today*, September 15, 2011. <http://www.taiwantoday.tw/ct.asp?xItem=175991&CtNode=414>.

218. Bloomberg, "ECFA [Economic Cooperation Framework Agreement] 'early harvest' list tariff cuts come into effect," January 2, 2011. <http://www.taipeitimes.com/News/front/archives/2011/01/02/2003492456>.

219. David Brown, "China-Taiwan Relations: Steady As She Goes," *Comparative Connections* (Washington, DC: Center for Strategic and International Studies, May 2011), p. 2.



220. Ko Shu-ling, "Taipei, Beijing set up trade committee," *Taipei Times*, January 7, 2011. <http://www.taipeitimes.com/News/front/archives/2011/01/07/2003492879>.

221. *China Post* (Taiwan), "ECFA [Economic Cooperation Framework Agreement] follow-up negotiations slated for Aug. 1-7," August 1, 2011. <http://www.chinapost.com.tw/taiwan/national/national-news/2011/08/01/311844/ECFA-follow-up.htm>.

222. Officials of Taiwan's Ministry of Economic Affairs, meeting with Commissioners, Taipei, Taiwan, August 17, 2011.

223. Taipei Economic and Cultural Office, "MOEA [Ministry of Economic Affairs] further eases rules on mainland Chinese investment," March 3, 2011. <http://www.roc-taiwan.org/us/ct.asp?xItem=185760&ctNode=2300&mp=12>.

224. Mainland Affairs Council, *Cross-Strait Economic Statistics Monthly* No. 217 (Taipei, Taiwan: May 30, 2011). <http://www.mac.gov.tw/ct.asp?xItem=95294&ctNode=5934&mp=3>.

225. *China Post* (Taiwan), "Chinese investment in Taiwan remains lackluster," December 20, 2010. <http://www.asianewsnet.net/home/news.php?id=16246>.

226. Fanny Liu and Paul Mozur, "Taiwan Opens More Sectors to Chinese Investors," *Wall Street Journal*, March 2, 2011. <http://online.wsj.com/article/SB10001424052748703559604576176074279169148.html>.

227. Fanny Liu and Paul Mozur, "Taiwan, China Discuss Possible Rare-Earths Deal," *Wall Street Journal*, May 19, 2011. <http://online.wsj.com/article/SB10001424052748703509104576331002173001170.html>.

228. David Brown, "China-Taiwan Relations: Steady As She Goes," *Comparative Connections* (Washington, DC: Center for Strategic and International Studies, May 2011), p. 6.

229. Mainland Affairs Council, *Cross-Strait Economic Statistics Monthly* No. 217 (Taipei, Taiwan: May 30, 2011), p. 14. <http://www.mac.gov.tw/public/Attachment/15301134762.pdf>.

230. Mainland Affairs Council, *Cross-Strait Economic Statistics Monthly* No. 221 (Taipei, Taiwan: August 29, 2011), p. 14. <http://www.mac.gov.tw/public/Attachment/182914582215.pdf>.

231. U.S. Census Bureau, "Trade in Goods with Taiwan" (Washington, DC: U.S. Department of Commerce). <http://www.census.gov/foreign-trade/balance/c5830.html>.

232. Wendell Minnick, "Taiwan President Urges U.S. to Release F-16s," *Defense News*, May 13, 2011. <http://www.defensenews.com/story.php?i=6499441&c=AIR&s=ASI>.

233. Information Office of the State Council, *China's National Defense in 2010* (Beijing, China: January 2011).

234. Information Office of the State Council, *China's National Defense in 2010* (Beijing, China: January 2011); and Ko Shu-ling, "China's call for CBMs [confidence building measures] Rejected," Central News Agency (Taiwan), April 1, 2011. <http://www.taipeitimes.com/News/taiwan/archives/2011/04/01/2003499639>.

235. Ko Shu-ling, "China's call for CBMs [confidence building measures] measures Rejected," Central News Agency (Taiwan), April 1, 2011. <http://www.taipeitimes.com/News/taiwan/archives/2011/04/01/2003499639>.

236. U.S. Department of Defense, *Joint Press Conference with Adm. Mullen and Gen. Chen from the Pentagon*, May 18, 2011. <http://www.defense.gov/transcripts/transcripts.aspx?transcriptid=4824>.

237. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: U.S. Department of Defense, August, 2011), p. 2. Taiwan's recently released defense white paper posits a slightly higher number at more than 1,400. However, this number is slightly ambiguous, since it includes both short-range ballistic missiles and ground-launched cruise missiles. Taiwan Ministry of National Defense, "Zhonghua Minguo Yi Bai Nian Guofang Baogaoshu" (2011 National Defense Report, the Republic of China) (Taipei, Taiwan: July 2011), p. 69.

238. Agence France-Presse, "Ten mainland moles 'infiltrated' Taipei," February 13, 2011. [http://www.google.com/hostednews/afp/article/ALeqM5gDv7A4cNvPRIwO5Kb3lO\\_3-GfeQ?docId=CNG.7fc4d4a85840416799351787f9748bf5.301](http://www.google.com/hostednews/afp/article/ALeqM5gDv7A4cNvPRIwO5Kb3lO_3-GfeQ?docId=CNG.7fc4d4a85840416799351787f9748bf5.301).

239. Agence France-Presse, "Taiwan defense damaged, says ex-spy master," February 14, 2011. <http://www.scmp.com/portal/site/SCMP/menuitem.2af62ecb329d3d7733492d9253a0a0a0/?vgnnextoid=547bb73881e210VgnVCM100000360a0a0aRCRD&ss=china&s=news>.

240. Joseph Yeh, "No High-Ranking Officers Involved in Latest Alleged Spy Case: MND [Ministry of National Defense]," *China Post* (Taiwan), June 15, 2011. <http://www.chinapost.com.tw/taiwan/china-taiwan-relations/2011/06/15/306244/No-high-ranking.htm>.

241. Agence France-Presse, "Ten mainland moles 'infiltrated' Taipei," February 13, 2011. [http://www.google.com/hostednews/afp/article/ALeqM5gDv7A4cNvPRI\\_wO5Kb3lO\\_3-GfeQ?docId=CNG.7fc4d4a85840416799351787f9748bf5.301](http://www.google.com/hostednews/afp/article/ALeqM5gDv7A4cNvPRI_wO5Kb3lO_3-GfeQ?docId=CNG.7fc4d4a85840416799351787f9748bf5.301).
242. *Taiwan Today*, "Military stages highway landing, takeoff drill in Hainan," April 12, 2011. <http://www.taiwantoday.tw/ct.asp?xitem=159578&CtNode=414>.
243. Paul Mozur, "Taiwan Seeks to Move U.S. on Arms Sales," *Wall Street Journal*, April 13, 2011. <http://online.wsj.com/article/SB10001424052748704336504576258711163099214.html>.
244. Paul Mozur, "Taiwan Produces New Type of Missile," *Wall Street Journal*, December 10, 2010. [http://online.wsj.com/article/SB10001424052748704720804576009320033954668.html?mod=WSJ\\_hps\\_sections\\_world](http://online.wsj.com/article/SB10001424052748704720804576009320033954668.html?mod=WSJ_hps_sections_world).
245. Wendell Minnick, "Taiwan's 'Carrier Killer' Aims To Sink China's Carrier," *Defense News*, August 10, 2011. <http://www.defensenews.com/story.php?i=7356595>.
246. Paul Mozur, "Taiwan Produces New Type of Missile," *Wall Street Journal*, December 10, 2010. [http://online.wsj.com/article/SB10001424052748704720804576009320033954668.html?mod=WSJ\\_hps\\_sections\\_world](http://online.wsj.com/article/SB10001424052748704720804576009320033954668.html?mod=WSJ_hps_sections_world).
247. Agence France-Presse, "Taiwan to Deploy Supersonic Missile on Warships," May 8, 2011. <http://www.defensenews.com/story.php?i=6447237&c=ASI&s=SEA>.
248. Agence France-Presse, "Taiwan supersonic missile test flops," June 28, 2011. <http://www.scmp.com/portal/site/SCMP/menuitem.2af62ecb329d3d7733492d9253a0a0a0/?vgnextoid=5f629af3694d0310VgnVCM100000360a0a0aRCRD&ss=china&s=news>.
249. Agence France-Presse, "Taiwan inaugurates missile ships amid buildup vow," April 7, 2011. <http://www.defensenews.com/story.php?c=ASI&s=TOP&i=6173472>; and Agence France-Presse, "Taiwan Inaugurates 'Stealth' Missile Boat Squadron," May 18, 2010. <http://www.defensenews.com/story.php?i=4630623>.
250. J. Michael Cole, "Taiwanese military reportedly develops 'stealth' coating," *Taipei Times*, July 5, 2011. <http://www.taipetimes.com/News/front/archives/2011/07/05/2003507440>.
251. Agence France-Presse, "Taiwan unveils upgraded fighter jets," June 30, 2011. [http://www.google.com/hostednews/afp/article/ALeqM5j2duqRzA\\_oUE2O2ow3l17zx3xmJw?docId=CNG.1c577930381fad6dfc4d633656a73e2f.61](http://www.google.com/hostednews/afp/article/ALeqM5j2duqRzA_oUE2O2ow3l17zx3xmJw?docId=CNG.1c577930381fad6dfc4d633656a73e2f.61).
252. Aries Poon and Fanny Liu, "Taiwan's Test of Missiles Falls Short," *Wall Street Journal*, January 19, 2011. <http://online.wsj.com/article/SB10001424052748703954004576089404084137200.html>.
253. Agence France-Presse, "Taiwan air force missile test flops again," March 23, 2011. [http://www.google.com/hostednews/afp/article/ALeqM5jMBuC2\\_AlSKy8KjrkC9kwG7Ank4g?docId=CNG.708d1a839f1c5f21bc13ae791866aef8.2a1](http://www.google.com/hostednews/afp/article/ALeqM5jMBuC2_AlSKy8KjrkC9kwG7Ank4g?docId=CNG.708d1a839f1c5f21bc13ae791866aef8.2a1).
254. Officials of Taiwan's Ministry of National Defense, meeting with Commissioners, Taipei, Taiwan, August 17, 2011.
255. Vincent Y. Chao, "Pundits say defense cuts invite aggression," *Taipei Times*, June 22, 2011. <http://www.taipetimes.com/News/front/archives/2011/06/22/2003506383>; and Agence France-Presse, "Taiwan to cut 9,200 troops as ties warm," March 7, 2011. <http://www.scmp.com/portal/site/SCMP/menuitem.2af62ecb329d3d7733492d9253a0a0a0/?vgnextoid=dd0dc15ea8e8e210VgnVCM100000360a0a0aRCRD&ss=china&s=news>.
256. Agence France-Presse, "Taiwan to Delay Buying Arms From US: Lawmaker," May 10, 2011. <http://www.defensenews.com/story.php?i=6460744&c=ASI&s=TOP>.
257. Associated Press, "Taiwan to postpone purchases of US weapons," May 10, 2011. <http://www.cbsnews.com/stories/2011/05/10/ap/asia/main20061683.shtml>.
258. Office of the Assistant Secretary of Defense (Public Affairs), "Contracts" No. 566-11 (Washington, DC: U.S. Department of Defense, June 30, 2011). <http://www.defense.gov/Contracts/Contract.aspx?ContractID=4568>.
259. Defense Security Cooperation Agency, "News Release: Taipei Economic and Cultural Representative Office in the United States—Retrofit of F-16A/B Aircraft" (Washington, DC: U.S. Department of Defense, September 21, 2011).
260. Defense Security Cooperation Agency, "News Release: Taipei Economic and Cultural Representative Office in the United States—Retrofit of F-16A/B Aircraft" (Washington, DC: U.S. Department of Defense, September 21, 2011).
261. U.S. Department of Defense, "Joint Press Conference with Secretary Gates and General Liang from Beijing, China," January 10, 2011. <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4750>; and Amy Chang, "The Chinese People's Liberation Army Delegation Visit to the United States, May 2011: A Summary of Key Actors and Issues," *Staff Backgrounder* (Washington, DC: U.S.-China Economic and Security Review Commission, June 30, 2011), p. 1.
262. Xinhua, "Foreign Ministry Spokesman Ma Zhaoxu Expounds on China's Solemn Stance on the Announced Arms Sale Package to Taiwan by the US Government," September 21, 2011. <http://www.fmprc.gov.cn/eng/xwfw/s2510/t861278.htm>.

263. Yang Jiechi (foreign minister of China), speech to the National Committee on U.S.-China Relations and the U.S.-China Business Council, September 22, 2011, New York City. <http://www.mfa.gov.cn/chn/pds/ziliao/zyjh/t861433.htm>.

264. Josh Rogin, "China to Suspend some Military-to-Military Activities with U.S. over Taiwan Arms Sales," *Financial Times*, September 26, 2011.

265. Shirley A. Kan, "Taiwan: Major U.S. Arms Sales since 1990" (Washington, DC: Congressional Research Service, August 2, 2011), pp. 19–23.

266. Ma Ying-jeou (president of Taiwan), meeting with Commissioners, August 17, 2011, Taipei, Taiwan.

267. Zhang Fan, "Zongtong Pan Jixu Zhengqu F-16C/D" (President Hopes to Continue to Fight for F-16C/D), *Radio Taiwan International*, September 22, 2011. [http://news.rti.org.tw/index\\_newsContent.aspx?nid=319109](http://news.rti.org.tw/index_newsContent.aspx?nid=319109).

268. Shirley A. Kan, "Taiwan: Major U.S. Arms Sales since 1990" (Washington, DC: Congressional Research Service, August 2, 2011), pp. 10–14.

269. Ma Ying-jeou (president of Taiwan), meeting with Commissioners, August 17, 2011, Taipei, Taiwan.

270. Kao Hua-chu (minister of Defense, Taiwan), meeting with Commissioners, Taipei, Taiwan, August 17, 2011.

271. National People's Congress of the People's Republic of China, *The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China* (Beijing, China: April 4, 1990). [http://www.basiclaw.gov.hk/en/basiclawtext/images/basiclaw\\_full\\_text.pdf](http://www.basiclaw.gov.hk/en/basiclawtext/images/basiclaw_full_text.pdf).

272. Frank Ching, "Hong Kong's Autonomy Slips Away," *Hong Kong Journal* (April 2011). [http://www.hkjournal.org/archive/2011\\_summer/1.htm](http://www.hkjournal.org/archive/2011_summer/1.htm); Li Keqiang, "Step Up Cooperation for Development and Prosperity" (Speech at the Forum on 12th Five-Year Plan and Mainland-Hong Kong Economic, Trade and Financial Cooperation," Hong Kong, August 17, 2011).

273. Li Keqiang, "Step Up Cooperation for Development and Prosperity" (Speech at the Forum on the 12th Five-Year Plan and Mainland-Hong Kong Economic, Trade and Financial Cooperation," Hong Kong, August 17, 2011).

274. Koh Gui Qing, "Factbox: How will China internationalize the yuan?" Reuters, August 31, 2011. <http://www.reuters.com/article/2011/08/24/us-china-yuan-factbox-idUSTRE77N1XG20110824>; Robert Cookson, "Renminbi has yet to find great favour in loan market," *Financial Times*, September 13, 2011. <http://www.ft.com/cms/s/0/816111d8-d2ec-11e0-9aae-00144feab49a.html#axzz1YXNp9EeK>.

275. Hong Kong Economic and Trade Office, "Cato Institute Releases 15th Report on Global Economic Freedom" (Hong Kong, SAR [Special Administrative Region]: September 20, 2011). <http://www.sacbee.com/2011/09/20/3925114/hong-kong-remains-worlds-freest.html>.

276. Goldman Sachs representative, meeting with the U.S.-China Economic and Security Review Commission, Hong Kong, August 15, 2011.

277. Li Keqiang, "Step Up Cooperation for Development and Prosperity" (Speech at the Forum on 12th Five-Year Plan and Mainland-Hong Kong Economic, Trade and Financial Cooperation," Hong Kong, August 17, 2011); Wang Yong, "Internationalizing the Yuan: Completing the Circuit" (Ontario, Canada: The Centre for International Governance Innovation, August 31, 2011). <http://www.cigionline.org/publications/2011/8/internationalizing-yuan-completing-circuit>.

278. Goldman Sachs representatives, Hong Kong Economic and Trade Office officials, and journalists, meetings with the U.S.-China Economic and Security Review Commission, Hong Kong, August 15, 2011.

279. Hong Kong Economic and Trade Office officials, meetings with U.S.-China Economic and Security Review Commission, Hong Kong, August 15, 2011.

280. Andy Lau, "KC Chan: Yuan globalization to drive growth of China's financial market," *International Business Times*, May 21, 2011. <http://hken.ibtimes.com/articles/149626/20110521/china-gdp-yuan-hong-kong-rmb-qfii-qdii.htm>; Hong Kong Information Services Department, "RMB deposits up 6.4%," September 30, 2011. <http://www.news.gov.hk/en/categories/finance/html/2011/09/20110930-165401.shtml>.

281. Ben Richardson and Sophie Leung, "China Vice Premier's Hong Kong Tour Shows City in Dual Light," Bloomberg News, August 16, 2011. <http://www.bloomberg.com/news/2011-08-16/chinese-vice-premier-s-hong-kong-tour-shows-city-in-dual-light.html>.

282. Anthony B. L. Cheung, "Hong Kong: A City of Unhappiness," *Hong Kong Journal* (July 2011). [http://www.hkjournal.org/archive/2011\\_fall/1.htm](http://www.hkjournal.org/archive/2011_fall/1.htm); Robert Keatley, "Mid-Year Malaise: No Progress on Leading Issues," *Hong Kong Journal* (July 2011). <http://www.hkjournal.org/archive/commentaries/072011.htm>; and Kevin Drew, "Growing Discontent Seen in Annual Hong Kong Protest," *New York Times*, July 1, 2011. <http://www.nytimes.com/2011/07/02/world/asia/02iht-hong02.html?pagewanted=all>.

283. Ben Richardson and Sophie Leung, "China Vice Premier's Hong Kong Tour Shows City in Dual Light," Bloomberg News, August 16, 2011. <http://www.bloomberg.com/news/2011-08-16/chinese-vice-premier-s-hong-kong-tour-shows-city-in-dual-light.html>; Ding Qingfen, Li Xiang, and Joseph Li, "Li Keqiang expresses support for Hong Kong," *China Daily*, August 17, 2011. [http://www.china.org.cn/china/2011-08/17/content\\_23226159.htm](http://www.china.org.cn/china/2011-08/17/content_23226159.htm).

284. Martin Wong, "The poor go short as food prices bite," *South China Morning Post*, August 18, 2011. <http://topics.scmp.com/news/hk-news-watch/article/The-poor-go-short-as-food-prices-bite>; Robert Keatley, "Mid-Year Malaise: No Progress on Leading Issues," *Hong Kong Journal* (July 2011). <http://www.hkjournal.org/archive/commentaries/072011.htm>.

285. Rahul Jacob, "Entrepot with political attitude," *Financial Times*, September 12, 2011. <http://www.ft.com/intl/cms/s/0/93d33e44-d71b-11e0-bc73-00144feabdc0.html#axzz1YXNp9EeK>; Ng Tze-wei and Chris Ip, "Beijing to bring HK courts into line," *South China Morning Post*, August 25, 2011. <http://topics.scmp.com/news/hk-news-watch/article/Beijing-to-bring-HK-courts-into-line>.

286. Ng Tze-wei and Chris Ip, "Beijing to bring HK courts into line," *South China Morning Post*, August 25, 2011. <http://topics.scmp.com/news/hk-news-watch/article/Beijing-to-bring-HK-courts-into-line>; Dina Lee, "You be the judge," *Standard (Hong Kong)*, June 9, 2011. [http://www.thestandard.com.hk/news\\_detail.asp?sid=32661341&art\\_id=111924&con\\_type=1&pp\\_cat=30](http://www.thestandard.com.hk/news_detail.asp?sid=32661341&art_id=111924&con_type=1&pp_cat=30); and Isabella Steger and Lam Thuy Vo, "Hong Kong Foreign Labor Law Challenged," *Wall Street Journal*, August 22, 2011. <http://online.wsj.com/article/SB10001424053111904070604576517911520701054.html>.

287. U.S. Library of Congress, "China/Hong Kong: Congo Assets Case Tests Sovereign Immunity" (Washington, DC: September 1, 2011). [http://www.loc.gov/lawweb/servlet/lloc\\_news?disp3\\_l205402793\\_text](http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205402793_text).

288. Agence France-Presse, "Lessons in patriotism for Hong Kong children," May 5, 2011. <http://www.google.com/hostednews/afp/article/ALeqM5il-twQLD7GQZm9LgZHmNeaZFz-uQ?docId=CNG.b7f0a9c0dbc00c090e2f00b13916c384.11>; Gordon Chang, "China Tries to 'Brainwash' Hong Kong," *World Affairs Journal* (May 16, 2011). [http://www.worldaffairsjournal.org/new/blogs/chang/China\\_Tries\\_to\\_Brainwash\\_Hong\\_Kong](http://www.worldaffairsjournal.org/new/blogs/chang/China_Tries_to_Brainwash_Hong_Kong).

289. Ad Hoc Committee on Moral and National Education, *Consultation on Moral and National Education Curriculum (Summary)* (Hong Kong, SAR [Special Administrative Region]: Hong Kong Ministry of Education, 2011), p. 19. [http://www.edb.gov.hk/FileManager/TC/Content\\_2428/Consultation\\_on\\_MNE\\_Curriculum\\_%28Summary%29\\_2.pdf](http://www.edb.gov.hk/FileManager/TC/Content_2428/Consultation_on_MNE_Curriculum_%28Summary%29_2.pdf).

290. National Democratic Institute, *The Promise of Democratization in Hong Kong Report #14, Taking Stock: The Passage of the Political Reform Package* (Washington, DC: November 2010), p. 14. [http://www.ndi.org/files/Hong\\_Kong\\_political\\_assessment\\_14.pdf](http://www.ndi.org/files/Hong_Kong_political_assessment_14.pdf); Ngok Ma, "Hong Kong's Democrats Divide," *Journal of Democracy* 22:1 (January 2011): 55.

291. National People's Congress of the People's Republic of China, *The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China* (Beijing, China: April 4, 1990). [http://www.basiclaw.gov.hk/en/basiclawtext/images/basiclaw\\_full\\_text.pdf](http://www.basiclaw.gov.hk/en/basiclawtext/images/basiclaw_full_text.pdf).

292. Michael F. Martin, *Prospects for Democracy in Hong Kong: The 2012 Election Reforms* (Washington, DC: Congressional Research Service, February 2011), pp. 9–10. [http://assets.opencrs.com/rpts/R40992\\_20110201.pdf](http://assets.opencrs.com/rpts/R40992_20110201.pdf).

293. National People's Congress of the People's Republic of China, *Decision of the Standing Committee of the National People's Congress on Issues Relating to the Methods for Selecting the Chief Executive of the Hong Kong Special Administrative Region and for Forming the Legislative Council of the Hong Kong Special Administrative Region in the Year 2012 and on Issues Relating to Universal Suffrage* (Beijing, China: December 29, 2007). [http://news.xinhuanet.com/english/2007-12/29/content\\_7334596.htm](http://news.xinhuanet.com/english/2007-12/29/content_7334596.htm).

294. Michael F. Martin, *Prospects for Democracy in Hong Kong: The 2012 Election Reforms* (Washington, DC: Congressional Research Service, February 2011), pp. 5–15. [http://assets.opencrs.com/rpts/R40992\\_20110201.pdf](http://assets.opencrs.com/rpts/R40992_20110201.pdf); Hong Kong Special Administrative Region Chief Executive Election (Amendment) Ordinance #1 of 2011, March 10, 2011. <http://www.legco.gov.hk/yr10-11/english/ord/ord001-11-e.pdf>; Hong Kong Special Administrative Region Legislative Council (Amendment) Ordinance #2 of 2011, March 10, 2011. <http://www.legco.gov.hk/yr10-11/english/ord/ord002-11-e.pdf>.

295. *China Daily*, "Nod to HK electoral reform 'a victory,'" June 26, 2010. [http://www.chinadaily.com.cn/cndy/2010-06/26/content\\_10022648.htm](http://www.chinadaily.com.cn/cndy/2010-06/26/content_10022648.htm).

296. Chan Kin Man, "Cleavages and Challenges in Hong Kong's Pro-Democracy Camp," *Hong Kong Journal* (July 2011): 3. [http://www.hkjournal.org/PDF/2011\\_fall/](http://www.hkjournal.org/PDF/2011_fall/)



3.pdf; Chris Yeung, "Political Changes Cloud the Future," *Hong Kong Journal* (January 2011). [http://www.hkjjournal.org/archive/2011\\_spring/2.htm](http://www.hkjjournal.org/archive/2011_spring/2.htm).

297. Chan Kin Man, "Cleavages and Challenges in Hong Kong's Pro-Democracy Camp," *Hong Kong Journal* (July 2011): 3. [http://www.hkjjournal.org/PDF/2011\\_fall/3.pdf](http://www.hkjjournal.org/PDF/2011_fall/3.pdf); Chris Yeung, "Political Changes Cloud the Future," *Hong Kong Journal* (January 2011). [http://www.hkjjournal.org/archive/2011\\_spring/2.htm](http://www.hkjjournal.org/archive/2011_spring/2.htm).

298. Coleen Lee, "Democrats lick wounds as 30 reform radicals quit," *Standard (Hong Kong)*, December 20, 2011. [http://www.thestandard.com.hk/news\\_detail.asp?sid=30685198&art\\_id=106201&con\\_type=1&pp\\_cat=12](http://www.thestandard.com.hk/news_detail.asp?sid=30685198&art_id=106201&con_type=1&pp_cat=12).

299. Hak Yin Li and Yongnian Zheng, "Grassroots Participation in Hong Kong: 2007 District Council Elections and Their Aftermath" (Nottingham, United Kingdom: University of Nottingham China Policy Institute, 2008), p. 2. <http://www.nottingham.ac.uk/cpi/documents/briefings/briefing-37-hk-grassroots-elections.pdf>; Peter So and Tanna Chong, "Radicals take poll protest direct to Democratic Party," *South China Morning Post*, September 21, 2011. <http://www.scmp.com/portal/site/SCMP/menuitem.2af62ecb329d3d7733492d9253a0a0a0/?vgnextoid=4dccb46a80782310VgnVCM100000360a0a0aRCD&ss=Hong+Kong&s=News>.

300. Tanna Chong, "Poll losses could endanger reform policy: Democrat," *South China Morning Post*, October 6, 2011. <http://www.scmp.com/portal/site/SCMP/menuitem.2af62ecb329d3d7733492d9253a0a0a0/?vgnextoid=bbf31564134d2310VgnVCM100000360a0a0aRCD&ss=Hong+Kong&s=News>.

301. Willy Lam, "Beijing's Hand in Hong Kong Politics," *The Jamestown Foundation China Brief* 4:12 (June 9, 2011) [http://www.jamestown.org/single/?no\\_cache=1&tx\\_ttnews\[tt\\_news\]=26643](http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=26643); National Democratic Institute, *The Promise of Democratization in Hong Kong Report #12, The 2007 District Council Elections, Legislative Council By-election, and Prospects for Constitutional Reform* (Washington, DC: December 2007). [http://www.ndi.org/files/2243\\_hk\\_report\\_122807\\_0.pdf](http://www.ndi.org/files/2243_hk_report_122807_0.pdf).

302. Fanny W.Y. Fung and Lo Wei, "Voters spoil for choice on crowded campaign trail," *South China Morning Post*, March 29, 2011. <http://topics.scmp.com/news/who-runshk/article/Voters-spoilt-for-choice-on-crowded-campaign-trail1>; Chan Kin Man, "Cleavages and Challenges in Hong Kong's Pro-Democracy Camp," *Hong Kong Journal* (July 2011): 7. [http://www.hkjjournal.org/PDF/2011\\_fall/3.pdf](http://www.hkjjournal.org/PDF/2011_fall/3.pdf); and Ngok Ma, "Hong Kong's Democrats Divide," *Journal of Democracy* 22:1 (January 2011).

303. Chan Kin Man, "Cleavages and Challenges in Hong Kong's Pro-Democracy Camp," *Hong Kong Journal* (July 2011): 7. [http://www.hkjjournal.org/PDF/2011\\_fall/3.pdf](http://www.hkjjournal.org/PDF/2011_fall/3.pdf).

304. Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A109938&lang=en-US>; Human Rights Watch, "Hong Kong: Investigate Police Actions at July 1 Rally," July 11, 2011. <http://www.hrw.org/news/2011/07/11/hong-kong-investigate-police-actions-july-1-rally>.

305. Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A109938&lang=en-US>.

306. Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-938&lang=en-US>.

307. Human Rights Watch, "Hong Kong: Investigate Police Actions at July 1 Rally," July 11, 2011. <http://www.hrw.org/news/2011/07/11/hong-kong-investigate-police-actions-july-1-rally>.

308. Hong Kong Press Photographers Association and Hong Kong Journalists Association, "Stop bullying Hong Kong People, we have a right to know!" August 20, 2011. <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-950&lang=en-US>.

309. Hong Kong Press Photographers Association and Hong Kong Journalists Association, "Stop bullying Hong Kong People, we have a right to know!" August 20, 2011. <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-950&lang=en-US>.

310. Associated Press, "Hong Kong worries about China's tightening grip," September 1, 2011. <http://news.yahoo.com/hong-kong-worries-china-tightening-grip-092019428.html>.

311. Associated Press, "Hong Kong worries about China's tightening grip," September 1, 2011. <http://news.yahoo.com/hong-kong-worries-china-tightening-grip-092019428.html>.

312. International Federation of Journalists, "IFJ Fears Erosion of Editorial Independence in Hong Kong," September 13, 2011. <http://asiapacific.ifj.org/en/articles/ifj-fears-erosion-of-editorial-independence-in-hong-kong>; Reuters, "Broadcasters pro-



test over bureaucratic editor,” September 15, 2011. <http://tvnz.co.nz/world-news/broadcasters-protest-against-bureaucratic-editor-4404462>.

313. Michael Wines, “Hong Kong TV Officials Resign Over False Report,” *New York Times*, September 7, 2011. [http://www.nytimes.com/2011/09/07/world/asia/07hongkong.html?\\_r=1](http://www.nytimes.com/2011/09/07/world/asia/07hongkong.html?_r=1).

314. Martin Wong, “ATV [Asia Television Limited] journalists told to ‘tune down report,’” *South China Morning Post*, September 8, 2011. <http://topics.scmp.com/news/hk-news-watch/article/ATV-journalists-told-to-tune-down-report>.

315. Hong Kong University Public Opinion Programme, “HKU POP SITE releases people’s appraisal of local news media,” April 26, 2011. <http://hkupop.hku.hk/>.

316. Hong Kong University Public Opinion Programme, “HKU POP SITE releases people’s appraisal of local news media,” April 26, 2011. <http://hkupop.hku.hk/>.

317. Alan Leong (Hong Kong legislative councilor and leader of the democratic Civic Party), meeting with the U.S.-China Economic and Security Review Commission, Washington, DC, July 19, 2011.

318. Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-938&lang=en-US>.

319. Diana Lee, “Sleepless in Mei Foo,” *Standard (Hong Kong)*, April 4, 2011. [http://thestandard.com.hk/news\\_detail.asp?pp\\_cat=30&art\\_id=109827&sid=31902147&con\\_type=3](http://thestandard.com.hk/news_detail.asp?pp_cat=30&art_id=109827&sid=31902147&con_type=3); Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-938&lang=en-US>.

320. Tiffany Lam, “Protests over development near one of Hong Kong’s best beaches,” *CNN International*, July 20, 2010. <http://www.cnn.com/hong-kong/hong-kong-races-save-one-its-best-beaches-851163>; Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-938&lang=en-US>.

321. Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-938&lang=en-US>.

322. Hong Kong business representatives, meeting with the U.S.-China Economic and Security Review Commission, August 15, 2011.

323. Alan Leong (Hong Kong legislative councilor and leader of the democratic Civic Party), meeting with the U.S.-China Economic and Security Review Commission, Washington, DC, July 19, 2011.

324. Kevin Drew, “Growing Discontent Seen In Annual Hong Kong Protest,” *New York Times*, July 1, 2011. <http://www.nytimes.com/2011/07/02/world/asia/02iht-hong02.html?pagewanted=all>.

325. Isabella Steger and Paul Mozur, “Thousands Rally in Hong Kong for Human Rights,” *Wall Street Journal*, June 4, 2011. [http://online.wsj.com/article/SB100014240527023037453045763\\_65371935162988.html](http://online.wsj.com/article/SB100014240527023037453045763_65371935162988.html); Keith Bradsher, “Thousands gather in Hong Kong for Tiananmen Vigil,” *New York Times*, June 4, 2009. <http://www.nytimes.com/2009/06/05/world/asia/05hong.html>.

326. Reuters, “Pressure builds on Hong Kong after anti-budget protests,” March 6, 2011. <http://www.reuters.com/article/2011/03/07/us-hongkong-budget-arrest-idUSTRE7260LG20110307>; Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-38&lang=en-US>.

327. Alan Leong (Hong Kong legislative councilor and leader of the democratic Civic Party), meeting with the U.S.-China Economic and Security Review Commission, Washington, DC, July 19, 2011.

328. Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-938&lang=en-US>.

329. Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-938&lang=en-US>.

330. Lai Ying-kit, “Police confront protesters at Tamar,” *South China Morning Post*, August 18, 2011. <http://www.scmp.com/portal/site/SCMP/menuitem.2af62ecb329d3d7733492d9253a0a0a0/?vgnextoid=051d123758cd1310VgnVCM100000360a0a>

0aRCRD&ss=Hong+Kong&s=News; Peter So, Stuart Lau, and Simpson Cheung, "Police chief defends tactics against protesters," *South China Morning Post*, August 19, 2011. <http://topics.scmp.com/news/hk-news-watch/article/Police-chief-defends-tactics-against-protesters>.

331. Tanna Chong, "HKU [Hong Kong University] expert says protesters can sue," *South China Morning Post*, August 25, 2011. <http://topics.scmp.com/news/hk-news-watch/article/HKU-expert-says-protesters-can-sue>.

332. Joseph Li, "Police: Standard procedures applied during Li's visit," *China Daily*, August 30, 2011. [http://www.chinadaily.com.cn/hkedition/2011-08/30/content\\_13215502.htm](http://www.chinadaily.com.cn/hkedition/2011-08/30/content_13215502.htm).

333. Peter So, Stuart Lau, and Simpson Cheung, "Police chief defends tactics against protesters," *South China Morning Post*, August 19, 2011. <http://topics.scmp.com/news/hk-news-watch/article/Police-chief-defends-tactics-against-protesters>.

334. Simpson Cheng and Tanna Chong, "Comments put police chief under fresh pressure," *South China Morning Post*, September 2, 2011. [South China Morning Post, September 1, 2011. <http://www.scmp.com/portal/site/SCMP/menuitem.2af62ecb329d3d7733492d9253a0a0a0a0/?vgnnextoid=09767ba226422310VgnVCM100000360a0a0aRCRD&ss=Hong+Kong&s=News>.](http://www.scmp.com/portal/site/SCMP/menuitem.2af62ecb329d3d7733492d9253a0a0a0/?vgnnextoid=16b516d0f7522310VgnVCM100000360a0a0a0aRCRD&ss=Hong+Kong&s=News; Lai Ying-kit, )

335. Hong Kong Journalists Association, *2011 Annual Report: Two Systems Compromised, Free Expression Under Threat in Hong Kong* (Hong Kong, SAR [Special Administrative Region]: July 2011). <http://www.hkja.org.hk/site/portal/Site.aspx?id=A1-938&lang=en-US>; Beh Lih Yi, "Over 1,000 march in Hong Kong for Ai's freedom," *Agence France-Presse*, April 23, 2011. <http://www.google.com/hostednews/afp/article/ALeqM5jRr6JgrC-LjNtlkJx5AN6R84BHrw?docId=CNG.1162cc65f46ade8c93d4c3d8b3d59307.3c1>.

336. Alan Leong (Hong Kong legislative councilor and leader of the democratic Civic Party), meeting with the U.S.-China Economic and Security Review Commission, Washington, DC, July 19, 2011.

337. Kevin Drew, "Hong Kong Denies Entry to 2 Tiananmen Protesters," *New York Times*, January 26, 2011. <http://www.nytimes.com/2011/01/27/world/asia/27hong.html>.

338. Kevin Drew, "Hong Kong Denies Entry to 2 Tiananmen Protesters," *New York Times*, January 26, 2011. <http://www.nytimes.com/2011/01/27/world/asia/27hong.html>.

339. Albert Ho, chairperson of the Democratic Party of Hong Kong, letter to PRC Vice Premier Li Keqiang, August 17, 2011. <http://eng.dphk.org/?p=6691>.

340. Andrew Batson, "China Takes Aim at Dollar," *Wall Street Journal*, March 24, 2009. <http://online.wsj.com/article/SB123780272456212885.html>.

341. Rahul Jacob, "Entrepot with political attitude," *Financial Times*, September 12, 2011. <http://www.ft.com/cms/s/0/93d33e44-d71b-11e0-bc73-00144feabdc0.html#axzz1YXNp9EeK>.

342. *United States-Hong Kong Policy Act of 1992*, Public Law 102-383, 102nd Congress, 2nd sess. October 5, 1992. [http://hongkong.usconsulate.gov/ushk\\_pa\\_1992.html](http://hongkong.usconsulate.gov/ushk_pa_1992.html).



## CHAPTER 4

# CHINA'S PUBLIC DIPLOMACY INITIATIVES REGARDING FOREIGN AND NATIONAL SECURITY POLICY

### Introduction

Recent years have seen significant debate about what China's emergence as a great power means for the rest of the world.<sup>1</sup> As China's economy has grown, Chinese investments, diplomatic influence, and military presence have assumed ever more prominent international profiles. Furthermore, the emergence of a more complex field of foreign policy actors in the People's Republic of China (PRC) has brought diverse—and sometimes conflicting—institutional interests and voices into China's foreign and national security decision-making process.<sup>2</sup> (For further discussion of this topic, see chap. 3, sec. 2, of this Report, "Actors in China's Foreign Policy.")

Major questions have circulated regarding the future intentions of the Chinese state: Having achieved economic and diplomatic clout that might have seemed unimaginable a generation ago, what do China's leaders intend to do with it? And how will the steadily increasing capabilities of the People's Liberation Army (PLA) factor into future Chinese foreign policy, particularly given the PRC's growing economic interests abroad and its continuing territorial disputes with many of the countries on its periphery? In response to these questions, the Chinese government has declared itself to be focused, in the economic realm, on development and mutually beneficial trade; in the military sphere, on building an adequate self-defensive capacity and protecting its sovereignty and territorial integrity, while striving to maintain peaceful relations with its neighbors; and in international affairs, on pursuing cooperative action on issues such as climate change, terrorism, and counterproliferation.<sup>3</sup>

Other observers have questioned such messages, however, in light of China's continued backing for North Korea and its aggressive efforts to assert sovereignty over disputed territories in regions such as the South China Sea and the border with India.<sup>4</sup> Such reassurances are also called into question by scholars who describe the influence on China's leaders of zero-sum thinking about international relations,<sup>5</sup> as well as by those who identify a legacy of deception either in China's traditional strategic culture<sup>6</sup> or in the practices of the Chinese Communist Party (CCP).<sup>7</sup>

The Commission undertook efforts in 2011 to assess the nature of China's propaganda messages directed to international audi-

ences. This chapter will seek to offer greater insight into how China frames its role in the world and its relations with other countries, as well as the implications for U.S. policy in the Asia-Pacific region.

### **The Chinese Government's Formulation of Messages in Media and Public Diplomacy**

The CCP treats the control of propaganda/public diplomacy messages\* to foreign audiences as a fundamental tool of statecraft.<sup>8</sup> Furthermore, it is highly critical of what it calls the “Western media’s ideological assault on the rest of the world”<sup>9</sup> and sees itself as engaged in a “global war for public opinion.”<sup>10</sup> As an illustration of this outlook, Li Changchun, a member of the Standing Committee of the Politburo and the CCP’s most senior official in charge of the government’s ideology and propaganda system,<sup>11</sup> stated in November 2008 that:

*Communication capacity determines influence. In the modern age ... whichever nation’s communication capacity is strongest, it is that nation whose culture and core values are able to spread far and wide, and that nation that has the most power to influence the world. ... Enhancing our communication capacity domestically and internationally is of direct consequence to our nation’s international influence and international position ... and of direct consequence to the function and role of our nation’s media within the international public opinion structure.*<sup>12</sup>

The processes by which leadership messages are formulated and then transmitted through China’s informational bureaucracy are opaque. At a minimum, these decisions involve the leaders of the CCP Central Committee’s Foreign Affairs/National Security Leading Small Group (chaired since 2002–2003 by CCP General Secretary Hu Jintao) and the Propaganda and Ideology Leading Small Group (chaired since 2003 by Politburo Member Li Changchun).<sup>13</sup> As described to the Commission this year by Ashley Esarey, an academic specialist on China’s propaganda system:

*By far the most powerful decision-making body in the propaganda system overall is the Central Leading Group on Propaganda. ... This secretive body hides the extent to which it controls information in China to blunt criticism of its actions. ... Efforts to promote foreign propaganda, in particular, are managed by the CCP Central Committee Foreign Propaganda Office [whose director] concurrently serves as the Deputy Director of the [CCP] Central Propaganda Department and Director of the State Council Infor-*

\*The Chinese term for “propaganda” does not necessarily carry a pejorative meaning, and the term is used extensively in Chinese discourse. See U.S.-China Economic and Security Review Commission, *Hearing on China’s Narratives Regarding National Security Policy*, written testimony of Ashley Esarey, March 10, 2011. As defined by another expert witness, Nicholas Cull, the term “public diplomacy” is “simply the process by which an international actor conducts foreign policy by engaging a foreign public.” See U.S.-China Economic and Security Review Commission, *Hearing on China’s Propaganda and Influence Operations, its Intelligence Activities that Target the United States, and its Resulting Impacts on US National Security*, written testimony of Nicholas Cull, April 30, 2009.



*mation Office. Day-to-day supervision of foreign propaganda is handled by the State Council Information Office, which pays attention to media coverage of salient issues in foreign affairs and interacts with foreign journalists in China.*<sup>14</sup>

In pursuit of a larger voice in international affairs, Chinese media officials have significantly increased resources for state-controlled foreign language media outlets.<sup>15</sup> In 2009, the *Global Times*, an official Chinese Communist Party newspaper, launched a new English edition; and in July 2010, the Xinhua News Agency launched a global 24-hour English-language television channel titled “CNC World.”<sup>16</sup> In May 2011, Xinhua moved its North American headquarters from an office in New York City’s borough of Queens to a much more prominent location on the top floor of a skyscraper in Manhattan’s Times Square.<sup>17</sup> In addition to expanding its international news outlets, in recent years the Chinese government has sponsored increased lobbying efforts directed at U.S. policymakers.<sup>18</sup>

The Chinese government has also attempted to reach out directly to public audiences in the United States through large-scale advertising campaigns. The Chinese government sponsored commercials hailing China’s cultural achievements that appeared on television networks and in Times Square during President Hu Jintao’s official visit to the United States in January 2011.<sup>19</sup> In August 2011, the Xinhua News Agency complemented the move of its New York bureau by signing a lease of at least six years for a 60 foot by 40 foot electronic billboard on the side of 2 Times Square.<sup>20</sup> The state-owned newspaper *China Daily* has paid for “advertorial” inserts in major newspapers such as the *Washington Post* (see image below) and the *New York Times*.<sup>21</sup> The *Washington Post* has also created the *China Watch* page on its website to present further news articles provided by *China Daily*.<sup>22</sup> These articles emphasize China’s desire for a “harmonious” world;<sup>23</sup> the benefits to Americans of Chinese economic policies; and the necessity for China to maintain CCP one-party rule.<sup>24</sup> Such advertising campaigns involve a significant outlay of resources: For example, the cost of a single instance of publishing an editorial advertising insert of the type placed by *China Daily* in the *Washington Post* is approximately \$300,000, not including additional fees for any related web content.<sup>25</sup>



Despite such efforts, the Chinese government's attempt to find a more persuasive international voice may be hampered by its own misperceptions regarding foreign societies. Many Chinese officials believe that western governments direct the media in their countries to cast China in a negative light<sup>26</sup> as part of a vast campaign to contain China's emergence as a great power.<sup>27</sup> The fact that the CCP feels the need to push back with ambitious media and public diplomacy efforts against an imaginary U.S.-led international conspiracy (see box, below) is highly revealing—both of the CCP's national security worldview and of the challenges the CCP faces in successfully adapting its propaganda messages to international audiences.

### **The Chinese Communist Party and its View of the United States**

The CCP's formulation of foreign and national security narratives proceeds from the prism through which the party views the world. This outlook differs significantly from the win-win messages on international cooperation promoted by the PRC diplomatic corps and foreign language media. Domestic PRC media and internal party messages reflect a view of the outside world characterized by perceptions that China is surrounded by hostile actors. This produces a blinkered and distorted understanding of the international system as a whole and the United States in particular.

**The Chinese Communist Party and its  
View of the United States—Continued**

Despite widespread cynicism throughout Chinese society regarding Communist doctrine, Marxist social analysis is still a central element of CCP discourse,<sup>28</sup> to include traditional Marxist analysis on capitalism and imperialism: As stated in summer 2010 by an author in the *Global Times*, a newspaper controlled by the CCP Central Propaganda Department:<sup>29</sup>

*To understand the provocations made by America ... you must have a basic understanding of this country's nature and its global strategy. ... As seen from its history, America is constantly conducting war, searching for enemies, and in fact this is a normal condition of its social development. Without war, America cannot stimulate its economy. ... America is set upon a path of war from which it cannot turn back.*<sup>30</sup>

Senior PRC officials have also described the United States as an imperialist and militarist power, as when PRC Vice Premier and former Foreign Minister Qian Qichen stated in November 2004 that U.S. policy “advocates [that] the United States should rule over the whole world with overwhelming force, military force in particular.”<sup>31</sup> CCP analysis depicts the U.S. “hegemon”<sup>32</sup> as carrying out a “highly cohesive master plan designed to strengthen and expand its global domination ... this perception breeds a conspiratorial view, which in turn predisposes China to see ill intentions and sinister motives in every U.S. act.”<sup>33</sup> The United States is specifically accused of:

- Fomenting social unrest aimed at destabilizing Chinese society and overturning the government.<sup>34</sup> This narrative has been dominant since 1989, when CCP leaders blamed the Tiananmen protests on a U.S.-led plot by “hostile, reactionary foreign forces” intent on overthrowing China’s “socialist system”;<sup>35</sup>
- Intentionally bombing the PRC embassy annex in Belgrade in 1999 to intimidate and humiliate a rising China;<sup>36</sup>
- Linking U.S. overseas bases and military alliances into a “C-shaped ring of encirclement” (ranging from Japan and South Korea, down to Southeast Asia and the Indian Ocean, and up to Afghanistan) directed at containing China;<sup>37</sup>
- Making calls for China to be a “responsible stakeholder” in the international system, with the intent to weaken China by trapping it in foreign entanglements;<sup>38</sup>
- Fostering the 2008 global financial crisis in an effort to hurt China’s economic growth;<sup>39</sup>
- Pressuring China to let the renminbi (RMB) appreciate as part of a “currency war” started by “American hegemony” against China’s economy;<sup>40</sup>

**The Chinese Communist Party and its  
View of the United States—Continued**

- Conducting “hegemonistic deeds of using human rights issues to interfere in other countries’ internal affairs” and employing this as “a political instrument to defame other nations’ image and seek [the United States’] own strategic interests;”<sup>41</sup>
- Using covert means to instigate ethnic unrest in regions such as Tibet and Xinjiang, with the goal of weakening China or even causing it to break apart;<sup>42</sup> and
- Orchestrating the award of the 2010 Nobel Peace Prize to Chinese dissident Liu Xiaobo as part of an effort to embarrass China.<sup>43</sup> The PRC state press described the awarding of the prize to Mr. Liu, an “incarcerated criminal,” as “a political tool that serves an anti-China purpose . . . the Nobel committee would like to see the country split by an ideological rift, or better yet, collapse like the Soviet Union.”<sup>44</sup>

The accusations made against the United States in official PRC discourse reveal a great deal about the anxieties and distorted worldview of Chinese political elites, and the PRC’s more assertive behavior in 2010 may be explained in part by a perceived need to push back forcefully against this imagined U.S.-led “conspiracy” directed against China.<sup>45</sup> However, the centrality of the U.S. role in the international system, and the importance of the U.S. market for Chinese-made goods, means that China’s leaders continue to treat relations with the United States as “one of the most dynamic and important bilateral relations in the world,”<sup>46</sup> despite their suspicious views of American power and intentions.<sup>47</sup>

**Chinese Messages and Policy Debates on Geopolitics in East Asia and China’s Emergence as a Great Power**

CCP propaganda officials set the parameters for debate on foreign policy issues inside China and also actively promote the party’s official narratives. Over the past two decades, China’s official propaganda messages to foreign audiences have emphasized four broad themes:

1. The primacy of “stability” for China while continuing the policies of social and economic “reform and opening up” under the continued political leadership of the CCP;
2. The primacy of economic development in China’s foreign policy goals, the mutually beneficial nature of China’s economic growth for other countries, and the attractiveness of China as a destination for investment;
3. The desire to maintain a stable and peaceful international environment in order to facilitate China’s domestic development;
4. The completely defensive nature of China’s military modernization, and China’s peaceful intentions toward neighboring countries.<sup>48</sup>

Although the slogans change over time, official PRC foreign policy narratives overlap with, and do not supersede, one another. Instead, they represent shifts in message emphasis rather than changes in actual policy.

### **The Foreign Policy Guidelines of Deng Xiaoping**

Deng Xiaoping's "24-Character Strategy" first emerged in 1990 in response both to the global backlash from the 1989 Tiananmen Square crackdown and to the CCP's sense of alarm following the collapse of the communist states of Eastern Europe.<sup>49</sup> The strategy provided basic principles on how China should protect its national interests while increasing its interactions with the world. The "24-Character Strategy" has been roughly translated as:

*Observe calmly; secure our position; cope with affairs calmly; hide our capacities and bide our time; be good at maintaining a low profile; and never claim leadership.*<sup>50</sup>

Chinese officials and scholars have interpreted these policy guidelines to mean that China should avoid military rivalries; gradually grow China's comprehensive economic, military, and political strength; and minimize international responsibilities.<sup>51</sup> CCP General Secretary Jiang Zemin continued this policy throughout the 1990s, making it a central tenet of Chinese foreign policy for more than ten years. The result was that China's strategic orientation "demonstrate[d] unusual consistency from the 1980s through the 2000s," with China's leaders "insisting on the importance of sticking to Deng Xiaoping's realist legacy."<sup>52</sup>

### ***Overview of Three Leading PRC Foreign Policy Narratives***

<b>China's Global Narratives</b>	<b>Leading Spokesman</b>	<b>Year</b>	<b>Synopsis</b>
"Five Principles of Peaceful Coexistence" <sup>53</sup>	Zhou Enlai	1954	States should conduct relations with one another on an equal basis, with high regard for sovereignty and non-interference in each other's internal affairs.
The "24-Character Strategy" <sup>54</sup>	Deng Xiaoping	1990	Keep focused on domestic economic growth while avoiding the burdens of international commitments and military competition. Stay alert for efforts to subvert China through "peaceful evolution," but do not challenge western countries.
"Peaceful Rise" <sup>55</sup> —shifts to— "Peaceful Development" <sup>56</sup>	Zheng Bijian  Hu Jintao	Nov. 2003  April 2004	Remain focused on economic growth above all other priorities while pursuing peaceful integration into the international system as a great power. As above, but with less emphasis on China's emergence as a great power and greater emphasis on how China's growth benefits other countries. China will undertake selected international roles while avoiding binding commitments or military competition with other powers.



### **The Themes of “Peaceful Rise” vs. “Peaceful Development”**

The “peaceful rise” theme was unveiled by Zheng Bijian (an influential foreign policy advisor to Hu Jintao) at the Boao Forum for Asia in November 2003.<sup>57</sup> Mr. Zheng described this as a “new strategic path [of] China’s peaceful rise through independently building socialism with Chinese characteristics, while participating in rather than detaching from economic globalization.”<sup>58</sup> This theme was also articulated to international audiences through an article by Mr. Zheng published in *Foreign Affairs* in 2005 titled “China’s ‘Peaceful Rise’ to Great Power Status.”<sup>59</sup>

While the slogan of “peaceful rise” continued to circulate, by April 2004 the term had been replaced in official statements by the phrase “peaceful development,” which was confirmed as the official narrative with the release of a December 2005 government white paper titled “China’s Peaceful Development Road.”<sup>60</sup> In the white paper, the Chinese government outlined its new official foreign policy narrative as follows:

*To take the road of peaceful development is to unify domestic development with opening to the outside world, linking the development of China with that of the rest of the world, and combining the fundamental interests of the Chinese people with the common interests of all peoples throughout the world. China persists in its pursuit of harmony and development internally while pursuing peace and development externally; the two aspects, closely linked and organically united, are an integrated whole, and will help to build a harmonious world of sustained peace and common prosperity.*<sup>61</sup>

One academic expert has suggested that the change could be attributable to concerns that some neighboring countries or the United States might interpret the use of “rise” as too threatening a sign of hegemonic aspirations.<sup>62</sup> It is also possible that Hu Jintao may have wished for China’s foreign policy narrative to more closely parallel his overarching domestic propaganda theme of the “Scientific Outlook on Development.”<sup>63</sup> However, the reason for the change from “peaceful rise” to “peaceful development” is unknown.

#### **China Studies Historical Great Powers**

In debating how China should adapt to its growing economic, diplomatic, and military power, the leadership circles of the CCP have searched for answers in historical precedents, as when the Politburo undertook a “study session” in November 2003 to examine the development of major powers from the 15th to the 20th centuries.<sup>64</sup> This same theme was also on display in a major television documentary series produced on Chinese state television in 2006 titled “Rise of the Great Powers.” The documentaries catalogued the rise to great power status of Britain, France, Germany, Japan, Russia/the Soviet Union, and the United States.<sup>65</sup>

### **China Studies Historical Great Powers—Continued**

This interest in the emergence of great powers has been further influenced by traditional concepts of statecraft drawn from China's own Warring States Period (approximately 475–221 BCE), in which rising states frequently fell into conflict with dominant “hegemonic” states that sought to protect their position by striking out at the challengers.<sup>66</sup> Chinese leaders also reportedly have been alarmed by parallels comparing China's rise in the late 20th century with that of Imperial Germany in the late 19th/early 20th century and the attendant arms race and geopolitical competition that ensued between Germany and Great Britain—the dominant “hegemon” of the international system in the early 20th century.<sup>67</sup>

Therefore, the PRC has embarked on an active propaganda/public diplomacy campaign to reassure audiences in other states—and most particularly policymakers in the United States, the “hegemon” of the current international order—that China has no intent either to threaten its neighbors or to upset the international system.<sup>68</sup> Singapore's “Minister Mentor” Lee Kuan Yew noted this informational campaign in an interview in October 2007, when he made reference to the “Rise of the Great Powers” television series. Mr. Lee stated that the Chinese government intended the series to be “a lesson to support their gradual opening up and their idea of how they can do it without conflict—the ‘peaceful rise.’ They have worked out this scheme, this theory, this doctrine to assure America and the world that they're going to play by the rules.”<sup>69</sup>

### **The Path of “Peaceful Development” in 2010–2011**

China adopted a much more assertive international profile in 2010, to include actions such as harassing U.S. survey vessels operating in international waters off the Chinese coast, aggressively pressing unrecognized territorial claims in the East and South China Seas, and supporting North Korea in the aftermath of unprovoked acts of aggression against South Korea.<sup>70</sup> This behavior has unnerved neighboring countries and undone much of China's goodwill diplomacy of the past decade.<sup>71</sup> Alongside these provocative actions, the messages emerging from China about its foreign and national security policy were also in a state of flux over the past year, as new policy directions were debated and a more diverse group of PRC foreign policy actors promoted their views.<sup>72</sup>

The themes of “peaceful development,” along with parallel messages on seeking a “harmonious” international environment,<sup>73</sup> continue to dominate official PRC foreign policy messages. These messages grew even more emphatic in late 2010 and early 2011, voiced in prominent fora by very senior PRC officials, a possible sign of public diplomacy damage control undertaken in reaction to the backlash that China faced over its aggressive behavior in 2010. In a speech to the United Nations (UN) General Assembly on September 23, 2010, Premier Wen Jiabao stated that:

*China will stay firmly committed to peaceful development.  
You may ask what is the essence of peaceful development?*

*It is to foster a peaceful international environment for our development and at the same time contribute to world peace through our development. ... China's development will not harm anyone or pose a threat to anyone. There were powers who sought hegemony once they grew strong. China will never follow in their footsteps.*<sup>74</sup>

This was followed by a December 2010 article in the English-language *Beijing Review* by PRC State Councilor Dai Bingguo titled “Stick to the Path of Peaceful Development.”<sup>75</sup> As described in testimony to the Commission by John Park of the U.S. Institute of Peace:

*With over 60 references to ‘peace’ and an explicit assurance that ‘China has no culture or tradition of seeking expansion or hegemony’ and that ‘benevolence and harmony are at the heart of our political and cultural tradition, which values harmony, good-neighborliness and friendship with all’ throughout its thousands of years of history, Dai’s article appeared to be conspicuously overcompensating for the events and statements of a summer that seemed to confirm many countries’ suspicions about the nature of China’s rise.*<sup>76</sup>

In a similar vein, in January 2011, PRC Vice Premier and Politburo Standing Committee Member Li Keqiang, the likely successor to Wen Jiabao as state premier, published an op-ed in the *Financial Times* titled “The World Need Not Fear a Growing China.” In the article, Mr. Li strongly asserted “China’s pursuit of the path of peaceful development,” its desire for “harmonious relations with our neighbours,” and China’s contributions to world economic growth.<sup>77</sup>

Prominent PRC academics have also been engaged in the PRC’s redoubled efforts at strategic reassurance. Wang Jisi, dean of the School of International Studies at Beijing University, asserted in a February 2011 *Foreign Affairs* article that China would continue to adhere to nonconfrontational policies as it emerged as a major world power. He explained away China’s more abrasive foreign policy actions in 2010, writing that:

*In recent years, China’s power and influence relative to those of other great states have outgrown the expectations of even its own leaders. Based on the country’s enhanced position, China’s international behavior has become increasingly assertive. ... Last year, some Chinese commentators reportedly referred to the South China Sea and North Korea as [‘core interests’], but these reckless statements, made with no official authorization, created a great deal of confusion. ... As long as no grave danger ... threatens the CCP leadership or China’s unity, Beijing will remain pre-occupied with the country’s economic and social development, including in its foreign policy.*<sup>78</sup>

These more moderate views of Wang Jisi—which could reasonably be interpreted as the official message that China’s leaders hope that international audiences will believe<sup>79</sup>—are directed in large part to policymakers and public opinion in the United States,

a result of the uncertainty and anxiety that CCP leaders feel about U.S. strategic intentions toward China.<sup>80</sup>

Although the general narrative framework of the PRC's foreign propaganda is unlikely to change in the near term, the emergence in 2012 of a new Central Committee and Politburo leadership following the Eighteenth Party Congress may produce new slogans, and possibly modified explanatory language, to reflect the public diplomacy priorities of the CCP's new leadership circle.

### **Should “Peaceful Development” Be Taken at Face Value?**

Some expert witnesses who testified before the Commission this year raised concerns that the PRC's official messages may be a deceptive cover for revisionist PRC foreign policy goals. Gilbert Rozman of Princeton University testified that “[t]here [has been] a calculated duality to Chinese writings. Has the Chinese narrative been intentionally deceptive? I think so . . . Having closely followed Chinese works [I believe] that positions taken in 2010 that are at variance with earlier positions are a result of prior concealment of China's attitudes.”<sup>81</sup> This opinion was also reflected in the testimony of Jacqueline Newmyer Deal of the Long Term Strategy Group, who told the Commission that:

*The Chinese government prioritizes manipulating information more than most Americans realize and perhaps more than any other major power. My analysis indicates that Chinese elites manage to deliver a range of messages tailored to American audiences that could have the effect of encouraging us to act, or in some cases refrain from acting, in ways that serve Chinese interests at the expense of U.S. interests or broader international norms.*<sup>82</sup>

The testimonies of Dr. Rozman and Dr. Newmyer Deal are supported by limited anecdotal evidence available from within the Chinese Communist Party itself. In early 2011, lecture notes taken at the CCP's Central Party School were leaked on the news website *China Digital Times*. According to the notes of this anonymous official, Central Party School lecturers told their students that the relationship between the CCP and “American imperialism” was one of “strategic adversaries” and that “the so-called cooperative partnership is deceptive.”<sup>83</sup>

If there is a disparity between what the Chinese government says to different audiences about China's rise as a great power, it is not surprising: The CCP informational bureaucracy has long held an “insider” and “outsider” view of access to information, as this pertains both to non-Chinese Communist Party members and to foreigners.<sup>84</sup> The CCP has a deeply ingrained institutional culture favoring secrecy<sup>85</sup> and a long history of proactively using information to promote the party's objectives while suppressing information deemed harmful to its interests.<sup>86</sup> China's leaders have selected the reassuring message of “peaceful development” as the public diplomacy narrative that they believe to be most advantageous to China's interests as well as the one that most accords with their self-image of China as “a force for stability and peace.”<sup>87</sup> However, the extent to which this optimistic narrative may diverge

from the CCP's actual view of international relations, and from China's longer-term policy goals, remains an open question.

### **The “Shanghai Spirit”**

In June 2011, on the tenth anniversary of the founding of the Shanghai Cooperation Organization (SCO), the Chinese media began to extol the institution's “Shanghai Spirit” as the embodiment of a new model of international relations. According to an article published in English by PRC Foreign Minister Yang Jiechi:

*The SCO embodies ... the ‘Shanghai Spirit’ whose essence is mutual trust, mutual benefit, equality, consultation, respect for diverse civilizations and seeking common development. It reflects the member states’ fresh perspectives on security, development, cooperation and civilization. An inspiration to the world, it is a major contribution to efforts to foster a new type of state-to-state relations and build a harmonious region.*<sup>88</sup>

Material published in Chinese is more revealing as to why the Chinese government holds up the SCO as its preferred model for an international organization. In thinly veiled code language referring to the threat allegedly posed by the United States and other western governments, the *People's Daily* has written that:

*The SCO supports the democratization of international relations, actively advancing the building of a new international order. In our world, although the Cold War is over, the paths of unilateralism and new interventionism are still prevalent; the ‘Superiority of Western Civilization,’ ‘Democratic Reform,’ and other such concepts still threaten the balanced and stable development of international politics.*<sup>89</sup>

In contrast to other institutions that “the PRC had little role in creating and had to join on a take-it-or-leave-it basis, Chinese officials have been able to shape the design and evolution of the SCO more than any other country ... allowing the Chinese to construct the SCO as an institution that reflects their preferred values.”<sup>90</sup> Such values include “full respect for independence, sovereignty and territorial integrity, as well as upholding the principle of non-interference in internal affairs of all states;” and “democratic development with due regard for [members’] national realities as well as cultural historical features.”<sup>91</sup> They also include “democratizing international relations”—that is, excluding from participation the “hegemonic” United States and its allies, who have historically played a prominent role in international institutions. (For further discussion of the increasingly influential role of China in international organizations, see the March 2011 contracted research report, “The Evolving Role of China in International Institutions,” available on the Commission's website at [www.uscc.gov](http://www.uscc.gov)).



### **The Chinese Government's Messages Related to China's Military Modernization and Defense Policies**

In referring to China's military modernization and its national security policies, Chinese writings consistently assert China's peaceful military tradition and its rejection of "hegemony" and "power politics." Chinese messages often contrast the Chinese military tradition with that of the West, which they characterize as violent and expansionist.<sup>92</sup> Notably, since 2005 PRC messaging has made particular use of the story of the 15th century Ming Dynasty maritime explorer Zheng He, stressing the theme that China's naval expansion will be peaceful in nature and beneficial to surrounding countries.<sup>93</sup>

All of these themes have figured prominently in official PRC policy documents intended for foreign audiences. As stated in China's 2010 defense white paper:

*The pursuit of a national defense policy which is defensive in nature is determined by China's development path, its fundamental aims, its foreign policy, and its historical and cultural traditions. [China] promotes the building of a harmonious world enjoying lasting peace and common prosperity externally [and] maintains ... its belief in valuing peace above all else, advocating the settlement of disputes through peaceful means, prudence on the issue of war, and the strategy of 'attacking only after being attacked.' China will never seek hegemony, nor will it adopt the approach of military expansion now or in the future, no matter how its economy develops.<sup>94</sup>*

These messages have also been promoted in U.S.-China military-to-military exchanges. In May 2011, General Chen Bingde, the chief of the People's Liberation Army (PLA) General Staff Department and a member of the 17th CCP Central Committee,<sup>95</sup> led a 24-member delegation to the United States to restart high-level military exchanges that the PRC had halted following U.S. military sales to Taiwan in October 2008 and January 2010.<sup>96</sup>

In an address at the National Defense University in Washington, DC, General Chen offered statements consistent with the messages on foreign policy and national security issues that the Chinese government promotes to foreign audiences: Foremost, that China has a peaceful military tradition and poses no threat to its neighbors, and that it is focused on promoting a peaceful external environment to allow for its own domestic economic development. General Chen repeatedly stressed the capabilities gap between the Chinese and U.S. armed forces and that China has no intent to challenge U.S. military superiority or the U.S. position in the international system. He also stressed the prospects for security cooperation between the United States and China on transnational issues such as terrorism, piracy, and counterproliferation. However, General Chen attached conditions to closer military-to-military ties—in particular, the need for the United States to "respect" China's "core interests," especially in regard to Taiwan.<sup>97</sup> (For a fuller discussion of General Chen's visit and the issues surrounding it, see the USCC backgrounder "The Chinese People's Liberation Army Dele-

gation Visit to the United States, May 2011: A Summary of Key Actors and Issues,” available on the USCC website at [www.uscc.gov](http://www.uscc.gov).)

### What Constitutes a “Core Interest” of China?

The term “core interests” has been invoked by PRC officials and state media in reference to multiple policy areas, and the use of the term has increased dramatically from 2008 to the present.<sup>98</sup> The phrase has been used most commonly in regard to issues of national sovereignty but has also been invoked in relation to economic development, “social stability,” and territorial integrity.<sup>99</sup> According to one author writing in an authoritative CCP forum, “National core interests are a country’s paramount interests, related to the life or death of a country and its people. Therefore, in international contacts and negotiations one cannot yield, and there is no room for compromise.”<sup>100</sup>

At the close of the first round of the Strategic and Economic Dialogue in July 2009, PRC State Councilor Dai Bingguo described China’s “core interests” as follows:

*To ensure that our bilateral relationship will move forward on the track of long-term and sound development, a very important thing is that we need to support, respect, and understand each other, and to maintain our core interests. And for China, our concern is we must uphold our basic systems,\* our national security; and secondly, the sovereignty and territorial integrity; and thirdly, economic and social sustained development.*<sup>101</sup>

Despite such comments, Beijing has not made clear which issue areas merit classification as a “core interest.” In past years, the term was used primarily to denote sovereignty issues—particularly in regard to Taiwan, Tibet, and Xinjiang.<sup>102</sup> However, the term was used more expansively by PRC officials throughout 2010–2011. In May 2010, Mr. Dai told Secretary of State Hillary Rodham Clinton that the South China Sea represented one of China’s “core interests”;<sup>103</sup> this was followed in July 2010 by a PRC Defense Ministry spokesman who stated that “China has indisputable sovereignty of the South [China] Sea.”<sup>104</sup> In the ensuing international controversy, PRC officials backed away from the explicit assertion that the region qualified as a “core interest” but did not withdraw the claim.<sup>105</sup>

\*The context of Mr. Dai’s remarks indicates that by “basic systems” he meant China’s current political order—i.e., the continued rule of the CCP. Jin Canrong, a professor at Renmin University, has written that Mr. Dai’s term “basic system” refers to China’s system of “multiparty cooperation and political consultation led by the Communist Party of China.” See *Global Times Online* (in English), “China Denies Taking Tough Stance on International Affairs,” March 8, 2010. <http://www.globaltimes.cn/china/diplomacy/2010-03/510467.html>.

**What Constitutes a “Core Interest” of China?—Continued**

Additionally, PRC officials and media have become more vocal in protesting U.S. actions that “touch upon” China’s “core interests.” These include arms sales to Taiwan<sup>106</sup> as well as pressure to revalue the renminbi (RMB), which “would harm Chinese policymakers’ core interest of managing the economic wellbeing of the Chinese people.”<sup>107</sup> The term has also been invoked in reference to foreign criticism of China’s human rights practices, as when CCP General Secretary Hu Jintao referred in November 2006 to “Taiwan, Tibet, human rights and other major questions involving China’s state sovereignty and core interests.”<sup>108</sup>

Confusing messages regarding what qualifies as a “core interest” of China may reflect a lack of consensus among competing voices in the PRC foreign policy process. (For further discussion of this topic, see chap. 3, sec. 2, of this Report, “Actors in China’s Foreign Policy.”) However, it also reflects a growing assertiveness on the part of PRC foreign policy decisionmakers, who feel that China’s rise into the ranks of great powers gives it the necessary clout to reshape international practices to which it objects:

*[I]f a country’s identity changes as its power grows, it may cease to accept another party’s policies and behavior, although the country may have swallowed the bitter fruit in the past ... with the growth of China’s power and [the] Chinese people’s growing attention to foreign affairs, China cannot accept some behaviors such as arms sales to Taiwan, which has been done for decades. However ... the offensive taken by China is not a move of expansion. In fact, Beijing’s offensive strategy on arms sales to Taiwan is a small step of counterattack after its core national interest has been infringed repeatedly and for decades.<sup>109</sup>*

Such a sense of China’s increasing power, tied to a deep sense of grievance regarding China’s historical treatment at the hands of foreign powers,<sup>110</sup> suggests that PRC officials will prove increasingly expansive and assertive in how they choose to define the list of China’s “core interests.”<sup>111</sup>

**China’s “Defensive” Military Tradition**

Authoritative PRC military commentators consistently declare that China maintains a purely defensive military orientation and that this is the continuation of a long historical legacy: “The Chinese nation has a time-honored tradition of loving peace. In the history of military development over thousands of years, it always pursued a defensive type of military strategy.”<sup>112</sup> However, some scholars of historical Chinese statecraft have identified a real-politik readiness to use military force in the pursuit of state interests, thinly veiled beneath official rhetoric on peace and benevolence.<sup>113</sup> Andrew Scobell, senior political scientist at the RAND

Corporation, has described the result as a dualistic Chinese strategic culture that “paradoxically tends to dispose Chinese leaders to pursue offensive military operations as a primary alternative in pursuit of national goals, while rationalizing these actions as being purely defensive and last resort.”<sup>114</sup> One example of this thinking is PRC discourse on China’s 1979 invasion of Vietnam, which is invariably referred to as a “self-defensive counterattack” made in response to Vietnamese provocations.<sup>115</sup>

More recently, the PRC’s assertion of a peaceful, defensive military posture has also been questioned due to increasing Chinese aggressiveness in asserting sovereignty claims in areas such as the South China Sea,<sup>116</sup> as well as to its increasing development of capabilities for strike warfare.\* Many of China’s neighbors in East Asia are hedging against the possibility of China’s future intentions being less peaceful than its narratives would attest, as is revealed in the most recent Japanese and Australian defense white papers<sup>117</sup> and in summer 2011 exercises conducted between the U.S. Navy and naval vessels from the Philippines and Vietnam.<sup>118</sup> These same concerns have also been displayed in South Korea’s efforts to strengthen its security alliance with the United States following attacks from North Korea and the subsequent moves taken by the PRC to shield Pyongyang from any serious repercussions for its actions.<sup>119</sup>

### Nationalist Rhetoric from the PLA Officer Corps

The peaceful prospects of China’s military modernization have also been called into question by hawkish comments from senior PLA officers that clash with the official themes advocating peaceful economic development and international cooperation.<sup>120</sup> One of the most high-profile examples from the past year was provided by General Liu Yuan, the political commissar of the PLA General Logistics Department, and the son of former PRC head of state Liu Shaoqi.<sup>121</sup> General Liu has emerged as a prominent voice among the group of “princelings”—the children of high-ranking CCP officials—who extol the virtues of the party’s past.<sup>122</sup>

General Liu has accused unnamed CCP leaders of selling out the country to foreign interests<sup>123</sup> and has called upon party members to embrace revolutionary-era communist values, described as a return to “New Democracy.”<sup>124</sup> General Liu’s comments are evocative of the worrisome trend of a “Maoist revival” in some quarters of the CCP, with calls for assertive nationalism, a return to Marxist ideological orthodoxy, reinforced state control over the economy, and harsher repression of dissent.<sup>125</sup> General Liu has also praised war as a unifying and progressive force in Chinese history,<sup>126</sup> writing that “[t]he state is an apparatus for the use of force, forged for vio-

\* Strike warfare is defined as “operations to destroy or neutralize enemy targets ... including attack against strategic and tactical targets such as manufacturing facilities and operating bases from which the enemy is capable of conducting or supporting air, surface, or subsurface operations against friendly forces.” See U.S. Department of Defense, *Joint Publication 3-04: Doctrine for Joint Maritime Operations (Air)* (Washington DC: July 1991), p. GL-5. [http://edocs.nps.edu/dodpubs/topic/jointpubs/JP3/JP3\\_04\\_910731.pdf](http://edocs.nps.edu/dodpubs/topic/jointpubs/JP3/JP3_04_910731.pdf). For a discussion of the PLA’s increasing capabilities for strike warfare operations, see U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2010).

lence; history is written in massacres and blood sacrifices, and new civilizations and new cultures often have their origins in warfare.”<sup>127</sup>

General Liu’s extreme language is not an authoritative reflection of Chinese government policy. However, General Liu is a rising figure in the PLA and enjoys the favor of Xi Jinping, who is on track to assume the role of paramount CCP leader in 2012.<sup>128</sup> Mr. Xi is himself a princeling—the son of former PRC Vice Premier Xi Zhongcun—and has been described as a staunch supporter of promoting fellow princelings to senior government positions.<sup>129</sup> The two men are also believed to share an orthodox interpretation of Communist ideology.<sup>130</sup> Some expert observers of Chinese politics believe that Mr. Xi is laying the groundwork for General Liu to be appointed as a vice chairman of the CCP Central Military Commission at the 18th CCP Party Congress in autumn 2012.<sup>131</sup> If this were to prove true, it would make General Liu one of the two most senior officers in the PLA, as well as its highest-ranking political commissar<sup>132</sup>—thereby giving him a powerful platform for shaping both the military’s internal political indoctrination as well as the messages that the PLA promotes beyond the ranks.

General Liu also is not isolated in his views, as provocative nationalist commentary from PLA officers became more prominent throughout 2010 and 2011.<sup>133</sup> In one such example, in May 2010 a U.S. delegation in Beijing received an angry, three-minute lecture from Rear Admiral Guan Youfei, deputy director of the Foreign Affairs Office in the PRC Defense Ministry. Admiral Guan lambasted the United States for treating China as an enemy (as proven by arms sales to Taiwan); for being a bullying “hegemon” of the international system; and for plotting to encircle China with strategic alliances.<sup>134</sup> Such commentary from senior-ranking officers has generated concerns that nationalist impulses within the PLA may be driving more aggressive behavior in PRC foreign policy<sup>135</sup> or that elements of the PLA may be acting in a “roguish” fashion outside of full civilian control.<sup>136</sup> It has also contributed to concerns that political and personnel changes underway in the lead-up to the 18th CCP Party Congress in autumn 2012 could serve to boost the political influence of the PLA and amplify nationalist voices in the PRC’s foreign policy decision-making process.<sup>137</sup>

### **Track Two Exchanges and PRC Messages Regarding Military and National Security Policy**

There are many “track two” exchanges between U.S. and Chinese host institutions, which bring together scholars and former government officials to discuss diplomatic, security, and economic topics of concern to both countries.\* Additionally, a number of “track 1.5” exchanges have also appeared in recent years, which involve gov-

\* “Track two” diplomatic exchanges are those that take place between representatives of non-governmental groups (think tanks, academics, retired senior political figures, or military officers, etc.) who may nonetheless be in a position to relay the results to active policymakers or to otherwise influence government policy or public opinion in regard to particular issues in foreign relations. See Dalia Dassa Kaye, *Talking to the Enemy: Track Two Diplomacy in the Middle East and South Asia* (Santa Monica, CA: RAND Corporation, 2007).



ernment officials conducting discussions in an unofficial capacity.\* Such exchanges have come to occupy a prominent place in U.S.-Chinese relations as conducted outside of formal government channels. For example, from 2002–2008 the Institute for U.S.-China Issues at the University of Oklahoma conducted annual meetings of “The Sino-American Security Dialogue” in partnership with Chinese academic institutions; this subsequently changed to the “US–China Diplomatic Dialogue” for mid-career U.S. and Chinese diplomats, which last met in summer 2011 in Anhui, China.<sup>138</sup>

Track two exchanges offer many potential benefits, to include greater mutual understanding and the opportunity for discussion of contentious topics outside of the restrictions of official diplomatic channels. However, the representatives of PRC friendship associations and think tanks are not independent actors: Virtually all are subordinate to a government ministry or Communist Party body,<sup>139</sup> and their personnel appointments are dependent upon CCP vetting and approval.<sup>140</sup> Therefore, such exchanges also offer opportunities for Chinese government-controlled front organizations to reinforce official propaganda messages and to conduct subtle perception management efforts under the guise of nominally independent person-to-person and scholarly exchanges.

The Commission’s examination of this issue revealed a prominent role for PRC intelligence entities in organizing and hosting track two exchanges. For example, one prominent Chinese sponsor of exchange trips and dialogues is the China Association for International Friendly Contact (CAIFC), which is a front organization for the International Liaison Department of the PLA General Political Department.<sup>141</sup> The International Liaison Department performs dual roles of intelligence collection and conducting PRC propaganda and perception management† campaigns, particularly in the case of efforts focused on foreign military forces.<sup>142</sup>

\*According to a definition provided by the Berghof Foundation for Conflict Studies, a Danish think tank, track 1.5 exchanges involve “informal dialogue and problem-solving formats with high ranking politicians and decision-makers. Involves Track 1 participants, but employs Track 2 approaches.” See Berghof Foundation for Conflict Studies. “Glossary: Track 1.5,” <http://www.berghof-foundation.de/en/glossary/track-1.5>.

†The term “perception management” has been defined by the Department of Defense as follows: “Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator’s objectives.” See U.S. Department of Defense, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: April 2001 [as amended through October 31, 2009]), p. 411.

<b>Selected CAIFC/CPD Track Two Exchanges with Government Officials and Think Tank Scholars in 2009–2010</b> <sup>143</sup>	
<p>In addition to activities that it sponsors directly, the Chinese Association for International Friendly Contact also operates its own associated think tank, the Center for Peace and Development (CPD).<sup>144</sup> Not counting the extensive number of programs run by other Chinese organizations, the CAIFC and CPD conduct a very active list of exchanges. A list of selected exchanges sponsored by CAIFC and/or CPD from the years 2009–2010 includes the following:</p>	
<b>Dates</b>	<b>Participating Foreign Organization(s)/Person(s) and Issues Discussed (If Known)</b>
June 27–July 9, 2010	A delegation from CAIFC meets in Washington, DC, with Members of Congress and representatives of the Asia Society and the Center for Strategic and International Studies, among others. They also meet in New York with faculty at Columbia University. Topics discussed reportedly focused on U.S. and Chinese policy in Central Asia.
June 15, 2010	CAIFC hosts a visit to China by the governor of Hawaii and an accompanying delegation from the Hawaii Chamber of Commerce.
April 4–13, 2010	CAIFC sponsors a delegation of five former Members of Congress to visit China; in Beijing, they visit the National People's Congress, the Ministry of Foreign Affairs, the Ministry of Commerce, and the People's Bank of China.
November 25, 2009	CPD hosts a visiting delegation from Britain's Royal United Services Institute for Defence and Security Studies. Topics discussed reportedly included Chinese-European relations, Afghanistan, and the Iranian nuclear program.
October 16–24, 2009	In the second round of meetings of the "Sanya Initiative," <sup>145</sup> a delegation of retired Chinese generals visits the United States. They visit U.S. Pacific Command headquarters in Honolulu; and subsequently travel to Washington, D.C., where they meet with Secretary of State Hillary Rodham Clinton, Vice Chairman of the Joint Chiefs General James Cartwright, and members of the China Working Group caucus of the U.S. House of Representatives.
May 19, 2009	CAIFC representatives, including former Foreign Minister Li Zhaoxing, entertain a visiting delegation of senior-ranking retired Japanese military officers at the Diaoyutai Guest House in Beijing.
May 15, 2009	Hosted by CAIFC, a delegation from the Asia-Pacific Center for Security Studies visits the Ministry of Foreign Affairs, the China Institute of International Studies, the Chinese Academy of Social Sciences Institute of American Studies, and Qinghua University.
April 8–18, 2009	A delegation of CAIFC representatives travels to Washington State to meet with state political and business leaders and subsequently to Washington, DC, for discussions at The Brookings Institution and the Center for Strategic and International Studies.

Despite concerns raised by the sponsorship role of Chinese intelligence and Communist Party-controlled entities—and their role as conduits for propaganda messages targeted at foreign elites—many U.S. participants involved with track two exchanges have emphasized the value of dialogue with PRC state-controlled think tanks and other like bodies, noting that these discussions offer insights into the policy positions favored by the government parent organization.<sup>146</sup> In testimony before the Commission this year, Abraham

Denmark, a senior fellow at the Center for a New American Security, defended track two exchanges with Chinese interlocutors as “an invaluable source of information,” as well as an avenue for building contacts and communication with Chinese foreign policy thinkers.<sup>147</sup> The Commission itself has met on multiple occasions for discussions with representatives of Chinese think tanks, to include those operated by intelligence entities. For example, in July 2010 members of the Commission met in Beijing with representatives of the China Institute for International Strategic Studies (operated by PLA military intelligence<sup>148</sup>) and the China Institute of Contemporary International Relations (a branch of the Ministry of State Security, China’s leading civilian intelligence service<sup>149</sup>).

### Implications for the United States

The official foreign policy narrative of the Chinese government expresses its desire for a peaceful and “harmonious” international environment as well as for economic growth that benefits China and the rest of the world. If true, this offers hope for exchanges between the United States and China that could produce a mutually beneficial trade relationship, avoid military competition, and bring about cooperative efforts on pressing international issues such as piracy, counterproliferation, and global climate change.

However, multiple messages are emerging from China regarding its place in the world, and some of these messages conflict with the official ones. All governments seek to present their policy choices in the most favorable light and frequently may claim high-minded justifications for actions motivated by *realpolitik* interests. However, the case may be particularly serious in relation to China: Although China’s diplomats and informational bureaucracy speak to international audiences in terms of mutually beneficial cooperation, Chinese domestic discourse reveals a profound distrust of the United States and a focus on approaches that favor China’s state interests regardless of the effects on other countries.

This disparity in external and internal messages, as well as between China’s words and deeds as observed in 2010 and 2011, carries with it troubling implications. If China’s leaders are presenting reassuring messages to the outside world for public relations purposes while actually implementing a contrary set of revisionist and self-interested policies, this bodes ill for policy initiatives that proceed from *prima facie* acceptance of stated PRC intentions. It could also portend increased security competition in Asia: By themselves, reassuring Chinese statements about a “harmonious” international order will prove unconvincing to neighboring states alarmed by China’s military buildup and its aggressive behavior in disputed maritime territories.

### Conclusions

- The Chinese government places a high priority on the management of information as a tool of policy, to include the messages that it promotes to international audiences regarding its goals in foreign and national security policy. The central leadership of the Chinese Communist Party selects official foreign policy messages intended to support state policy goals. These messages are then

disseminated through diplomatic channels, state-controlled media, advertising, and “track two” exchanges.

- The Chinese government’s official narratives stress China’s desire for mutually beneficial “peaceful development” and for a “harmonious” international environment that will allow China to focus attention and resources on its economic and social development. China’s statements on its defense policies emphasize that they are entirely defensive in nature and that China will never pose a threat to any of its neighbors.
- There are notable differences between the optimistic character of China’s official messages on national security policy, which stress prospects for international cooperation, and the nature of its domestic discourse, which portrays the United States as a dangerous and predatory “hegemon” of the international system.
- The Chinese government frequently discusses important policy issues in terms of China’s “core interests,” accompanied by an insistence that other countries accept the PRC’s non-negotiable positions on these issues. However, conflicting statements from different parts of the Chinese government leave it unclear as to exactly which issues fall into the category of a “core interest.” In order to prevent misunderstandings with the United States and other countries that could have serious diplomatic consequences, Beijing should clarify which issues it sees as truly representing a “core interest.”
- The emergence of a more outspoken field of PRC foreign policy actors has produced messages that are sometimes at variance with official government narratives. This is particularly true of nationalist voices within the Chinese military.
- The Chinese government makes extensive use of front organizations. Congress and the American public often are not aware that nominally private civic organizations in China that purport to have educational, cultural, or professional purposes are frequently controlled by military, intelligence, or Communist Party organs. These front organizations are used to advance PRC state interests while disguising the guiding role of the government.

## **RECOMMENDATIONS**

The Commission recommends that:

- Congress evaluate the effectiveness of U.S. government public diplomacy programs in the East Asian region.
- Congress urge the administration to seek clarification on the Chinese government's views as to what represents a "core interest" as well as what this formulation means for U.S.-China relations, and the implications for U.S. allies and friends.
- Congress ensure that its own Members are made fully aware of the Chinese institutional actors engaged in exchange programs involving officials of the U.S. Government.



## ENDNOTES FOR CHAPTER 4

1. As one prominent example of the debate between international relations scholars about what the rise of China as a great power means for the United States and the rest of the world, see John Mearsheimer and Zbigniew Brzezinski, "Clash of the Titans," *Foreign Policy* 146 (January/February 2005).

2. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of David Lampton, March 10, 2011. See also Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute, Policy Paper No. 26, September 2010). <http://books.sipri.org/files/PP/SIPRIPP26.pdf>.

3. Cheng Bingde, "Speech presented at the U.S. National Defense University" (Washington, DC, May 18, 2011). Notes taken by USCC staff. Many Chinese academics have reinforced these positive messages, and their writings have found a supportive audience among many distinguished American scholars of Chinese affairs. As an example, see Wang Jisi, "A Rising Great Power Finds its Way," *Foreign Affairs* (March/April 2011); and the comments on Dr. Wang's article in U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of David Lampton, March 10, 2011. For further arguments providing an optimistic view of the rise of China and of future U.S.-China relations, see John Ikenberry, "The Rise of China and the Future of the West; Can the Liberal System Survive?" *Foreign Affairs* (January/February 2008).

4. For two such examples, see Aaron Friedberg, "Hegemony with Chinese Characteristics," *National Interest* (July-August 2011); and John Mearsheimer, "The Gathering Storm: China's Challenge to US Power in Asia," *The Chinese Journal of International Politics* 3 (2010).

5. Michael Pillsbury, *China Debates the Future Security Environment* (Honolulu, HI: University Press of the Pacific, 2005).

6. Gilbert Rozman, *Chinese Strategic Thought Toward Asia* (New York, NY: Palgrave MacMillan, 2010), p. 4. For a further survey on trends in Chinese strategic culture, see Eric C. Anderson and Jeffrey G. Engstrom, *China's Use of Perception Management and Strategic Deception* (research report prepared by Science Applications International Corporation on behalf of the U.S.-China Economic and Security Review Commission, November 2009). <http://www.uscc.gov/researchpapers/2009/ApprovedFINALSAICStrategicDeceptionPaperRevisedDraft06Nov2009.pdf>. See also Alastair Iain Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History* (Princeton, NJ: Princeton University Press, 1995); Andrew Scobell, *China's Use of Military Force: Beyond the Great Wall and the Long March* (New York, NY: Cambridge University Press, 2003); and Thomas G. Mahnken, "Secrecy and Stratagem: Understanding Chinese Strategic Culture" (Sydney, Australia: Lowy Institute for International Policy, 2011), <http://www.lowyinstitute.org/Publication.asp?pid=1515>.

7. "Like communist and revolutionary parties throughout history, formed and nurtured by underground cells and violent conflict with the regimes they sought to overthrow, the Party in China is secretive by habit and inclination." Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York, NY: Harper Collins, 2010), p. 20. See also U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), pp. 297-298.

8. For discussion of this concept, see U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2009), pp. 292-293.

9. U.S.-China Economic and Security Review Commission, *Hearing on China's Propaganda and Influence Operations, Its Intelligence Activities that Target the United States, and the Resulting Impacts on U.S. National Security*, written testimony of Anne-Marie Brady, April 30, 2009.

10. David Bandurski, "Li Changchun on the Media and China's 'Global Influence'" (Hong Kong, SAR [Special Administrative Region]: China Media Project). <http://cmp.hku.hk/2009/01/19/1457>.

11. Anne-Marie Brady, "Guiding Hand: The Role of the CCP Central Propaganda Department in the Current Era" (London, United Kingdom: University of Westminster, *Westminster Papers in Communication and Culture*, 2006).

12. Li Changchun, speech made on the occasion of the fiftieth anniversary of China Central Television. See David Bandurski, "Li Changchun on the Media and China's 'Global Influence'" (Hong Kong, SAR [Special Administrative Region]: China Media Project). <http://cmp.hku.hk/2009/01/19/1457>.

13. Alice Miller, “The CCP Central Committee’s Leading Small Groups,” *China Leadership Monitor* 26 (Fall 2008). <http://www.hoover.org/publications/china-leadership-monitor/article/5689>.

14. U.S.-China Economic and Security Review Commission, *Hearing on China’s Narratives Regarding National Security Policy*, written testimony of Ashley Esarey, March 10, 2011. Note that “the Office of Foreign Propaganda, which is more commonly known by its other nameplate, the State Council Information Office, oversees matters relating to external propaganda. The two bureaucracies are closely linked and coordinated.” See U.S.-China Economic and Security Review Commission, *Hearing on China’s Propaganda and Influence Operations, Its Intelligence Activities that Target the United States, and the Resulting Impacts on U.S. National Security*, testimony of Anne-Marie Brady, April 30, 2009.

15. For a fuller discussion of this phenomenon, see U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2009), pp. 294–297.

16. U.S.-China Economic and Security Review Commission, *Hearing on China’s Narratives Regarding National Security Policy*, written testimony of Gary D. Rawnley, March 10, 2011; and Xinhua News Service (in English, “Xinhua Launches CNC World English Channel,” July 1, 2010. <http://news.xinhuanet.com/english/2010/china/2010-7/01/cG7<13378575.htm>.

17. Xinhua News Service (in English), “Xinhua Opens New Office in NYC’s Time Square,” May 20, 2011. [http://news.xinhuanet.com/english/2010/business/2011-05/20/c\\_13884252.htm](http://news.xinhuanet.com/english/2010/business/2011-05/20/c_13884252.htm); and Stuart Elliott, “Sign of Arrival, for Xinhua, Is 60 Feet Tall,” *New York Times*, July 25, 2011.

18. For discussion of this point, see U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2009), pp. 304–307.

19. The advertisement showcased notable Chinese accomplishments in various sections including business, sports, and the arts. See Loretta Chao, “Pro-China Ad Debuts in Times Square,” *Wall Street Journal*, January 18, 2011; and Yidi Zhao, “China Airs Commercial in U.S. to Present Positive Image During Hu’s Visit,” *Bloomberg News*, January 17, 2011. The advertising videos themselves may be seen at *YouTube.com*, “China Publicity Ads Time Square New York 2011.” <http://www.youtube.com/watch?v=570LHTMWOmw&feature=related>.

20. Stuart Elliott, “Sign of Arrival, for Xinhua, Is 60 Feet Tall,” *New York Times*, July 25, 2011.

21. James Fallows, “Happy Birthday, China Daily!” *The Atlantic* (on-line blog edition), June 1, 2011. <http://www.theatlantic.com/national/archive/2011/06/happy-birthday-china-daily/239619/>.

22. See James Fallows, “Official Chinese Propaganda: Now Online from the WaPo [Washington Post]!” *The Atlantic* (online blog edition), February 3, 2011. <http://www.theatlantic.com/international/archive/2011/02/official-chinese-propaganda-now-online-from-the-wapo/70690/>; and Laura McGann, “State-Run Papers from China and Russia Buy Convincing Advertorial Sections on the WaPo’s [Washington Post] Website” (Cambridge, MA: Nieman Journalism Lab, Nieman Foundation at Harvard University), December 1, 2010. <http://www.niemanlab.org/2010/12/state-run-papers-from-china-and-russia-buy-convincing-advertorial-sections-on-the-wapos-website/>.

23. The theme of “harmony” has become a staple of CCP propaganda, both stressing the creation of a “socialist harmonious society” inside China and providing a reassuring message to foreign audiences. See John Dotson, “The Confucian Revival in the Propaganda Narratives of the Chinese Government” (Washington, DC: U.S.-China Economic and Security Review Commission, staff research report, July 20, 2011). [http://www.uscc.gov/researchpapers/2011/Confucian\\_Revival\\_Paper.pdf](http://www.uscc.gov/researchpapers/2011/Confucian_Revival_Paper.pdf).

24. As two such examples from the *China Watch* website (“A Paid Supplement to the Washington Post”), see “China ‘Best Served’ with [Chinese Communist Party] at the Helm,” July 1, 2011, <http://chinawatch.washingtonpost.com/2011/07/china-best-served-with-cpc-at-the-helm.php>; and Zhang Yuwei, “Land of Opportunity Chinese Companies Help Grow US Economy,” May 18, 2011, <http://chinawatch.washingtonpost.com/2011/05/land-of-opportunity—chinese-companies-help-grow-us-economy.php>.

25. \$300,000 is the approximate cost of placing a six-page, full-color, preprinted advertising insert “with editorial content” (the format employed by the *China Daily*) in a weekday edition of the *Washington Post*. The actual rate per instance of publication may be lower, as clients placing multiple advertising inserts over time can negotiate a lower rate. Additional fees would be charged for hosting web content, such as that found on the *China Watch* website. Source: Telephone inquiry by Commission staff to *Washington Post* advertising department, August 17, 2011.

26. U.S.-China Economic and Security Review Commission, *Hearing on China's Propaganda and Influence Operations, Its Intelligence Activities that Target the United States, and the Resulting Impacts on U.S. National Security*, written testimony of Ross Terrill and oral testimony of Anne-Marie Brady, April 30, 2009.

27. For an example of PRC accusations that negative views of China are fostered by western governments as part of a broader campaign of containment, see Mo Nong, "Part of the Plot to Contain China," *China Daily*, October 11, 2010. [http://www.chinadaily.com.cn/opinion/2010-10/11/content\\_11392433.htm](http://www.chinadaily.com.cn/opinion/2010-10/11/content_11392433.htm).

28. David Shambaugh, *Beautiful Imperialist: China Perceives America, 1972-1990* (Princeton, NJ: Princeton University Press, 1992); Philip Saunders, "China's America Watchers: Changing Attitudes Towards the United States," *China Quarterly* 161 (March 2000); Rosalie Chen, "China Perceives America: Perspectives of International Relations Experts," *Journal of Contemporary China* 12: 35 (2003); and David Shambaugh, "Coping with a Conflicted China," *Washington Quarterly* (Winter 2011).

29. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of Gary Rawnsley, March 10, 2011.

30. Dai Xu, "Zhongguo Ying Gei Meiguo Weidu Xingwei Hua Hong Xian" (China Must Draw a Red Line Against America's Encircling Actions), *Huanqiu Shibao* (*Global Times*), August 2, 2010. Translation by USCC staff. <http://opinion.huanqiu.com/roll/2010-08/977633.html>.

31. BBC News OnLine, "China Attacks Bush Foreign Policy," November 1, 2004. <http://news.bbc.co.uk/2/hi/asia-pacific/3971271.stm>.

32. The depiction of the United States as a predatory "hegemon" is a pillar of the official CCP conception of international affairs. This term has two specific sets of connotations as employed by Chinese writers. One is tied to ancient Chinese concepts of statecraft: As described by author Michael Pillsbury, "One specific Chinese premise from the ancient statecraft of the Warring States era seems to influence Chinese authors who write about the United States today — the concept of how to diagnose and deal with a powerful 'hegemon' (*ba*) that seeks to dominate several other less powerful states. The way hegemony conducted themselves during the Warring States period of ancient China forms one of the sources of the classic lessons of Chinese statecraft ... One set of 'lessons' (among many) was how to become a hegemon; another was how to survive destruction at the hands of a predatory hegemon." See Michael Pillsbury, *China Debates the Future Security Environment* (Honolulu, HI: University Press of the Pacific, 2005), pp. xxxv-xxxvi. The second set of connotations is tied to the CCP's official Marxist interpretations of modern history and in particular to the analysis of the contemporary world system as laid down by Deng Xiaoping in the late 1980s: "The world is so full of colonialism, neocolonialism, hegemony and power politics! ... one Cold War ... is being waged against all the countries of the South and the Third World, and the other against socialism. The Western countries ... want to bring about the peaceful evolution of socialist countries towards capitalism. ... National sovereignty is far more important than human rights, but they often infringe upon the sovereignty of poor, weak countries of the Third World. Their talk about human rights, freedom and democracy is only designed to safeguard the interests of the strong, rich countries, which take advantage of their strength to bully weak countries, and which pursue hegemony and practice power politics." See Deng Xiaoping, "We Must Adhere To Socialism and Prevent Peaceful Evolution Towards Capitalism" (excerpt from a conversation with Julius Nyerere, former president of Tanzania), November 23, 1989. From the *Selected Works of Deng Xiaoping*, Vol. 3 (Beijing, China: Foreign Languages Press, 1994). [http://www.archive.org/stream/SelectedWorksOfDengXiaopingVol.3/Deng03\\_djvu.txt](http://www.archive.org/stream/SelectedWorksOfDengXiaopingVol.3/Deng03_djvu.txt).

33. Yong Deng, "Hegemon on the Offensive: Chinese Perspectives on U.S. Global Strategy," *Political Science Quarterly* 116: 3 (2001).

34. For examples, see *Global Times*, "Turbulent Mid-East Disrupts the World," February 26, 2011. <http://opinion.globaltimes.cn/editorial/2011-02/627723.html>; U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2009), pp. 278-280; and *Beijing Ribao* (*Beijing Daily*), "Wei hu Wendong cong Meigeren Zuqi" (Maintaining Stability Starts with Every Person), March 6, 2011. Translation by USCC staff. [http://bjrb.bjd.com.cn/html/2011-03/06/content\\_375830.htm](http://bjrb.bjd.com.cn/html/2011-03/06/content_375830.htm).

35. Andrew Nathan and Perry Link, eds., *The Tiananmen Papers* (New York, NY: Public Affairs Books, 2001). See in particular "Excerpts from State Security Ministry, 'On Ideological and Political Infiltration into Our Country from the United States and Other International Political Forces,' report to Party Central, June 1," pp. 338-348.

36. Peter Hays Gries, "Tears of Rage: Chinese Nationalist Reactions to the Belgrade Embassy Bombing," *The China Journal* 46 (July 2001); and Peter Hays Gries, *China's New Nationalism* (Berkeley, CA: University of California Press, 2004), pp. 98–108. The 1999 U.S.-led North Atlantic Treaty Organization's (NATO) bombing campaign against the former Republic of Yugoslavia has itself been consistently depicted in PRC commentary as part of an effort to "further contain and weaken Russia" by diminishing a Russian ally and expanding NATO military control of Europe. See Wang Naicheng, "Failure of the New Strategic Concept," *Jiefangjun Bao (PLA Daily)*, May 22, 1999. OSC ID FBIS-CHI-1999-0601, as cited in Michael Pillsbury, *China Debates the Future Security Environment* (Honolulu, HI: University Press of the Pacific, 2005), p. 169.

37. Li Mingbo, "Mei Mimou Jian Dongya Fandao Tixi" (America's Scheme to Build an Anti-Missile System in East Asia), *Guangzhou Ribao (Guangzhou Daily)*, online edition, February 13, 2010. Available as "PRC Experts on US 'Plot' To Build East Asia Antimissile System To 'Encircle' PRC." OSD ID CPP201002140 01002. [www.opensource.gov](http://www.opensource.gov).

38. "Most Chinese analysts believe (and there is virtual consensus across the spectrum) that the whole concept of global governance is a Western trap which tries to undermine China's sovereignty and lure it into a variety of entanglements where China does not belong. There is a widespread perception that U.S. and EU calls for China to be a 'responsible power' (*fuzeren de daguo*) or 'responsible international stakeholder' are just the latest ruse for retarding and undermining China's power." David Shambaugh, "Coping with a Conflicted China," *Washington Quarterly* (Winter 2011).

39. "Quangiu Jinrong Weiji Shi Meiguo de Yinmou Ma" (Is the Financial Crisis an American Conspiracy?) *Huanqiu Shibao (Global Times)*, October 23, 2008. Translation by USCC staff. [http://www.otliba.com/show\\_news.asp?ID=40](http://www.otliba.com/show_news.asp?ID=40). See also Oiwan Lam, "U.S. Economic Crisis a Hot Topic on Chinese Blogs," *Global News Journal Blog* (Reuters News Service), October 2, 2008. <http://blogs.reuters.com/global/2008/10/02/us-economic-crisis-a-hot-topic-on-chinese-blogs>.

40. Shi Jianxun, "RMB Appreciation Pressure Harmful to Interests of China, EU," *People's Daily OnLine* (in English), October 9, 2010. <http://english.people.com.cn/90001/90780/91421/7161021.html>. See also *China Stakes.com*, "Conspiracy Theory Stalks China-US Financial Relations," January 25, 2008. <http://www.chinastakes.com/2008/1/conspiracy-theory-stalks-china-us-financial-relations.html>.

41. People's Republic of China State Council Information Office, "Human Rights Record of the United States in 2010" (Beijing, China: April 11, 2011). [http://www.chinadaily.com.cn/china/2011-04/11/content\\_12300327.htm](http://www.chinadaily.com.cn/china/2011-04/11/content_12300327.htm).

42. As an example of PRC state media commentary on alleged U.S. involvement in Tibetan unrest, see Xinhua (in English), "Double Act, Old Trick Behind Tibet Chaos," April 18, 2008. The article is posted on the website of the Embassy of the People's Republic of China in the United States at <http://www.china-embassy.org/eng/xw/t426629>. For similar allegations of U.S. involvement in Xinjiang, see *People's Daily Online* (in English), "Rebiya Kadeer's Funding Sources," July 14, 2009. <http://www.globaltimes.cn/www/english/truexinjiang/urumqi-riot/rebiya-kadeer/2009-07/446397.html>.

43. Michael Wines, "Cables Reveal Early Tensions Between U.S. and China on Nobel Winner," *New York Times*, December 9, 2010; and Malcolm Moore, "China Steps Up Anti-Nobel Campaign by Blocking BBC Website," *Telegraph* (United Kingdom), December 9, 2010.

44. *Global Times*, "2010 Nobel Peace Prize a Disgrace," October 9, 2010. <http://opinion.globaltimes.com/editorial/2010-10/580091.html>. For a more detailed discussion of the controversy in China surrounding the awarding of the 2010 Nobel Peace Prize to Liu Xiaobo, see John Dotson, "The Confucian Revival in the Propaganda Narratives of the Chinese Government" (Washington, DC: U.S.-China Economic and Security Review Commission, staff research report), July 20, 2011. [http://www.uscc.gov/researchpapers/2011/Confucian\\_Revival\\_Paper.pdf](http://www.uscc.gov/researchpapers/2011/Confucian_Revival_Paper.pdf).

45. Bonnie Glaser, "Ensuring that China Rises Peacefully" (Clingendael, The Netherlands: Netherlands Institute of International Relations, December 23, 2010). [http://www.clingendael.nl/publications/2010/20101223\\_CAF\\_artikel\\_BGlaser.pdf](http://www.clingendael.nl/publications/2010/20101223_CAF_artikel_BGlaser.pdf).

46. Quotation attributed to PRC Vice President Xi Jinping in "China, U.S. Agree Bilateral Relations 'Most Important'" *People's Daily Online* (in English), January 13, 2009. <http://english.people.com.cn/90001/90776/90883/6572553.html>.

47. David Shambaugh, "Coping with a Conflicted China," *Washington Quarterly* (Winter 2011).

48. See U.S.-China Economic and Security Review Commission, *Hearing on China's Propaganda and Influence Operations, Its Intelligence Activities that Target the*



*United States, and the Resulting Impacts on U.S. National Security*, written testimony of Anne-Marie Brady, April 30, 2009; People's Republic of China State Council Information Office, *China's Peaceful Development Road* (government white paper on China's development goals) (Beijing, China: December 22, 2005). [http://english.peopledaily.com.cn/200512/22/eng20051222\\_230059.html](http://english.peopledaily.com.cn/200512/22/eng20051222_230059.html); and People's Republic of China State Council Information Office, *China's National Defense in 2010* (government white paper on China's defense policies) (Beijing, China: March 31, 2011). [http://news.xinhuanet.com/english/2010/china/2011-03/31/c\\_13806851.htm](http://news.xinhuanet.com/english/2010/china/2011-03/31/c_13806851.htm).

49. John Garver, "The Chinese Communist Party and the Collapse of Soviet Communism," *China Quarterly* 133 (March 1993).

50. Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2008* (Washington, DC: U.S. Department of Defense, 2008), p. 8. Some PRC commentators have written that western governments and media have misunderstood aspects of the "24 Character Strategy," particularly the phrase "hide our capacities and bide our time." As stated in a 2010 essay posted on an official CCP website, "Hide our capabilities and bide our time, make some contributions' and related thoughts, these were put forward by Deng Xiaoping for the 'special period' of the late 1980s and early 1990s, in the midst of sudden changes in Eastern Europe and the collapse of the socialist camp. ... Currently, there are people in other countries who have produced misunderstandings and distortions of 'hide our capabilities and bide our time.' These people believe that China's foreign policy strategy has a long-term, undeclared content and purpose: This is that China believes that its current strength is insufficient, and the time has not yet come to announce and implement this great strategy, and consequently must 'Hide our capabilities and bide our time,' concealing the true situation and waiting for the right time of opportunity. ... However, this is ... a serious misunderstanding and distortion of the 'hide our capabilities and bide our time' idea stated by Comrade Deng Xiaoping ... the original idea of using the expression 'hide our capabilities and bide our time' was the strategy of 'developing ourselves,' and not at all to 'seek revenge on others' after we have developed." See Xiao Feng, "Was Comrade Deng Xiaoping's Idea of 'Hide Our Capabilities and Bide Our Time' a Measure of Expediency?" (*Deng Xiaoping Tongzhi de 'Tao Guang Yang Hui' Sixiang shi 'Quan Yi Zhi Ji' Ma?*) *Beijing Daily* (in Chinese), April 6, 2010. <http://dangshi.people.com.cn/GB/138903/141370/11297254.html>. Translation by USCC staff.

51. Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2008* (Washington, DC: U.S. Department of Defense, 2008), p. 8.

52. Gilbert Rozman, *Chinese Strategic Thought Toward Asia* (New York, NY: Palgrave MacMillan, 2010), p. 3.

53. *Xinhuanet* (in English), "Backgrounder: Five Principles of Peaceful Coexistence," June 14, 2004. [http://news.xinhuanet.com/english/2005-04/08/content\\_2803638.htm](http://news.xinhuanet.com/english/2005-04/08/content_2803638.htm).

54. Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2008* (Washington, DC: U.S. Department of Defense), p. 8.

55. Zheng Bijian, "China's 'Peaceful Rise' to Great-Power Status," *Foreign Affairs* 84: 5 (September-October 2005).

56. Information Office of the State Council of the People's Republic of China, *China's Peaceful Development Road* (Beijing, China: December 22, 2005). Of note, President Hu's speech at the 2004 Boao Forum for Asia on Hainan Island was expected to reiterate the theme of "peaceful rise," but instead it emphasized a new narrative, "peaceful development." Robert L. Suttinger, "The Rise and Descent of 'Peaceful Rise,'" *China Leadership Monitor* 12 (2004).

57. Hsin Pao, *Hong Kong Economic Journal* (January 27, 2006). OSC ID: CPP20060222904001. <http://www.opensource.gov>; and Zheng Bijian, "China's 'Peaceful Rise' to Great-Power Status," *Foreign Affairs* 84: 5 (September-October 2005): 18-24.

58. Robert L. Suttinger, "The Rise and Descent of 'Peaceful Rise,'" *China Leadership Monitor* 12 (2004).

59. Zheng Bijian, "China's 'Peaceful Rise' to Great Power Status," *Foreign Affairs* (September/October 2005).

60. Information Office of the State Council, *China's Peaceful Development Road* (Beijing, China: December 22, 2005). Note that the Information Office of the State Council has a dual identity and also functions as the CCP Office of Foreign Propaganda.

61. Information Office of the State Council, *China's Peaceful Development Road* (Beijing, China: December 22, 2005).



62. Robert L. Seuttinger, "The Rise and Descent of 'Peaceful Rise,'" *China Leadership Monitor* 12 (2004).
63. For a summary of the CCP leadership's messages on this theme, see *People's Daily Online* (in English), "Hu Jintao Proposes Scientific Outlook on Development for Tackling China's Immediate Woes, Challenges," October 15, 2007. <http://english.peopledaily.com.cn/90001/6283112.html>.
64. Yiyi Lu, "The Collective Study Sessions of the Politburo: A Multipurpose Tool of China's Leadership," (Nottingham, United Kingdom: University of Nottingham, China Policy Institute, October 2007). For a discussion of the role of Politburo study sessions, see also Philip Saunders, "The Chinese Politburo Hits the Books" (Washington, DC: The Jamestown Foundation, *China Brief*, May 9, 2007).
65. China Central Television, homepage for the television series "The Rise of the Great Powers" (*Da Guo Jueqi*). <http://finance.cctv.com/special/C16860/01/index.shtml>.
66. For an illustrative discussion of how interpretations of the Warring States Period affect modern-day Chinese concepts of statecraft, see Wei Zongyou, "In the Shadow of Hegemony: Strategic Choices," *Chinese Journal of International Politics* 1: 2 (2006). For comment on the same phenomenon from an American perspective, see also Jacqueline Newmyer, "Oil, Arms, and Influence: The Indirect Strategy Behind Chinese Military Modernization," *Orbis* (Spring 2009).
67. For an example of an author making the comparison between a rising China and Imperial Germany, see John Mearsheimer's arguments in Zbigniew Brzezinski and John Mearsheimer, "Clash of the Titans," *Foreign Policy* 146 (January/February 2005) <http://mearsheimer.uchicago.edu/pdfs/A0034.pdf>; and in John Mearsheimer, "Why China's Rise Will Not Be Peaceful," on-line essay dated September 17, 2004. <http://mearsheimer.uchicago.edu/pdfs/A0034b.pdf>. For a discussion of the concerns that Chinese leaders felt over such parallels, and their reactions to them, see Robert Sutter, "Debate on How to Deal with the United States" (paper presented at the conference "Chinese Leadership Differences," Carnegie Endowment for International Peace, Washington, DC, November 2, 2005). [http://carnegieendowment.org/files/Sutter\\_Revised.pdf](http://carnegieendowment.org/files/Sutter_Revised.pdf).
68. Ashley Tellis, "A Grand Chessboard," *Foreign Policy* (January/February 2005). <http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=16540>.
69. *Asia Media*, "Full Transcript: Tom Plate and Jeffrey Cole interview Lee Kuan Yew" (Los Angeles, CA: University of California, Los Angeles International Institute, October 9, 2007). <http://www.asiamedia.ucla.edu/article.asp?parentid=9541>.
70. Bonnie Glaser, "Ensuring that China Rises Peacefully" (Clingendael, The Netherlands: Institute of International Relations, December 23, 2010). [http://www.clingendael.nl/publications/2010/20101223\\_CAF\\_artikel\\_BGlaser.pdf](http://www.clingendael.nl/publications/2010/20101223_CAF_artikel_BGlaser.pdf).
71. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of David Lampton, March 10, 2011.
72. David Shambaugh, "Coping with a Conflicted China," *Washington Quarterly* (Winter 2011); and Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute, SIPRI Policy Paper no. 26, September 2010). [http://books.sipri.org/product\\_info?c\\_product\\_id=410](http://books.sipri.org/product_info?c_product_id=410).
73. For a discussion of the themes of "harmony" in PRC public diplomacy, see John Dotson, "The Confucian Revival in the Propaganda Narratives of the Chinese Government" (Washington, DC: U.S.-China Economic and Security Review Commission, staff research report), July 20, 2011. [http://www.uscc.gov/researchpapers/2011/Confucian\\_Revival\\_Paper.pdf](http://www.uscc.gov/researchpapers/2011/Confucian_Revival_Paper.pdf).
74. Wen Jiabao, "Getting to Know the Real China" (speech delivered at the 65th Session of the United Nations General Assembly, New York, NY, September 23, 2010). Posted on the website of the Ministry of Foreign Affairs of the People's Republic of China. <http://www.fmprc.gov.cn/eng/wjdt/zyjh/t761353.htm>.
75. Dai Bingguo, "Stick to the Path of Peaceful Development," *Beijing Review*, December 24, 2010.
76. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives on National Security Policy*, written testimony of John Park, March 10, 2011.
77. Li Keqiang, "The World Need Not Fear a Growing China," *Financial Times*, January 9, 2011.
78. Wang Jisi, "China's Search for a Grand Strategy," *Foreign Affairs* (March/April 2011).
79. The themes in Mr. Wang's article closely mirror statements by senior Chinese leaders. Furthermore, Wang Jisi is a frequent commentator on foreign affairs, with a very prominent position as the dean of the School of International Studies

at Beijing University. Publishing a piece such as this, in a widely respected journal that is influential among English-speaking foreign policy circles, would almost certainly require political clearance by CCP authorities.

80. Michael Chase, "Chinese Suspicions and US Intentions," *Survival* 53:3 (June 2011); and John Lee, "China's America Obsession," *ForeignPolicy.com*, May 6, 2011. [http://www.foreignpolicy.com/articles/2011/05/06/china\\_s\\_america\\_obsession?page=0,0](http://www.foreignpolicy.com/articles/2011/05/06/china_s_america_obsession?page=0,0).

81. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives on National Security Policy*, written testimony of Gilbert Rozman, March 10, 2011.

82. A.U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives on National Security Policy*, written testimony of Jacqueline Newmyer Deal, March 10, 2011.

83. Author unknown, "Developing a New Understanding of the Communist Party at the Central Party School," January 17, 2011. <http://chinadigitaltimes.net/2011/01/developing-a-new-understanding-of-the-communist-party-at-a-party-school>. Translation by *China Digital Times* (Don Weiland) and USCC staff.

84. As noted in a 1998 propaganda handbook, officials should be careful when speaking with foreigners, "remembering that 'insiders and outsiders are different' and to be mindful of the need for secrecy." "Shandong Sheng Duiwai Xuanchuan Gongzuo Huibian Ziliao 1992-1998" (Shandong Province Foreign Propaganda Work Reference Materials 1992-1998), publisher unknown, Vol. 2 (1998), p. 1921. The work is cited in Anne-Marie Brady, *Marketing Dictatorship* (Lanham, MD: Rowman & Littlefield, 2008), p. 161. For a discussion of the party's practices of suppressing information on certain issues while making reports on these same issues available to senior party officials, see He Qinglian, *The Fog of Censorship: Media Control in China* (New York, NY: Human Rights in China, 2008), pp. 71-75.

85. "Like communist and revolutionary parties throughout history, formed and nurtured by underground cells and violent conflict with the regimes they sought to overthrow, the Party in China is secretive by habit and inclination." Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York, NY: Harper Collins, 2010), p. 20.

86. On the employment of "proactive" propaganda by the CCP, see David Shambaugh, "China's Propaganda System: Institutions, Processes and Efficacy," *China Journal* 57 (January 2007). For a discussion of the suppression of negative news, see Ashley Esarey, "Speak No Evil: Mass Media Control in Contemporary China" (Washington, DC: Freedom House Special Report, February 2006). <http://www.freedomhouse.org/uploads/specialreport/33.pdf>.

87. Andrew J. Nathan and Bruce Gilley, *China's New Rulers: The Secret Files* (New York, NY: The New York Review of Books, 2003), p. 233.

88. Yang Jiechi, "Strengthen Shanghai Spirit," *China Daily*, June 15, 2011. [http://www.chinadaily.com.cn/opinion/2011-06/15/content\\_12698267.htm](http://www.chinadaily.com.cn/opinion/2011-06/15/content_12698267.htm).

89. *People's Daily Online* (in Chinese), "Shanghai Jingshen' Zhangxian Wuxian Meili" (Displaying the Limitless Charm of the "Shanghai Spirit"), June 15, 2011. <http://world.people.com.cn/GB/57507/14910318.html>. Translation by USCC staff.

90. Richard Weitz, "Balancer-in-Chief: China Assumes SCO Chair," *China Brief*, July 1, 2011.

91. "Astana Declaration of the 10th Anniversary of the Shanghai Cooperation Organization," Shanghai Cooperation Organization statement issued in Astana, Kazakhstan, June 15, 2011. <http://www.sco2011.kz/en/kzsco/inform.php>.

92. Wang Guosheng, "Comments and Analysis on China's Traditional Strategy of Defense," *Zhongguo Junshi Kexue* (China Military Science) 4 (2005); and *People's Daily Online* (in Chinese), "Peaceful Journey, Sowing Civilization: Commemorating the 600th Anniversary of the Voyages of Zheng He" (*Heping zhi Lu, Bosan Wenming—Jinian Zheng He Xia Xiang 600 Zhounian*), June 29, 2005. <http://www.people.com.cn/GB/32306/32313/32330/3506449.html>.

93. See the discussion of recent PRC propaganda treatment of the Zheng He narrative in John Dotson, "The Confucian Revival in the Propaganda Narratives of the Chinese Government" (Washington, DC: U.S.-China Economic and Security Review Commission, staff research report), July 20, 2011. [http://www.uscc.gov/research/papers/2011/Confucian\\_Revival\\_Paper.pdf](http://www.uscc.gov/research/papers/2011/Confucian_Revival_Paper.pdf).

94. People's Republic of China State Council Information Office, *China's National Defense in 2010* (government white paper on China's defense policies) (Beijing, China: March 31, 2011). [http://news.xinhuanet.com/english2010/china/2011-03/31/c\\_13806851.htm](http://news.xinhuanet.com/english2010/china/2011-03/31/c_13806851.htm).

95. "Chen Bingde," biographical entry at *ChinaVitae.com*. [http://www.chinavitae.com/biography/Chen\\_Bingde/summary](http://www.chinavitae.com/biography/Chen_Bingde/summary).

96. Shirley A. Kan, "U.S.-China Military Contacts: Issues for Congress" (Washington, DC: Congressional Research Service, December 2010), pp. 3–4.

97. Chen Bingde "Speech presented at the National Defense University" (Washington, DC, May 20, 2011). Notes taken by USCC staff.

98. According to scholar Michael Swaine, the term "core interests" appeared in articles in the *People's Daily* three times in 2003; 55 times in 2005; 95 times in 2008; 260 times in 2009; and 325 times in 2010. See Michael Swaine, "China's Assertive Behavior, Part One: On 'Core Interests,'" *China Leadership Monitor* 34 (2011).

99. Comments made by Chinese academics in a roundtable discussion with members of the U.S.-China Economic and Security Review Commission, U.S. Consulate in Shanghai, August 11, 2011.

100. Huai Chengbo, "How Do We Understand 'National Core Interests'?" (*Zenmo Lijie* "Guojia Hexin Liyi"?), *Qsttheory.cn* (website of the official CCP theoretical journal *Qiushi*), January 25, 2011. [http://www.qsttheory.cn/hqwg/2011/201102/201101/t20110125\\_63092.htm](http://www.qsttheory.cn/hqwg/2011/201102/201101/t20110125_63092.htm). Translation by USCC staff.

101. PRC State Councilor Dai Bingguo, remarks made at the closing of the U.S.-China Strategic and Economic Dialogue, Washington, DC, July 28, 2009. <http://www.state.gov/secretary/rm/2009a/july/126599.htm>. Chinese academics have cited Mr. Dai's remarks as the authoritative position of the CCP, as with comments made by Chinese academics in a roundtable discussion with members of the U.S.-China Economic and Security Review Commission, U.S. Consulate in Shanghai, August 11, 2011.

102. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives on National Security Policy*, written testimony of John Park, March 10, 2011.

103. Greg Sheridan, "China Actions Meant as Test, Hillary Clinton Says," *Australian* (Sydney, Australia), November 9, 2010.

104. John Pomfret, "Beijing Claims 'Indisputable Sovereignty' Over South China Sea," *Washington Post*, July 31, 2010.

105. Edward Wong, "China Hedges Over Whether South China Sea Is a 'Core Interest' Worth War," *New York Times*, March 30, 2011. For commentary from a prominent PRC academic that seeks to downplay the significance of this controversy, see Wang Jisi, "A Rising Great Power Finds its Way," *Foreign Affairs* (March/April 2011).

106. Huai Chengbo, "How Do We Understand 'National Core Interests'?" (*Zenmo Lijie* "Guojia Hexin Liyi"?), *Qsttheory.cn* (website of the official CCP theoretical journal *Qiushi*), January 25, 2011. [http://www.qsttheory.cn/hqwg/2011/201102/201101/t20110125\\_63092.htm](http://www.qsttheory.cn/hqwg/2011/201102/201101/t20110125_63092.htm).

107. John Milligan-Whyte and Dai Min, "Getting Tough or a New Era of Partnership?" *People's Daily Online* (in English), March 26, 2010. <http://english.people-daily.com.cn/90001/90780/91343/6932227.html>.

108. Comments by Hu Jintao made in Islamabad, Pakistan, on November 24, 2006, as cited in Michael Swaine, "China's Assertive Behavior, Part One: On 'Core Interests,'" *China Leadership Monitor* 34 (2011).

109. Da Wei, "A Clear Signal of 'Core Interests' to the World," *China Daily*, August 2, 2010. [http://www.chinadaily.com.cn/usa/2010-08/02/content\\_11083124.htm](http://www.chinadaily.com.cn/usa/2010-08/02/content_11083124.htm).

110. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives on National Security Policy*, written statement of Alison Kaufman ("The 'Century of Humiliation' and China's National Narratives"), March 10, 2011. For a statement by a paramount Chinese leader on the direct linkage between the history of imperialism and China's present-day circumstances, see Deng Xiaoping, "We Must Adhere To Socialism and Prevent Peaceful Evolution Towards Capitalism" (excerpt from a conversation with Julius Nyerere, former president of Tanzania), November 23, 1989. From the *Selected Works of Deng Xiaoping*, Vol. 3 (Beijing, China: Foreign Languages Press, 1994). [http://www.archive.org/stream/SelectedWorksOfDengXiaopingVol.3/Deng03\\_djvu.txt](http://www.archive.org/stream/SelectedWorksOfDengXiaopingVol.3/Deng03_djvu.txt).

111. "China is to a considerable extent a bargaining culture in which prior bargains are open for renegotiation whenever the underlying power positions, or broader circumstances, of the two (or more) parties shift. China, meaning its government and its people, has been chafing at some of the implicit or explicit bargains struck in the past with the United States, most notably regarding Taiwan, the U.S. military's close-in surveillance of the Mainland, visits to the White House by the Dalai Lama, vulnerability of the PRC's nuclear deterrent, and so forth. Now that China perceives itself stronger, and America and its allies on a trajectory of decreased dominance, it is no surprise Beijing is asking to 'renegotiate' the prior bargains it finds most unsatisfactory." U.S.-China Economic and Security Review Commission,

*Hearing on China's Narratives on National Security Policy*, written testimony of David Lampton, March 10, 2011.

112. Wang Guosheng, "Comments and Analysis on China's Traditional Strategy of Defense," *Zhongguo Junshi Kexue* (China Military Science) 4 (2005).

113. Alastair Iain Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History* (Princeton, NJ: Princeton University Press, 1995).

114. Andrew Scobell, *China and Strategic Culture* (Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2002), p. V. <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub60.pdf>.

115. Xiaoming Zhang, "China's 1979 War with Vietnam: A Reassessment," *China Quarterly* 184 (December 2005). [http://www.viet-studies.info/kinhte/China\\_G7<War\\_With\\_Vietnam.pdf](http://www.viet-studies.info/kinhte/China_G7<War_With_Vietnam.pdf).

116. Jay Solomon, "U.S. Takes on Maritime Spats," *Wall Street Journal*, July 24, 2010. <http://online.wsj.com/article/SB10001424052748703294904575384561458251130.html>.

117. See Australian Government Department of Defence, *Defending Australia in the Asia-Pacific Century: Force 2030* (Canberra, Australia: 2009). [http://www.defence.gov.au/whitepaper/docs/defence\\_white\\_paper\\_2009.pdf](http://www.defence.gov.au/whitepaper/docs/defence_white_paper_2009.pdf); and Japanese Government Ministry of Defense, *Defense of Japan 2010* (Tokyo, Japan: 2010). [http://www.mod.go.jp/e/publ/w\\_paper/2010.html](http://www.mod.go.jp/e/publ/w_paper/2010.html).

118. Patrick Barta, "U.S., Vietnam in Exercises Amid Tensions with China," *Wall Street Journal*, July 16, 2011; and *Manila Times* (Philippines), "Spratlys Dispute Won't Affect PH-China Ties," July 18, 2011, <http://www.manilatimes.net/news/topstories/spratlys-dispute-won%E2%80%99t-affect-ph-china-ties-2/>.

119. Jim Garamone, "Cheonan Tragedy Strengthens U.S.-South Korea Alliance," *American Forces Press Service*, July 21, 2010; and Edward Luttwak, "The Guns of December," *ForeignPolicy.com*, December 21, 2010. [http://www.foreignpolicy.com/articles/2010/12/21/the\\_guns\\_of\\_december?page=0,1](http://www.foreignpolicy.com/articles/2010/12/21/the_guns_of_december?page=0,1).

120. David Lai, "The Coming of Chinese Hawks" (Carlisle, PA: U.S. Army War College Strategic Studies Institute, October 2010). <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1028.pdf>.

121. "Liu Yuan," biographical entry in *ChinaVita.com*. [http://www.chinavita.com/biography/Liu\\_Yuan/4071](http://www.chinavita.com/biography/Liu_Yuan/4071). In the early 1960s, Liu Shaoqi ranked second in the CCP hierarchy and was Mao Zedong's designated successor. However, the elder Mr. Liu was purged, and later died in prison, during the Cultural Revolution.

122. "Shaping history is particularly important to China's so-called princelings ... having secured influence and often wealth on the basis of their family's connections, members of this small but powerful group celebrate a wart-free version of the past that boosts their status—and sidesteps their parents' role as enforcers and then victims of party brutality," Andrew Higgins, "The Party Line on Party History," *Washington Post*, May 27, 2011.

123. John Garnaut, "Chinese General Rattles Sabre," *The Age* (Australia), May 23, 2011; and Andrew Higgins, "The Party Line on Party History," *Washington Post*, May 27, 2011.

124. Liu Yan, excerpts from text as cited in *Renminwang* (People's Daily Online), "Liu Shaoqi de Zi Liu Yuan Shangjiang: Hebu Mingzhengyanshun, Lizhiqizhuang de Juqi Xin Minzhu Zhuyi?" (Liu Shaoqi's Son General Liu Yuan: Why Aren't We Perfectly Justified in Upholding New Democracy?), May 16, 2011. <http://blog.163.com/lasz8720@126/blog/static/138019571201141674446665/>. Translation by USCC staff.

125. Willy Ho-Lap Lam, "The Death of Factions within the Chinese Communist Party?" *China Brief* 11:9 (May 20, 2011); Willy Ho-Lap Lam, "Hu Revives Quasi-Maoist Tactics to Stem Social Instability," *China Brief* 10:20 (October 8, 2010); and Willy Ho-Lap Lam, "Chinese Leaders Revive Marxist Orthodoxy," *China Brief* 10:9 (April 29, 2010).

126. John Garnaut, "Chinese General Rattles Sabre," *The Age* (Australia), May 23, 2011.

127. Liu Yan, excerpts from text as cited in *Renminwang* (People's Daily Online), "Liu Yuan: Hebu Mingzhengyanshun, Lizhiqizhuang de Juqi Xin Minzhu Zhuyi?" (Liu Yuan: Why Aren't We Perfectly Justified in Upholding New Democracy?), May 16, 2011. <http://history.people.com.cn/GB/205396/14651911.html>. Translation by USCC staff.

128. Willy Lam, "The Military Maneuvers of Xi Jinping," *Wall Street Journal*, Journal 26, 2011. [http://online.wsj.com/article/SB10001424052748704698004576103513580674214.html?mod=googlenews\\_wsj](http://online.wsj.com/article/SB10001424052748704698004576103513580674214.html?mod=googlenews_wsj).

129. Paul Eckert, "Sizing Up China's Next Leader," Reuters News Service, February 17, 2011. <http://graphics.thomsonreuters.com/11/01/XiJinping.pdf>. See also Peter Foster, "WikiLeaks: China's Politburo a Cabal of Business Empires," *Tele-*



graph (United Kingdom), December 6, 2010. <http://www.telegraph.co.uk/news/worldnews/wikileaks/8184216/WikiLeaks-Chinas-Politburo-a-cabal-of-business-empires.html>; and Malcolm Moore, "Light Cast on the Man China's Censors Have Been Trying to Hide," *Sydney Morning Herald* (Australia), January 5, 2011. <http://www.smh.com.au/technology/technology-news/light-cast-on-the-man-chinas-censors-have-been-trying-to-hide-20110104-19f2t.html>.

130. Warren Sun (professor at Monash University) as quoted in John Garnaut, "China's Party Princelings Fight for a Chance to Go Back to the Future," *Sydney Morning Herald* (Australia), May 24, 2011. <http://www.smh.com.au/business/chinas-party-princelings-fight-for-a-chance-to-go-back-to-the-future-20110523-1f0pu.html>.

131. Strategic Forecasting, Inc. (STRATFOR), "Former President's Son on Track for a Powerful Military Position," July 23, 2011; and Willy Lam, "The Military Maneuvers of Xi Jinping," *Wall Street Journal*, January 26, 2011. [http://online.wsj.com/article/SB10001424052748704698004576103513580674214.html?mod=googlenews\\_wsj](http://online.wsj.com/article/SB10001424052748704698004576103513580674214.html?mod=googlenews_wsj).

132. In recent years, the CCP Central Military Commission has had either ten or 11 members, normally consisting of: a chairman (the civilian CCP paramount leader, currently Hu Jintao); two uniformed vice chairmen, one a political commissar and the other a line officer (currently General Xu Caihou and General Guo Boxiong, respectively); at some times, another civilian vice chairman (the CCP heir apparent leader, currently Xi Jinping); the heads of the four PLA general departments (Staff, Political, Logistics, Armaments); and the heads of the four PLA service branches (army, navy, air force, and Second Artillery). The current PRC defense minister, General Liang Guanglie, also sits on the Central Military Commission, apparently providing dual representation for the Defense Ministry and for the ground forces.

133. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives on National Security Policy*, written testimony of Gilbert Rozman, March 10, 2011. This tendency is particularly true of books published by senior officers through military publishing houses, which frequently include strident language and predictions of inevitable conflict with the United States. Such writings do not reflect official policy, but they do reveal intense nationalist feeling and hostility to the United States within elements of the military as well as a receptive commercial audience for such ideas. See Chris Buckley, "China PLA Officer Urges Challenging U.S. Dominance," Reuters, February 28, 2010; and Peter Brown, "The PLA Raises Its Voice," *Asia Times*, March 8, 2010.

134. John Pomfret, "In Chinese Admiral's Outburst, a Lingering Distrust of U.S.," *Washington Post*, June 8, 2010.

135. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of Abraham Denmark, March 10, 2011.

136. For a discussion of this and other potential explanations for PLA nationalist commentary, see U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, written testimony of Andrew Scobell, March 10, 2011; and Andrew Scobell, "Is There a Civil-Military Gap in China's Peaceful Rise?" *Parameters* (Summer 2009).

137. Willy Lam, "The Military Maneuvers of Xi Jinping," *Wall Street Journal*, January 26, 2011. [http://online.wsj.com/article/SB10001424052748704698004576103513580674214.html?mod=googlenews\\_wsj.K](http://online.wsj.com/article/SB10001424052748704698004576103513580674214.html?mod=googlenews_wsj.K)

138. Website of the Institute for U.S.-China Issues at the University of Oklahoma, "The Sino-American Security Dialogue," <http://www.ou.edu/uschina/SASD/index.htm>; and Peter Gries (University of Oklahoma) e-mail communication with Commission staff, October 13–14, 2011.

139. For only three examples out of many that could be cited: the Chinese People's Institute for Foreign Affairs is subordinate to the PRC Foreign Ministry, and the China Association for International Understanding is subordinate to the CCP International Department [see David Shambaugh, "China's Propaganda System: Institutions, Processes and Efficacy," *China Journal* 57 (January 2007)]; and the China Institutes of Contemporary International Relations, or CICIR, is subordinate to the PRC Ministry of State Security (Open Source Center, "Profile of MSS-Affiliated PRC Foreign Policy Think Tank CICIR," August 25, 2011. [www.opensource.gov](http://www.opensource.gov).)

140. As an example, see the discussion of appointments to the Chinese Academy of Social Sciences in: U.S.-China Economic and Security Review Commission, *2008 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2008), p. 292.

141. According to Dr. David Shambaugh of The George Washington University, "[i]t appears that [the China Association for International Friendly Contact] is



linked to the Intelligence Bureau of the Liaison Department of the PLA's General Political Department . . . [with additional] ties to both the Ministry of State Security and the Ministry of Foreign Affairs." [See David Shambaugh, "China's International Relations Think Tanks: Evolving Structure and Process," *China Quarterly* 171 (September 2002).] In addition to serving as "a front for inviting and meeting with selected foreigners in China," the China Association for International Friendly Contact has also served as a vehicle "for sending active-duty intelligence collectors abroad under various kinds of cover." [See David Shambaugh, *Modernizing China's Military: Progress, Problems, and Prospects* (Los Angeles, CA: University of California Press, 2002), p. 136]. For further commentary on the role of the GPD/LD [Liaison Department] and the China Association for International Friendly Contact in sending agents abroad, see also Howard DeVore, *China's Intelligence and Internal Security Forces* (Alexandria, VA: Jane's Information Group, 1999), pp. 50–51; and Nicholas Eftimiades, *Chinese Intelligence Operations* (Annapolis, MD: Naval Institute Press, 1994), pp. 103–104.

142. The International Liaison Department of the PLA General Political Department has traditionally borne responsibility for conducting propaganda and psychological operations directed at other militaries. [See Howard DeVore, *China's Intelligence and Internal Security Forces* (Alexandria, VA: Jane's Information Group, 1999), p. 50–51; and Interagency OPSEC [Operational Security] Support Staff, *Intelligence Threat Handbook* (2004), p. 23. <http://www.fas.org/irp/threat/handbook/foreign.pdf>.] The Liaison Department conducts its perception management operations in accordance with centrally determined CCP propaganda narratives: As stated in the mid-1990s by Nicholas Eftimiades, an analyst with the Defense Intelligence Agency, "[P]olitical-military propaganda against foreign forces is a national function under the purview of the GPD's [General Political Department] liaison department. Implementation of a specific theme of disinformation must somehow advance national policy objectives. It is therefore probable that the GPD formulates propaganda in accordance with [Central Military Commission] military and policy decisions. Such campaigns are then implemented through the PLA's overt and intelligence channels under the supervision of political commissars." [See Nicholas Eftimiades, *Chinese Intelligence Operations* (Annapolis, MD: Naval Institute Press, 1994), pp. 92–93.]

143. Survey performed by USCC staff of the international exchanges listed on the CAIFC website for the years 2009–2010. The list is not exhaustive but instead shows a selected number of more prominent exchange activities. See Website of the China Association for International Friendly Contact. <http://www.caifc.org.cn>. Material translated by USCC staff.

144. The Center for Peace and Development shares office space with the CAIFC in a compound in the northern part of Beijing. The institute conducts exchanges with foreign academics and events with government officials and also publishes its own bimonthly journal on foreign affairs, eponymously titled *Peace and Development*. For a discussion of the connection between CAIFC and CPD, see David Shambaugh, *Modernizing China's Military: Progress, Problems, and Prospects* (Los Angeles, CA: University of California Press, 2002), p. 136. Brief profiles of recent CPD exchanges with foreign academics and Chinese government officials may be found in the website of the Center for Peace and Development, "Scholarly Exchange Activities." <http://www.caifc.org.cn/qk.aspx>. Lists of tables of contents from selected issues of *Peace and Development*, and abstracts of the articles, may be found on *China National Knowledge Infrastructure On-Line*, profile for *Peace and Development*. [http://www.acad.cnki.net/Kns55/oldnavi/n\\_item.aspx?NaviID=1&BaseID=HPFZ&NaviLink=](http://www.acad.cnki.net/Kns55/oldnavi/n_item.aspx?NaviID=1&BaseID=HPFZ&NaviLink=).

145. The "Sanya Initiative" is a series of track two dialogues between retired, senior-ranking flag officers of the U.S. and Chinese armed forces. On the Chinese side, the initiative is hosted by the China Association for International Friendly Contact. The exchanges commenced in February 2008 with meetings in Beijing and in the city of Sanya, on Hainan Island. The Sanya Initiative dialogues are not official military-to-military exchanges conducted by the U.S. Department of Defense.

146. For two such examples, see U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, testimonies of John Park and Abraham Denmark, March 10, 2011.

147. U.S.-China Economic and Security Review Commission, *Hearing on China's Narratives Regarding National Security Policy*, testimony of Abraham Denmark, March 10, 2011.

148. Michael Pillsbury, "China's Research Institutes" (paper written on behalf of the U.S.-China Economic and Security Review Commission, June 2001). [http://www.uscc.gov/researchpapers/2000\\_2003/pdfs/cr.pdf](http://www.uscc.gov/researchpapers/2000_2003/pdfs/cr.pdf).

149. Open Source Center, "Profile of MSS [Ministry of State Security]–Affiliated PRC Foreign Policy Think Tank CICIR," August 25, 2011. [www.opensource.gov](http://www.opensource.gov).



## **COMPREHENSIVE LIST OF THE COMMISSION'S RECOMMENDATIONS**

### **Introduction**

The Commission recommends that:

1. Congress, through legislation, require the president to assign the National Security Council to conduct an agency-wide comprehensive review of the U.S. economic and security policies toward China to determine the need for changes to address the increasingly complicated and serious challenges posed by China to U.S. international and domestic interests. Such a review should be examined and debated as appropriate by Congressional committees.

### **Chapter 1: The U.S.-China Trade and Economic Relationship**

#### ***Section 2: Chinese State-owned Enterprises and U.S.-China Bilateral Investment***

The Commission recommends that:

2. Congress urge the administration to employ all necessary remedies authorized by WTO rules to counter the anticompetitive and trade-distorting effects of the Chinese government's extensive subsidies for Chinese companies operating in China and abroad.
3. Congress assess the extent to which existing laws provide for effective remedies against the anticompetitive actions of Chinese state-owned or state-invested enterprises operating in the U.S. market. Appropriate remedies, if they are not readily available, should also be considered.
4. Congress urge the administration to include in any bilateral investment treaty with China the principles of nondiscrimination and competitive neutrality between SOEs and other state-invested or -supported entities and private enterprises.
5. Congress assess China's new national security review process for foreign investment to determine whether it is being used as a trade barrier.
6. Congress direct the U.S. Department of Commerce to report annually on Chinese investment in the United States including, among other things, data on investment in the United States by Chinese SOEs and other state-affiliated entities.
7. Congress direct the U.S. Securities and Exchange Commission to revise its protocols for reviewing filings by foreign entities listed on or seeking to be listed on the U.S. stock exchanges.

The Securities and Exchange Commission should develop country-specific data to address unique country risks to assure that U.S. investors have sufficient information to make investment decisions. The commission should focus, in particular, on state-owned and -affiliated companies, and subsidies and pricing mechanisms that may have material bearing on the investment.

8. Congress urge the administration to review federally subsidized contracts provided under the American Recovery and Reinvestment Act of 2009 and report on the extent to which Chinese-produced goods and services were procured using such funds.
9. Congress urge the administration to direct the USTR to move aggressively to bring more WTO cases against China for violating its obligations under the WTO Subsidies Agreement.
10. Congress urge the administration to direct the USTR to strengthen its mandated annual review of China's compliance with its WTO obligations by adding conclusions and recommendations to its annual report to Congress.

### ***Section 3: Indigenous Innovation and Intellectual Property Rights***

The Commission recommends that:

11. Congress request the administration to report on whether procurement catalogues are actionable under WTO obligations.
12. Congress instruct the administration to insist that all procurement catalogues at all levels of government be explicitly recalled in order to comply with assurances by President Hu Jintao to separate government procurement from the catalogues.
13. Congress urge the administration to raise with China in the Strategic and Economic Dialogue and the Joint Commission on Commerce and Trade and in other appropriate bilateral and multilateral venues the need for China to table a serious offer to join the Government Procurement Agreement that provides reciprocal opportunities for access to the estimated \$1 trillion in procurement controlled by central, provincial, and local governments as well as state-affiliated entities. If China fails to engage in serious negotiations, the U.S. government should restrict access to Chinese suppliers to government procurement opportunities and should coordinate policies with the states to limit procurement contracts with China.
14. Congress instruct the administration to make a top priority within the Joint Commission on Commerce and Trade and the Strategic and Economic Dialogue negotiations an agreement to lower the threshold for criminal prosecution of cases of piracy and counterfeiting of business and entertainment software.
15. Congress recommend the administration adopt a more reciprocal trading relationship in critical areas, such as intellectual property protection. The United States should demand the

same level of treatment from its major trading partners that it provides to those other nations. The administration should identify those sectors that China has failed to open up to trade in goods and services and identify the practices that act to nullify and impair anticipated economic benefits for U.S. producers and service providers. The administration should seek the elimination of such practices in a timely manner and, if unable to gain sufficient market access, should evaluate what reciprocal actions may be appropriate.

16. Congress urge the administration to insist that China audit the use of licensed software on government computers rather than just audit the budget for software procurement. The audit should be performed by the World Bank.
17. Congress assess the reauthorization of Super 301 to assist in the identification of the policies and practices that China pursues that create the greatest impediment to U.S. exports entering the Chinese market and the most important policies or practices that unfairly or unjustifiably harm U.S. producers and workers in the U.S. market. Priority should be given to addressing such practices by the United States Trade Representative under such legislation.
18. The President should direct USTR to move aggressively to bring cases to the WTO to enforce intellectual property rights.

#### ***Section 4: China's 12th Five-Year Plan and Technology Development and Transfers to China***

The Commission recommends that:

19. Congress hold hearings to assess the success of the Strategic and Economic Dialogue and the Joint Committee on Commerce and Trade in addressing Chinese actions to implement its WTO commitments, including with regard to the issue of technology transfers. In preparation for such hearings, Congress should request that the Government Accountability Office prepare an inventory of specific measures agreed to as part of these bilateral discussions and the implementation efforts of the Chinese.
20. Congress direct the Government Accountability Office to undertake an evaluation of investments and operations of U.S. firms in the Chinese market and identify what federally supported R&D is being utilized in such facilities and the extent to which, and on what terms, such R&D has been shared with Chinese actors in the last ten years.

#### ***Section 5: China's Internal Dilemmas***

The Commission recommends that:

21. The administration work with the Chinese leaders in the Strategic and Economic Dialogue and the Joint Commission on Commerce and Trade talks to identify specific commodities and products in the case where supply does not adequately meet demand in China and where enhanced access for U.S. goods



might help alleviate inflationary pressures. Specific attention should be given to agricultural commodities and Chinese barriers that may limit access to the Chinese market for American goods and products.

22. Congress direct the Government Accountability Office to conduct a review of efforts by the Chinese government to censor content on the Internet and identify the extent to which any foreign technology providers may be assisting the government in its efforts.

## **Chapter 2: China's Activities Directly Affecting U.S. Security Interests**

### ***Section 2: China's "Area Control Military Strategy"***

The Commission recommends that:

23. The relevant Congressional committees investigate the adequacy of security for the Department of Defense's logistics data system, the time-phased force deployment data system, to ensure that the data therein are secure from a cyberattack.
24. Congress assess the adequacy of Department of Defense capabilities to conduct major operations in a degraded command, control, communications, computer, intelligence, surveillance, and reconnaissance environment for an extended period of time.
25. Congress direct the Government Accountability Office to evaluate the Department of Defense's early warning systems to ensure that the department will have sufficient timely warning of a PLA attack in the event of a conflict.
26. Congress require that the Department of Defense conduct periodic peaceful naval and air exercises in the East Asian maritime region to demonstrate the U.S. commitment to freedom of navigation.
27. Congress assess the adequacy of funding for Department of Defense programs that ensure the military's ability to operate effectively against China's Area Control Strategy measures. Such programs could include, at a minimum, robust theater ballistic missile defense, antisubmarine warfare, advanced air-to-air combat, command and control, and electronic warfare capabilities.
28. Congress encourage the administration to continue to work diplomatically and militarily with regional allies and friends to improve their capacity to resist China's Area Control Strategy capabilities.

### ***Section 3: The Implications of China's Civil and Military Space Activities***

The Commission recommends that:

29. Congress mandate that the Department of Defense (and other government space operators, as appropriate) assess and report

upon their preparedness for potential Chinese counterspace activities. To the extent that commercial entities provide essential services, assessments should also cover their systems.

30. Congress assess the adequacy and regularity of U.S. military exercises and training activities that simulate the destruction, denial, degradation, or manipulation of U.S. space assets. In addition, Congress should periodically evaluate whether the Department of Defense is taking sufficient measures to diversify its traditionally space-oriented capabilities, such as in navigation, communications, intelligence, surveillance, and reconnaissance.

### **Chapter 3: China's Foreign Policy**

#### ***Section 1: An Overview of China's Relations with North Korea and Iran***

The Commission recommends that:

31. Congress investigate whether U.S. sanctions have been imposed on all Chinese firms that have violated the sanction laws by investing in Iran's petroleum industry or providing Iran with refined petroleum products or advanced conventional weapons.
32. Congress, in light of China's continued investments in North Korea, hold hearings to evaluate the effectiveness of expanding North Korean sanctions to cover foreign firms investing in North Korea's natural resource industry.

#### ***Section 2: Actors in China's Foreign Policy***

The Commission recommends that:

33. Congress investigate the extent to which the People's Liberation Army is becoming a more influential actor in China's foreign policy-making.
34. Members of Congress make an effort to engage with multiple official and unofficial foreign policy actors during their trips to China in order to better understand and establish channels of communication with these actors.

#### ***Section 3: Taiwan***

The Commission recommends that:

35. Congress urge the administration to sell Taiwan the additional fighter aircraft it needs to recapitalize its aging and retiring fleet.
36. Congress request from the administration an update on the Taiwan submarine program that was approved for sale by the U.S. government in 2001.
37. Congress explore in hearings the implications for the United States and the region of closer China-Taiwan relations.

***Section 4: Hong Kong***

The Commission recommends that:

38. Congress reauthorize Section 301 of the Hong Kong Policy Act of 1992, which requires the U.S. secretary of State to submit an annual report to Congress on political, social, and economic developments in Hong Kong as they relate to the United States. This should include reporting on China's measures to use Hong Kong as a platform for the internationalization of the renminbi.
39. Members of Congress, when visiting mainland China, also visit Hong Kong and that Congress encourage senior administration officials, including the secretary of State, to make visits to Hong Kong part of their travel.
40. Congress encourage its Members to raise the issue of preserving Hong Kong's special status when meeting with members of China's National People's Congress.

**Chapter 4: China's Public Diplomacy Initiatives Regarding Foreign and National Security Policy**

The Commission recommends that:

41. Congress evaluate the effectiveness of U.S. government public diplomacy programs in the East Asian region.
42. Congress urge the administration to seek clarification on the Chinese government's views as to what represents a "core interest" as well as what this formulation means for U.S.-China relations, and the implications for U.S. allies and friends.
43. Congress ensure that its own Members are made fully aware of the Chinese institutional actors engaged in exchange programs involving officials of the U.S. Government.

### **ADDITIONAL VIEWS OF COMMISSIONERS WILLIAM REINSCH AND ROBIN CLEVELAND**

We support this year's report despite our opposition to several of its recommendations because we think it adequately captures many of the dilemmas and difficulties that currently beset our relationship with China. At the very time our own country is faced with a vast range of difficulties and appears divided on the correct solutions, we must also deal with a rising China that appears to have ignored or forgotten then-U.S. Trade Representative Robert Zoellick's call for China to be a "responsible stakeholder."

On the economic front, the report details the growing number of problems the U.S.—and other developed economies—has with China such as its indigenous innovation policy, its continued failure to adequately protect intellectual property, subsidies, barriers to market access, discriminatory regulations, and its undervalued currency.

It is clear that China has made a sharp turn in its economic policy over the past five years in the direction of more state control and less free market competition. This comes as a huge disappointment to the American business community which supported Chinese WTO accession as a means to integrating it into the Western market trading system. Ten years later evidence is piling up to suggest that China wants to enter the system solely on its own terms, even when they are incompatible with WTO rules or modern business practices. Many of these practices will be litigated in the WTO, where we will likely win, but the damage will by that time be done.

On the military front, the Commission has rightly focused much of its attention in this report on China's activities in the South China Sea and on its relations with North Korea and Iran. While its policies with respect to the last two are not helpful, they are also not new, and the Commission has commented on them in the past. In the South China Sea, China's vigorous assertion of its exaggerated claims has been a destabilizing force in the region that threatens to grow worse. Ironically, this has helped enhance an appreciation among the other littoral states for a strong U.S. presence there, to which we believe the Administration has responded skillfully.

China's military buildup, which we have commented on in past reports, continues, and a number of the Commission's recommendations have correctly focused on the adequacy of U.S. preparation for an enhanced Chinese presence and capability.

It is on the economic side where we believe the Commission's recommendations go astray. As we said last year in our additional views,

"The United States, recovering too slowly from the worst recession in 80 years, seems tempted to act out of fear, blaming China for our economic problems just as 20 years ago we blamed the Japanese. While blame is tempting—and often well-placed—it is *our* destiny we control, not theirs. Faulting them for doing things in their own interest is emotionally satisfying but ultimately an empty gesture. Our politicians serve our people best when they act

in our interests and when they persuade the Chinese to work with us in pursuit of common interests.”

This means that the right answers lie in policies we should pursue to make ourselves more competitive rather than policies to hold the Chinese back. Many of those policies lie outside the Commission’s mandate, not to mention its competence. However, our inability to provide the right answers does not mean that we should suggest the wrong ones instead.

One such wrong answer is the Commission’s recommendation on tracking Chinese investment in the United States. We already have a process for blocking investments that raise national security issues. Recently updated by the Congress, it appears to be working smoothly. No doubt, there will be proposed Chinese investments that will be blocked, but there are also investments that will bring jobs and economic growth to our country, and we should welcome those as a constructive means of returning some of the dollars that China has accumulated. The recommendation is only for reporting, but it encourages a climate of paranoia about Chinese activities here that does not serve us well economically and does not dignify us as a people.

Likewise, the Commission’s recommendations for a GAO study of U.S. firms’ operations in China and a report on possible procurement of Chinese goods and services through federally subsidized contracts will contribute to the same climate while providing little useful information.

These recommendations are not in and of themselves fatal flaws in our report, but they reflect a disturbing trend in our country towards economic nationalism that focuses on finding people to blame for our problems rather than on what we must do to solve them. While this report is hardly the worst example of this trend, the Commission has missed an opportunity to rise above it and emphasize constructive rather than confrontational solutions.

In the long run, a constructive approach will be required. China is in the process of assuming a global role commensurate with its size, potential, and aspirations. As it does so, it is in our interest, as well as China’s and everyone else’s, that it take on the obligations of leadership, which require a degree of self-abnegation. China’s leaders have demonstrated that they have a clear understanding of what is in their immediate interest. Their challenge will be to demonstrate they also understand what is in the larger interest of the global system of which they are a part, that the health of that system is inextricably tied with their own, and that they are prepared to act on that understanding. The Commission’s job is to continue to make that point.



### **ADDITIONAL VIEWS OF COMMISSIONERS ROBIN CLEVELAND AND WILLIAM A. REINSCH**

The Commission's report provides a frank assessment of China's economic and political policies designed to protect the Communist Party's agenda of stability, growth and self-preservation. U.S. and European policy makers and investors have expressed well founded concern about China's increasing efforts to protect and promote domestic industries by relying on market barriers, pressure to transfer technology, and capital control policies. Notwithstanding these concerns, US foreign direct investment continues to grow year on year as China continues to be viewed as a key market opportunity.

As noted in the report, US economic growth and export strength relies on the production of advanced technology and equipment including aircraft, medical and scientific equipment and energy related machinery. Since 2004, China has captured a larger share of the advanced technology market as evidenced by the fact that US imports of Chinese advanced technology exceeded \$10 billion, while American exports fell slightly under \$2 billion. While troubling, not all of this trade imbalance can be explained by China's aggressive mix of corporate subsidies, tax incentives, protectionism and industrial policy as the report might lead any reader to conclude.

In briefings and conversations with American corporate leaders, opportunity in China is viewed both in terms of "pull" and "push". The pull is obvious; the Chinese attract direct investment with various commercial incentives and the prospect of market opportunities. What the report fails to discuss are the reasons US companies feel pushed to move productive capacity to China. For example, in two sections in the report, GE is singled out for its decision to establish a joint venture in integrated modular avionics with the Aviation Industry Corporation of China. While several other companies are involved in similar aviation related joint ventures, the report irresponsibly relies on anonymous sources from press accounts to make a case that there are unique risks of diversion of GE's civilian technology for Chinese military purposes, notwithstanding the fact that the US government approved the transaction. As is the case with much of the report, the Commission's emphasis on China's aggressive acquisitive strategy and pursuit of security interests has the effect of presenting US companies in the unfair light of appearing to facilitate Chinese goals. The report fails to discuss key elements of business decisions GE and other companies have offered as reasons they are pushed to move production and jobs overseas.

In both hearings and meetings, witnesses have cited increasing and excessive US regulation and onerous tax burdens as among the principal business-based reasons for moving abroad. While the Commission views its primary responsibility as serving the Congress by evaluating China's security and economic policies and their impact on the United States, that focus, unfortunately, only provides a partial accounting of the reasons for our significant trade imbalances and weakening manufacturing base. Criticizing US companies for making business based decisions to prosper and drawing attention to China's aggressive and often unfair policies and practices alone will not reverse the dangerous trends in US-

China economic ties. To assure Members of Congress have a full and balanced set of options, the Commission's report should include witness' policy views and recommendations addressing the domestic factors which push US companies to move production and jobs to China.

**ADDITIONAL VIEWS OF COMMISSIONERS  
CAROLYN BARTHOLOMEW AND  
DR. LARRY WORTZEL**

In previous reports, the Commission has examined some of China's influence operation tools, including its mass media outlets, lobbyists, think tanks, and academic institutions. This year, chapter 4 looks at how China is using intelligence organizations in quasi-official (track two) policy and academic exchanges.

We believe that the Commission's research reveals that the Chinese government, through the intelligence component of the People's Liberation Army (PLA), targets retired U.S. senior-ranking flag officers as a means to convey propaganda messages and conduct perception management. This dissent expresses our disappointment that the Commission did not include in this report a vigorous explanation of this effort by the PLA and its China Association for International Friendly Contact (CAIFC).

One venue for this targeting is track two exchanges. Track two exchanges can serve useful purposes, facilitating dialogue between scholars and former government officials, increasing communication and understanding. They can also serve other, less laudable goals. Chinese participants in track two activities are vetted by, approved by, and controlled by, the Chinese Communist Party; these participants include the former chief of intelligence for the PLA, the former commander of the Nanjing Military Region (which is opposite Taiwan), and the former commander of the PLA Navy's East Sea Fleet (whose operational area includes the waters around Taiwan).

Some of the U.S. participants in these exchanges have business interests in China, which they expand through close contact with Chinese officials and former officials. Track two exchanges are useful venues to cultivate those contacts. The retired U.S. senior-rank officers also have continuing relationships with high-ranking U.S. officials with whom they previously served and with whom some communicate about their track two findings.

Inquiries made to a Commissioner by House and Senate offices and witness testimony led Commission staff to examine one particular track two exchange, the Sanya initiative. The research raises some serious questions.

The Sanya initiative was started by Admiral William Owens (USN-ret) and the China Association for International Friendly Contact. CAIFC is a front organization for the International Liaison Department of the People's Liberation Army's General Political Department, which is responsible both for intelligence collection and conducting People's Republic of China propaganda and perception management campaigns, particularly focused on foreign military forces. Admiral Owens is the former vice chairman of the Joint Chiefs of Staff. He started consulting for Huawei, the Chinese telecommunications company, in September 2009, and founded Amerilink Telecom, a start-up helping Huawei to gain access to the U.S. market. Some Members of Congress and Commissioners have voiced concern about possible Huawei ties to the Chinese military and state security apparatus and the national security implications of its participation in the U.S. market. (For example, Huawei's

chairwoman, Sun Yafang, worked for the Ministry of State Security's Communications Department before joining the company.)

The Commission's research documented participants in Sanya initiative exchanges, Chinese foreign policy propaganda messages, and follow-up meetings that some of the former U.S. military participants held with currently serving officials. It also reviewed articles published by these U.S. participants and tracked how the articles reflected Chinese government messaging. It is possible, of course, that the U.S. participants were only espousing views that they already held. We need to ensure, though, that they are not using their former positions in violation of the public trust and the positions they once held to the detriment of U.S. national security all for the benefit of their own financial interests.

We are disappointed that the Commission, while in possession of the facts, chose not to include this information in the 2011 Report. We believe that the issue warrants a deeper and more thorough investigation by the U.S. Congress.

## APPENDIX I

### UNITED STATES–CHINA ECONOMIC AND SECURITY REVIEW COMMISSION CHARTER

#### 22 U.S.C. 7002 (2001)

The Commission was created on October 30, 2000, by the Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Pub. L. No. 106–398, 114 STAT. 1654A–334 (2000) (codified at 22 U.S.C. § 7002 (2001), as amended by the Treasury and General Government Appropriations Act for 2002 § 645 (regarding employment status of staff) & § 648 (regarding changing annual report due date from March to June), Pub. L. No. 107–67, 115 STAT. 514 (November 12, 2001); as amended by Division P of the “Consolidated Appropriations Resolution, 2003,” Pub. L. No. 108–7 (February 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of Commission); as amended by Pub. L. No. 109–108 (enacted November 22, 2005) (regarding responsibilities of Commission and applicability of FACA); as amended by Pub. L. No. 110–161 (enacted December 26, 2007) (regarding changing annual report due date from June to December; reporting unobligated balances and submission of quarterly financial reports; deemed Commission a committee of Congress for printing and binding costs; amended employee compensation levels, and performance-based reviews and awards subject to Title 5 USC; and directed that travel by members of the Commission and its staff shall be arranged and conducted under the rules and procedures applying to travel by members of the House of Representatives and its staff).

#### **§ 7002. United States-China Economic and Security Review Commission**

(a) Purposes. The purposes of this section are as follows:

(1) To establish the United States-China Economic and Security Review Commission to review the national security implications of trade and economic ties between the United States and the People’s Republic of China.

(2) To facilitate the assumption by the United States-China Economic and Security Review Commission of its duties regarding the review referred to in paragraph (1) by providing for the transfer to that Commission of staff, materials, and infrastructure (including leased premises) of the Trade Deficit Review Commission that are appropriate for the review upon the submittal of the final report of the Trade Deficit Review Commission.

(b) Establishment of United States-China Economic and Security Review Commission.



(1) In general. There is hereby established a commission to be known as the United States-China Economic and Security Review Commission (in this section referred to as the “Commission”).

(2) Purpose. The purpose of the Commission is to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People’s Republic of China.

(3) Membership. The United States-China Economic and Security Review Commission shall be composed of 12 members, who shall be appointed in the same manner provided for the appointment of members of the Trade Deficit Review Commission under section 127(c)(3) of the Trade Deficit Review Commission Act (19 U.S.C. 2213 note), except that—

(A) Appointment of members by the Speaker of the House of Representatives shall be made after consultation with the chairman of the Committee on Armed Services of the House of Representatives, in addition to consultation with the chairman of the Committee on Ways and Means of the House of Representatives provided for under clause (iii) of subparagraph (A) of that section;

(B) Appointment of members by the President pro tempore of the Senate upon the recommendation of the majority leader of the Senate shall be made after consultation with the chairman of the Committee on Armed Services of the Senate, in addition to consultation with the chairman of the Committee on Finance of the Senate provided for under clause (i) of that subparagraph;

(C) Appointment of members by the President pro tempore of the Senate upon the recommendation of the minority leader of the Senate shall be made after consultation with the ranking minority member of the Committee on Armed Services of the Senate, in addition to consultation with the ranking minority member of the Committee on Finance of the Senate provided for under clause (ii) of that subparagraph;

(D) Appointment of members by the minority leader of the House of Representatives shall be made after consultation with the ranking minority member of the Committee on Armed Services of the House of Representatives, in addition to consultation with the ranking minority member of the Committee on Ways and Means of the House of Representatives provided for under clause (iv) of that subparagraph;

(E) Persons appointed to the Commission shall have expertise in national security matters and United States-China relations, in addition to the expertise provided for under subparagraph (B)(i)(I) of that section;

(F) Each appointing authority referred to under subparagraphs (A) through (D) of this paragraph shall—

(i) appoint 3 members to the Commission;

(ii) make the appointments on a staggered term basis, such that—

(I) 1 appointment shall be for a term expiring on December 31, 2003;

(II) 1 appointment shall be for a term expiring on December 31, 2004; and

(III) 1 appointment shall be for a term expiring on December 31, 2005;

(iii) make all subsequent appointments on an approximate 2-year term basis to expire on December 31 of the applicable year; and

(iv) make appointments not later than 30 days after the date on which each new Congress convenes.

(G) Members of the Commission may be reappointed for additional terms of service as members of the Commission; and

(H) Members of the Trade Deficit Review Commission as of the date of the enactment of this Act [enacted Oct. 30, 2000] shall serve as members of the United States-China Economic and Security Review Commission until such time as members are first appointed to the United States-China Economic and Security Review Commission under this paragraph.

(4) Retention of support. The United States-China Economic and Security Review Commission shall retain and make use of such staff, materials, and infrastructure (including leased premises) of the Trade Deficit Review Commission as the United States-China Economic and Security Review Commission determines, in the judgment of the members of the United States-China Economic and Security Review Commission, are required to facilitate the ready commencement of activities of the United States-China Economic and Security Review Commission under subsection (c) or to carry out such activities after the commencement of such activities.

(5) Chairman and vice chairman. The members of the Commission shall select a Chairman and Vice Chairman of the Commission from among the members of the Commission.

(6) Meetings.

(A) Meetings. The Commission shall meet at the call of the Chairman of the Commission.

(B) Quorum. A majority of the members of the Commission shall constitute a quorum for the transaction of business of the Commission.

(7) Voting. Each member of the Commission shall be entitled to one vote, which shall be equal to the vote of every other member of the Commission.

(c) Duties.

(1) Annual report. Not later than June 1 each year [beginning in 2002], the Commission shall submit to Congress a report, in both unclassified and classified form, regarding the national security implications and impact of the bilateral trade and economic relationship between the United States and the People's Republic of China. The report shall include a full analysis, along with conclusions and recommendations for legislative and administrative actions, if any, of the national security implications for the United States of the trade and current balances with the People's Republic of China in goods and services, financial transactions, and technology transfers. The Commission shall also take into account patterns of trade and transfers through third countries to the extent practicable.

(2) Contents of report. Each report under paragraph (1) shall include, at a minimum, a full discussion of the following:

(A) The portion of trade in goods and services with the United States that the People's Republic of China dedicates to military systems or systems of a dual nature that could be used for military purposes.

(B) The acquisition by the People's Republic of China of advanced military or dual-use technologies from the United States by trade (including procurement) and other technology transfers, especially those transfers, if any, that contribute to the proliferation of weapons of mass destruction or their delivery systems, or that undermine international agreements or United States laws with respect to nonproliferation.

(C) Any transfers, other than those identified under subparagraph (B), to the military systems of the People's Republic of China made by United States firms and United States-based multinational corporations.

(D) An analysis of the statements and writing of the People's Republic of China officials and officially-sanctioned writings that bear on the intentions, if any, of the Government of the People's Republic of China regarding the pursuit of military competition with, and leverage over, or cooperation with, the United States and the Asian allies of the United States.

(E) The military actions taken by the Government of the People's Republic of China during the preceding year that bear on the national security of the United States and the regional stability of the Asian allies of the United States.

(F) The effects, if any, on the national security interests of the United States of the use by the People's Republic of China of financial transactions and capital flow and currency manipulations.

(G) Any action taken by the Government of the People's Republic of China in the context of the World Trade Organization that is adverse or favorable to the United States national security interests.

(H) Patterns of trade and investment between the People's Republic of China and its major trading partners, other than the United States, that appear to be substantively different from trade and investment patterns with the United States and whether the differences have any national security implications for the United States.

(I) The extent to which the trade surplus of the People's Republic of China with the United States enhances the military budget of the People's Republic of China.

(J) An overall assessment of the state of the security challenges presented by the People's Republic of China to the United States and whether the security challenges are increasing or decreasing from previous years.

(3) Recommendations of report. Each report under paragraph (1) shall also include recommendations for action by Congress or the President, or both, including specific recommendations for the United States to invoke Article XXI (relating to security exceptions) of the General Agreement on Tariffs and Trade 1994 with respect to the People's Republic of China, as a result of any adverse impact on the national security interests of the United States.

(d) Hearings.

(1) In general. The Commission or, at its direction, any panel or member of the Commission, may for the purpose of carrying out the provisions of this section, hold hearings, sit and act at times and places, take testimony, receive evidence, and administer oaths to the extent that the Commission or any panel or member considers advisable.

(2) Information. The Commission may secure directly from the Department of Defense, the Central Intelligence Agency, and any other Federal department or agency information that the Commission considers necessary to enable the Commission to carry out its duties under this section, except the provision of intelligence information to the Commission shall be made with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, under procedures approved by the Director of Central Intelligence.

(3) Security. The Office of Senate Security shall—

(A) provide classified storage and meeting and hearing spaces, when necessary, for the Commission; and

(B) assist members and staff of the Commission in obtaining security clearances.

(4) Security clearances. All members of the Commission and appropriate staff shall be sworn and hold appropriate security clearances.

(e) Commission personnel matters.

(1) Compensation of members. Members of the United States-China Economic and Security Review Commission shall be compensated in the same manner provided for the compensation of members of the Trade Deficit Review Commission under section 127(g)(1) and section 127(g)(6) of the Trade Deficit Review Commission Act [19 U.S.C. 2213 note].

(2) Travel expenses. Travel expenses of the United States-China Economic and Security Review Commission shall be allowed in the same manner provided for the allowance of the travel expenses of the Trade Deficit Review Commission under section 127(g)(2) of the Trade Deficit Review Commission Act [19 U.S.C. § 2213 note].

(3) Staff. An executive director and other additional personnel for the United States-China Economic and Security Review Commission shall be appointed, compensated, and terminated in the same manner provided for the appointment, compensation, and termination of the executive director and other personnel of the Trade Deficit Review Commission under section 127(g)(3) and section 127(g)(6) of the Trade Deficit Review Commission Act [19 U.S.C. § 2213 note]. The executive director and any personnel who are employees of the United States-China Economic and Security Review Commission shall be employees under section 2105 of title 5, United States Code, for purposes of chapters 63, 81, 83, 84, 85, 87, 89, and 90 of that title [language of 2001 amendment, Sec. 645].

(4) Detail of government employees. Federal Government employees may be detailed to the United States-China Economic and Security Review Commission in the same manner provided for the detail of Federal Government employees to the Trade Deficit Review Commission under section 127(g)(4) of the Trade Deficit Review Commission Act [19 U.S.C. § 2213 note].

(5) Foreign travel for official purposes. Foreign travel for official purposes by members and staff of the Commission may be authorized by either the Chairman or the Vice Chairman of the Commission.

(6) Procurement of temporary and intermittent services. The Chairman of the United States-China Economic and Security Re-

view Commission may procure temporary and intermittent services for the United States-China Economic and Security Review Commission in the same manner provided for the procurement of temporary and intermittent services for the Trade Deficit Review Commission under section 127(g)(5) of the Trade Deficit Review Commission Act [19 U.S.C. § 2213 note].

(f) Authorization of appropriations.

(1) In general. There is authorized to be appropriated to the Commission for fiscal year 2001, and for each fiscal year thereafter, such sums as may be necessary to enable the Commission to carry out its functions under this section.

(2) Availability. Amounts appropriated to the Commission shall remain available until expended.

(g) Federal Advisory Committee Act. The provisions of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Commission.

(h) Effective date. This section shall take effect on the first day of the 107th Congress.

#### **Amendments:**

SEC. 645. (a) Section 1238(e)(3) of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (as enacted by Public Law 106–398) is amended by adding at the end the following: “The executive director and any personnel who are employees of the United States-China Economic and Security Review Commission shall be employees under section 2105 of title 5, United States Code, for purposes of chapters 63, 81, 83, 84, 85, 87, 89, and 90 of that title.” (b) The amendment made by this section shall take effect on January 3, 2001.”

SEC. 648. DEADLINE FOR SUBMISSION OF ANNUAL REPORTS BY UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. Section 1238(c)(1) of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (as enacted into law by section I of Public Law 106–398) is amended by striking “March” and inserting “June”.

Changes: Enacted into law by Division P of the “Consolidated Appropriations Resolution, 2003” Pub. L. No. 108–7 dated February 20, 2003:

H. J. Res. 2—

#### **DIVISION P—UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION**

SECTION 1. SHORT TITLE.—This division may be cited as the “United States-China Economic and Security Review Commission”.

SEC. 2. (a) APPROPRIATIONS.—There are appropriated, out of any funds in the Treasury not otherwise appropriated, \$1,800,000, to remain available until expended, to the United States-China Economic and Security Review Commission.

(b) NAME CHANGE.—

(1) IN GENERAL.—Section 1238 of the Floyd D. Spence National Defense Authorization Act of 2001 (22 U.S.C. 7002) is amended— as follows:



In each Section and Subsection where it appears, the name is changed to the “U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION”—

(2) REFERENCES.—Any reference in any Federal law, Executive Order, rule, regulation, or delegation of authority, or any document of or relating to the United States-China Security Review Commission shall be deemed to refer to the United States-China Economic and Security Review Commission.

(c) MEMBERSHIP, RESPONSIBILITIES, AND TERMS.—

(1) IN GENERAL.—Section 1238(b)(3) of the Floyd D. Spence National Defense Authorization Act of 2001 (22 U.S.C. 7002) is amended by striking subparagraph (F) and inserting the following:

“(F) each appointing authority referred to under subparagraphs (A) through (D) of this paragraph shall—

“(i) appoint 3 members to the Commission;

“(ii) make the appointments on a staggered term basis, such that—

“(I) 1 appointment shall be for a term expiring on December 31, 2003;

“(II) 1 appointment shall be for a term expiring on December 31, 2004; and

“(III) 1 appointment shall be for a term expiring on December 31, 2005;

“(iii) make all subsequent appointments on an approximate 2-year term basis to expire on December 31 of the applicable year; and

“(iv) make appointments not later than 30 days after the date on which each new Congress convenes;”.

SEC. 635. (a) Modification of Responsibilities.—Notwithstanding any provision of section 1238 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (22 U.S.C. 7002), or any other provision of law, the United States-China Economic and Security Review Commission established by subsection (b) of that section shall investigate and report exclusively on each of the following areas:

(1) PROLIFERATION PRACTICES.—The role of the People’s Republic of China in the proliferation of weapons of mass destruction and other weapons (including dual use technologies), including actions, the United States might take to encourage the People’s Republic of China to cease such practices.

(2) ECONOMIC TRANSFERS.—The qualitative and quantitative nature of the transfer of United States production activities to the People’s Republic of China, including the relocation of high technology, manufacturing, and research and development facilities, the impact of such transfers on United States national security, the adequacy of United States export control laws, and the effect of such transfers on United States economic security and employment.

(3) ENERGY.—The effect of the large and growing economy of the People’s Republic of China on world energy supplies and the role the United States can play (including joint research and development efforts and technological assistance), in influencing the energy policy of the People’s Republic of China.

(4) UNITED STATES CAPITAL MARKETS.—The extent of access to and use of United States capital markets by the People's Republic of China, including whether or not existing disclosure and transparency rules are adequate to identify People's Republic of China companies engaged in harmful activities.

(5) REGIONAL ECONOMIC AND SECURITY IMPACTS.—The triangular economic and security relationship among the United States, Taipei and the People's Republic of China (including the military modernization and force deployments of the People's Republic of China aimed at Taipei), the national budget of the People's Republic of China, and the fiscal strength of the People's Republic of China in relation to internal instability in the People's Republic of China and the likelihood of the externalization of problems arising from such internal instability.

(6) UNITED STATES-CHINA BILATERAL PROGRAMS.—Science and technology programs, the degree of non-compliance by the People's Republic of China with agreements between the United States and the People's Republic of China on prison labor imports and intellectual property rights, and United States enforcement policies with respect to such agreements.

(7) WORLD TRADE ORGANIZATION COMPLIANCE.—The compliance of the People's Republic of China with its accession agreement to the World Trade Organization (WTO).

(8) FREEDOM OF EXPRESSION.—The implications of restrictions on speech and access to information in the People's Republic of China for its relations with the United States in the areas of economic and security policy.

(b) Applicability of Federal Advisory Committee Act.—Subsection (g) of section 1238 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 is amended to read as follows:

(g) Applicability of FACA.—The provisions of the Federal Advisory Committee Act (5 U.S.C. App.) shall apply to the activities of the Commission.

The effective date of these amendments shall take effect on the date of enactment of this Act [November 22, 2005].

*Changes:* Enacted into law by the Consolidated Appropriations Act, 2008, Pub. L. No. 110–161 dated December 26, 2007:

H.R. 2764—

For necessary expenses of the United States-China Economic and Security Review Commission, \$4,000,000, including not more than \$4,000 for the purpose of official representation, to remain available until September 30, 2009: *Provided*, That the Commission shall submit a spending plan to the Committees on Appropriations no later than March 1, 2008, which effectively addresses the recommendations of the Government Accountability Office's audit of the Commission (GAO–07–1128): *Provided further*, That the Commission shall provide to the Committees on Appropriations a quarterly accounting of the cumulative balances of any unobligated funds that were received by the Commission during any previous fiscal year: *Provided further*, That for purposes of costs relating to printing and binding, the Commission shall be deemed, effective on the date of its establishment, to be a committee of Congress: *Provided further*, That compensation for the executive director of the Commission may not exceed the rate payable for level II of the Ex-

ecutive Schedule under section 5314 of title 5, United States Code: *Provided further*, That section 1238(c)(1) of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, is amended by striking “June” and inserting “December”: *Provided further*, That travel by members of the Commission and its staff shall be arranged and conducted under the rules and procedures applying to travel by members of the House of Representatives and its staff.

#### COMMISSION FINANCIAL MANAGEMENT

SEC. 118. (a) REQUIREMENT FOR PERFORMANCE REVIEWS.—The United States-China Economic and Security Review Commission shall comply with chapter 43 of title 5, United States Code, regarding the establishment and regular review of employee performance appraisals.

(b) LIMITATION ON CASH AWARDS.—The United States-China Economic and Security Review Commission shall comply with section 4505a of title 5, United States Code, with respect to limitations on payment of performance-based cash awards.



## APPENDIX II

### BACKGROUND OF COMMISSIONERS

#### **The Honorable William A. Reinsch, Chairman**

Chairman William Reinsch was reappointed to the Commission by Senate Democratic Leader Harry Reid for a term expiring December 31, 2011. Chairman Reinsch served as Under Secretary for Export Administration in the U.S. Department of Commerce. As head of the Bureau of Export Administration, later named the Bureau of Industry and Security, Chairman Reinsch was charged with administering and enforcing the export control policies of the U.S. government, including its antiboycott laws. Major accomplishments during his tenure included refocusing controls regarding economic globalization, most notably on high-performance computers, microprocessors, and encryption, completing the first revisions of the Export Administration regulations in over 40 years. In addition, he revised the interagency process for reviewing applications and permitted electronic filing of applications over the Internet.

During this time, Chairman Reinsch delivered more than 200 speeches and testified 53 times before various committees of the Congress. Before joining the Department of Commerce, Mr. Reinsch was a senior legislative assistant to Senator John Rockefeller and was responsible for the senator's work on trade, international economic policy, foreign affairs, and defense. He also provided staff support for Senator Rockefeller's related efforts on the Finance Committee and the Commerce, Science, and Transportation Committee.

For over a decade, Chairman Reinsch served on the staff of Senator John Heinz as chief legislative assistant, focusing on foreign trade and competitiveness policy issues. During that period, Senator Heinz was either the chairman or the ranking member of the Senate Banking Committee's Subcommittee on International Finance. Senator Heinz was also a member of the International Trade Subcommittee of the Finance Committee. Mr. Reinsch provided support for the senator on both subcommittees. This work included five revisions of the Export Administration Act and work on four major trade bills. Prior to joining Senator Heinz's staff, Chairman Reinsch was a legislative assistant to Representatives Richard Ottinger and Gilbert Gude, acting staff director of the House Environmental Study Conference, and a teacher in Maryland.

Today Chairman Reinsch is president of the National Foreign Trade Council. Founded in 1914, the council is the only business organization dedicated solely to trade policy, export finance, international tax, and human resources issues. The organization represents over 300 companies through its offices in New York City and Washington.



In addition to his legislative and private sector work, Chairman Reinsch served as an adjunct associate professor at the University of Maryland University College Graduate School of Management and Technology, teaching a course in international trade and trade policy. He is also a member of the boards of the Executive Council on Diplomacy and KHI Services, Incorporated. Chairman Reinsch's publications include "Why China Matters to the Health of the U.S. Economy," published in *Economics and National Security*; "The Role and Effectiveness of U.S. Export Control Policy in the Age of Globalization" and "Export Controls in the Age of Globalization," both published in *The Monitor*. In addition, Chairman Reinsch has published "Should Uncle Sam Control U.S. Technology Exports," published in *Insight Magazine*; "Encryption Policy Strikes a Balance," published in the *Journal of Commerce*; and "Building a New Economic Relationship with Japan," published with others in *Beyond the Beltway: Engaging the Public in U.S. Foreign Policy*.

#### **Daniel M. Slane, Vice Chairman**

Daniel Slane was reappointed to the Commission by House Republican Leader John Boehner for a two-year term expiring on December 31, 2011. Vice Chairman Slane was elected as the Commission's vice chairman for the 2011 report cycle and served as the Commission's chairman for the 2010 report cycle.

Vice Chairman Slane served for two years on active duty as a U.S. Army Captain in Military Intelligence; in addition he served for a number of years as a case officer with the U.S. Central Intelligence Agency. Vice Chairman Slane worked in The White House during the Ford Administration.

In 1996, Vice Chairman Slane became a member of the board of trustees of The Ohio State University and was chairman from 2005 to 2006. Ohio State University is the nation's largest university, with an annual budget of over \$4 billion. He is also the former chairman of University Hospital, a 1,000 bed regional hospital in Columbus, and the former chairman of the James Cancer Hospital, a National Cancer Institute Comprehensive Cancer Center. Vice Chairman Slane serves on the board of two financial institutions and a number of nonprofit organizations.

Vice Chairman Slane is the founder and co-owner of the Slane Company, whose principal business includes real estate development, lumber, and furniture. He has extensive international business experience, including operating a business in China. Prior to becoming a member of the Commission, Vice Chairman Slane manufactured plywood and related wood products at factories in Harbin, Dalian, and Balu (Pizhou), China. In 2007, he sold his interest in that company.

Vice Chairman Slane received a Bachelor of Science in Business Administration and a Juris Doctorate from The Ohio State University. He holds a Master's Degree in International Law from the Europa Institute at the University of Amsterdam in The Netherlands. Vice Chairman Slane is a member of the Ohio Bar and formerly a partner in the law firm of Grieser, Schafer, Blumenstiel, and Slane.

### **Carolyn Bartholomew**

Carolyn Bartholomew was reappointed to the Commission by House Speaker Nancy Pelosi for a two-year term expiring on December 31, 2011. She previously served as the Commission's chairman for the 2007 and 2009 report cycles and as vice chairman for the 2010, 2008, and 2006 report cycles.

Commissioner Bartholomew has worked at senior levels in the U.S. Congress, serving as counsel, legislative director, and chief of staff to now House Democratic Leader Nancy Pelosi. She was a professional staff member on the House Permanent Select Committee on Intelligence and also served as a legislative assistant to then-U.S. Representative Bill Richardson. In these positions, Commissioner Bartholomew was integrally involved in developing U.S. policies on international affairs and security matters. She has particular expertise in U.S.-China relations, including issues related to trade, human rights, and the proliferation of weapons of mass destruction. Ms. Bartholomew led efforts in the establishment and funding of global AIDS programs and the promotion of human rights and democratization in countries around the world. She was a member of the first Presidential Delegation to Africa to Investigate the Impact of HIV/AIDS on Children and a member of the Council on Foreign Relations Congressional Staff Roundtable on Asian Political and Security Issues.

In addition to U.S.-China relations, her areas of expertise include terrorism, trade, proliferation of weapons of mass destruction, human rights, U.S. foreign assistance programs, and international environmental issues. Currently, she serves on the board of directors of the Kaiser Aluminum Corporation and the nonprofit organizations Polaris Project and Asia Catalyst.

Commissioner Bartholomew received a Bachelor of Arts degree from the University of Minnesota, a Master of Arts in Anthropology from Duke University, and a Juris Doctorate from Georgetown University Law Center. She is a member of the State Bar of California.

### **Daniel A. Blumenthal**

Daniel Blumenthal was reappointed to the Commission by Senate Republican Leader Mitch McConnell for a two-year term expiring December 31, 2011. Commissioner Blumenthal served as the Commission's vice chairman for the 2007 report cycle.

Commissioner Blumenthal was the country director for China, Taiwan, and Hong Kong in the Office of the Assistant Secretary of Defense for International Security Affairs, later becoming a senior director for China, Taiwan, Hong Kong, and Mongolia during the first term of President George W. Bush. Commissioner Blumenthal developed and implemented defense policy toward China, Taiwan, Hong Kong, and Mongolia. Commissioner Blumenthal was awarded the Office of the Secretary of Defense Medal for Exceptional Public Service.

Prior to joining the Defense Department, Commissioner Blumenthal was an associate attorney in the Corporate and Asia Practice Groups at Kelly Drye & Warren LLP. Earlier, he was an editorial and research assistant for *Near East Policy*.

Today, Commissioner Blumenthal is the director of Asian Studies and a resident fellow at the American Enterprise Institute for Public Policy Research, and a research associate with the National Asia Research Program. He is a member of the Academic Advisory Group of the Congressional U.S.-China Working Group and has been a member of the Project 2049 Institute's board of advisors since 2008. In addition, Commissioner Blumenthal has written extensively on national security issues. He has written articles and op-eds for the *Washington Post*, the *Wall Street Journal*, the *Weekly Standard*, *National Review*, and numerous edited volumes.

Commissioner Blumenthal received a Master of Arts in International Relations and International Economics from The Johns Hopkins University School of Advanced International Studies and a Juris Doctorate from Duke University.

#### **Peter T.R. Brookes**

Commissioner Brookes was reappointed to the Commission by House Republican Leader John Boehner for a two-year term expiring December 31, 2011. Commissioner Brookes is currently a senior fellow for National Security Affairs at The Heritage Foundation. Prior to Heritage, he served in the George W. Bush Administration as the deputy assistant secretary of Defense for Asian and Pacific Affairs, with the Committee on International Relations in the U.S. House of Representatives, at the Central Intelligence Agency, at the State Department at the United Nations, in the defense industry, and in the U.S. Navy. He is a doctoral candidate at Georgetown University, and a graduate of the U.S. Naval Academy, the Defense Language Institute, the Naval War College, and The Johns Hopkins University.

#### **Robin Cleveland**

Commissioner Cleveland was reappointed to the Commission by Senate Republican Leader Mitch McConnell for a two-year term expiring December 31, 2012. After three decades of government service, Commissioner Cleveland is now serving as a professional school counselor. Previously, Commissioner Cleveland worked for U.S. Senator Mitch McConnell in a number of senior positions on the Senate Select Committee on Intelligence, the Foreign Relations Committee, and the Senate Appropriations Committee. In addition, Commissioner Cleveland served as the counselor to the president of the World Bank, as the associate director of the Office of Management and Budget at The White House, and as principal with Olivet Consulting, LLC.

During her tenure in The White House, Commissioner Cleveland co-led the interagency effort to develop two presidential initiatives: the Millennium Challenge Corporation and the President's Emergency Plan for AIDS Relief. These efforts reflect her experience linking policy, performance, and resource management.

Commissioner Cleveland graduated from Wesleyan University with honors and received her M.A. in Education and Human Development from The George Washington University.

### **The Honorable C. Richard D'Amato**

Dick D'Amato was reappointed to the U.S.-China Economic and Security Review Commission by Senate Majority Leader Harry Reid on December 8, 2010, for a two-year term expiring December 31, 2012. He previously served on the Commission from March 2001 to December 2007, serving as the chairman and vice chairman of the Commission from April 2001 through December 20, 2005. He is an attorney and a member of the Maryland and DC Bars. He is a former delegate to the General Assembly of the State of Maryland (1998–2002), representing the Annapolis, Maryland, region, and served on the Appropriations Committee. He is also a retired captain in the United States Navy Reserve, served two tours of duty in the Vietnam theatre aboard the *USS KING* (DLG–10), and three years as an assistant professor of Government at the U.S. Naval Academy. He served on the Trade Deficit Review Commission, a Congressional advisory body, as a member from 1999 to 2000.

He served as vice president for development of Synergics, Inc., an international energy company and developer of alternative energy projects, particularly wind energy. He also serves as an official presenter and participant in former Vice President Gore's climate project, serves as a member of Maryland Governor O'Malley's commission on climate change, and is a trustee of St. Mary's College of Maryland.

From 1988 to 1998, Commissioner D'Amato was the Democratic counsel for the Committee on Appropriations of the U.S. Senate. He was responsible for coordinating and managing the annual appropriations bills and other legislation on policy and funding of U.S. defense, foreign policy, trade, and intelligence matters. He served from 1980 to 1988 as senior foreign policy and defense advisor to the former Democratic Senate leader, Senator Robert C. Byrd. In this position, he supervised work on major foreign policy, national security, and trade policies and was the co-director for the Senate Arms Control Observer Group, a bipartisan leadership organization, which served as liaison with The White House on all arms control negotiations with the Soviet Union. He also served on the Senate delegation to the Kyoto negotiations on global warming.

Mr. D'Amato began his career as legislative director for Congressman James Jeffords (Ind.–VT) from 1975 to 1978 and then as chief of staff for Senator Abraham Ribicoff (D–CT) until 1980.

He has been active in other aspects of public service, having founded the annual Taste-of-the-Nation dinner in Annapolis as part of the nationwide "Share Our Strength" hunger relief organization and created an annual scholarship for college-bound African-American women in Anne Arundel County, Maryland. He currently serves on the boards of the Annapolis Symphony Orchestra, the Annapolis Maritime Museum, The Johns Hopkins Cuba Exchange Program, and the University of Oxford Congressional Visitors program. He is a founding member of the National Sailing Hall of Fame.

Commissioner D'Amato received his B.A. (cum laude) from Cornell University in 1964 and served on the Cornell board of trustees' Advisory Council. He received his M.A. from the Fletcher School of Law and Diplomacy in Boston in 1967, and received his legal education from Harvard Law School and from the Georgetown Univer-

sity Law Center (J.D., 1980). He resides in Annapolis with his wife, Dee.

#### **Jeffrey L. Fiedler**

Commissioner Fiedler was reappointed to the Commission by House Speaker Nancy Pelosi on December 16, 2009, for a third term expiring December 31, 2011. He is assistant to the general president, and director, Special Projects and Initiatives, for the International Union of Operating Engineers. Previously, he was President of Research Associates of America (RAA) and the elected president of the Food and Allied Service Trades Department, AFL–CIO (“FAST”). This constitutional department of the AFL–CIO represented ten unions with a membership of 3.5 million in the United States and Canada. The focus of RAA, like FAST before it, was organizing and bargaining research for workers and their unions.

He served as a member of the AFL–CIO Executive Council committees on International Affairs, Immigration, Organizing, and Strategic Approaches. He also served on the board of directors of the Consumer Federation of America and is a member of the Council on Foreign Relations. In 1992, Mr. Fiedler co-founded the Laogai Research Foundation (LRF), an organization devoted to studying the forced labor camp system in China. When the foundation’s Executive Director, Harry Wu, was detained in China in 1995, Mr. Fiedler coordinated the campaign to win his release. He no longer serves as a director of the LRF.

Mr. Fiedler has testified on behalf of the AFL–CIO before the Senate Foreign Relations Committee and the House International Affairs Committee and its various subcommittees, as well as the Trade Subcommittee of the House Ways and Means Committee concerning China policy. He attended three of the American Assembly conferences on China sponsored by Columbia University and has participated in a Council on Foreign Relations task force and study group on China. He has been interviewed on CBS, NBC, ABC, CNN, and CNBC on China policy, international trade issues, human rights, and child labor.

A Vietnam veteran, he served with the U.S. Army in Hue in 1967–68. He received his B.A. in Political Science from Southern Illinois University. He is married with two adult children and resides in Virginia.

#### **The Honorable Patrick A. Mulloy**

Commissioner Patrick Mulloy has served four two-year terms as a commissioner and was reappointed in 2009 by Senate Democratic Leader Harry Reid for a new two-year term expiring December 31, 2011.

Commissioner Mulloy served as assistant secretary of Commerce for Market Access and Compliance in the department’s International Trade Administration during the second Clinton Administration. As assistant secretary, Commissioner Mulloy directed a trade policy unit of over 200 international trade specialists, which focused worldwide on removing foreign barriers to U.S. exports and on ensuring that foreign countries complied with trade agreements negotiated with the United States. This activity involved discus-



sions both in the World Trade Organization and with individual governments. Commissioner Mulloy traveled extensively, meeting with foreign leaders to advance market-opening programs in the European Union, China, India, Taiwan, Indonesia, Canada, and Central and South America. He was also appointed by President Clinton to serve as a member of the Commission on Security and Cooperation in Europe.

Before becoming assistant secretary, Commissioner Mulloy held various senior positions on the staff of the U.S. Senate Banking Committee, including chief international counsel and general counsel. In those positions, he contributed to much of the international trade and finance legislation formulated by the committee, such as the Foreign Bank Supervision Enhancement Act of 1991, the Export Enhancement Act of 1992, the Defense Production Act Amendments of 1994, and titles of the Omnibus Trade and Competitiveness Act of 1988 that dealt with foreign bribery, investment, exchange rates, and export controls.

Prior to his work in the Senate, Commissioner Mulloy was a senior attorney in the Antitrust Division of the Department of Justice, where he directed a staff of lawyers and economists who supervised participation of U.S. oil companies in the Paris-based International Energy Agency (IEA). In earlier duties at the Justice Department, he represented the United States in a variety of cases related to federal environmental laws, including criminal and civil enforcement actions in various U.S. district courts, several circuit courts of appeal, and the U.S. Supreme Court.

Commissioner Mulloy began his public service career as a foreign service officer, where he served in the Department of State's Office of United Nations Political Affairs, the Office of International Environmental and Oceans Affairs, and as vice counsel in the U.S. Consulate in Montreal, Canada.

Today, Commissioner Mulloy is a consultant to the president emeritus of the Alfred P. Sloan Foundation and is an adjunct professor of International Trade Law at the law schools of Catholic University and George Mason University. He is a member of the Asia Society and the Washington International Trade Association and serves on the advisory boards of the Center for the Study of the Presidency and Congress and of the Coalition for a Prosperous America. He has several times testified on international trade and investment matters before committees of the U.S. Senate and the House of Representatives.

Commissioner Mulloy, a native of Kingston, Pennsylvania, holds an LL.M. from Harvard University Law School, a Juris Doctorate from The George Washington University Law School, a Master of Arts from the University of Notre Dame, and a Bachelor of Arts from King's College. Commissioner Mulloy is a member of the District of Columbia and Pennsylvania Bars. He resides in Alexandria, Virginia, with his wife Marjorie, and they have three adult children.

#### **The Honorable Dennis C. Shea**

Commissioner Dennis Shea was reappointed by Senate Republican Leader Mitch McConnell for a two-year term expiring December 31, 2012. An attorney with 25 years of experience in govern-

ment and public policy, he is the founder of Shea Public Strategies LLC, a government relations firm based in Alexandria, Virginia. Before starting the firm, he served as vice president for Government Affairs—Americas for Pitney Bowes Inc., a Fortune 500 company.

Commissioner Shea's government service began in 1988 when he joined the Office of Senate Republican Leader Bob Dole as counsel, subsequently becoming the senator's deputy chief of staff in the Office of the Senate Majority Leader. In these capacities, he advised Senator Dole and other Republican senators on a broad range of domestic policy issues, was involved in the drafting of numerous pieces of legislation, and was recognized as one of the most influential staffers on Capitol Hill. In 1992, Commissioner Shea's service with Senator Dole was interrupted when he ran for Congress in the Seventh District of New York.

During the 1996 elections, Commissioner Shea continued to help shape the national public policy debate as the director of policy for the Dole for President Campaign. Following the elections, he entered the private sector, providing legislative and public affairs counsel to a wide range of clients while employed at BKSH & Associates and Verner, Liipfert, Bernhard, McPherson, and Hand.

In 2003, Commissioner Shea was named the executive director of the President's Commission on the United States Postal Service. Many of the Commission's recommendations were subsequently adopted in the landmark 2006 postal reform legislation.

In 2004, Commissioner Shea was confirmed as assistant secretary for Policy Development and Research at the U.S. Department of Housing and Urban Development. As assistant secretary, Commissioner Shea led a team responsible for conducting much of the critical analysis necessary to support the department's mission. In 2005, Commissioner Shea left to serve as senior advisor to Senator Elizabeth Dole in her capacity as chairman of the National Republican Senatorial Committee.

Commissioner Shea received a J.D., an M.A. in History, and a B.A. in Government from Harvard University. He is admitted to the bar in New York and the District of Columbia. He currently resides in Alexandria, Virginia, with his wife Elizabeth and daughter Juliette.

#### **Michael R. Wessel**

Commissioner Michael R. Wessel, an original member of the U.S.-China Economic and Security Review Commission, was reappointed by House Speaker Nancy Pelosi for a two-year term expiring December 31, 2012.

Commissioner Wessel served on the staff of House Democratic Leader Richard Gephardt for more than two decades, leaving his position as general counsel in March 1998. In addition, Commissioner Wessel was Congressman Gephardt's chief policy advisor, strategist, and negotiator. He was responsible for the development, coordination, management, and implementation of the Democratic leader's overall policy and political objectives, with specific responsibility for international trade, finance, economics, labor, and taxation.

During his more than 20 years on Capitol Hill, Commissioner Wessel served in a number of positions as Congressman Gephardt's principal Ways and Means aide, where he developed and implemented numerous tax and trade policy initiatives. He participated in the enactment of every major trade policy initiative from 1978 until his departure in 1998. In the late 1980s, he was the executive director of the House Trade and Competitiveness Task Force, where he was responsible for the Democrats' trade and competitiveness agenda as well as overall coordination of the Omnibus Trade and Competitiveness Act of 1988.

Commissioner Wessel was intimately involved in the development of comprehensive tax reform legislation in the early 1980s and every major tax bill during his tenure. Beginning in 1989, he became the principal advisor to the Democratic leadership on economic policy matters and served as tax policy coordinator to the 1990 budget summit. In 1995, he developed the Ten Percent Tax Plan, a comprehensive tax reform initiative that would enable roughly four out of five taxpayers to pay no more than a 10 percent rate in federal income taxes, the principal Democratic tax reform alternative.

In 1988, he served as national issues director for Congressman Gephardt's presidential campaign. During the 1992 presidential campaign, he assisted the Clinton presidential campaign on a broad range of issues and served as a senior policy advisor to the Clinton Transition Office. In 2004, he was a senior policy advisor to the Gephardt for President Campaign and later co-chaired the Trade Policy Group for the Kerry presidential campaign. In 2008, he was publicly identified as a trade and economic policy advisor to the Obama presidential campaign.

He has coauthored a number of articles with Congressman Gephardt, and a book, *An Even Better Place: America in the 21st Century*. Commissioner Wessel served as a member of the U.S. Trade Deficit Review Commission in 1999–2000, a congressionally created commission charged with studying the nature, causes, and consequences of the U.S. merchandise trade and current account deficits.

Today, Commissioner Wessel is president of The Wessel Group Incorporated, a public affairs consulting firm offering expertise in government, politics, and international affairs.

Commissioner Wessel is a member of the board of directors of Goodyear Tire and Rubber. Commissioner Wessel holds a Bachelor of Arts and a Juris Doctorate from The George Washington University. He is a member of the Bar of the District of Columbia and Pennsylvania and is a member of the Council on Foreign Relations. He and his wife Andrea have four children.

#### **Larry M. Wortzel, Ph.D.**

Larry Wortzel was reappointed by House Republican Leader John Boehner for a two-year term expiring December 31, 2012. Dr. Wortzel has served on the Commission since November 2001 and was the Commission's chairman for the 2006 and 2008 report cycles, and served as vice chairman for the 2009 report cycle.

A leading authority on China, Asia, national security, and military strategy, Commissioner Wortzel had a distinguished career in

the U.S. Armed Forces. Following three years in the marine corps, Commissioner Wortzel enlisted in the U.S. Army in 1970. His first assignment with the Army Security Agency took him to Thailand, where he focused on Chinese military communications in Vietnam and Laos. Within three years, he had graduated from the Infantry Officer Candidate School and the Airborne and Ranger schools. After four years as an infantry officer, Commissioner Wortzel shifted to military intelligence. Commissioner Wortzel traveled regularly throughout Asia while serving in the U.S. Pacific Command from 1978 to 1982. The following year, he attended the National University of Singapore, where he studied advanced Chinese and traveled in China and Southeast Asia. He next worked for the under secretary of Defense for Policy, developing counterintelligence programs to protect emerging defense technologies from foreign espionage. He also managed programs to gather foreign intelligence for the Army Intelligence and Security Command.

From 1988 to 1990, Commissioner Wortzel was the assistant army attaché at the U.S. embassy in Beijing, where he witnessed and reported on the 1989 Tiananmen Square Massacre. After assignments as an army strategist and managing army intelligence officers, he returned to China in 1995 as the army attaché. In December 1997, Commissioner Wortzel became a faculty member of the U.S. Army War College and served as the director of the Strategic Studies Institute. He retired from the army as a colonel.

After his military retirement, Commissioner Wortzel served as the director of the Asian Studies Center and vice president for foreign policy at The Heritage Foundation from 1999 to 2006. Commissioner Wortzel's books include *Class in China: Stratification in a Classless Society*; *China's Military Modernization: International Implications*; *The Chinese Armed Forces in the 21<sup>st</sup> Century*; and *Dictionary of Contemporary Chinese Military History*. Commissioner Wortzel regularly publishes articles on Asian security matters.

A graduate of the Armed Forces Staff College and the U.S. Army War College, Commissioner Wortzel earned his Bachelor of Arts from Columbus College and his Master of Arts and Ph.D. from the University of Hawaii. He and his wife, Christine, live in Williamsburg, Virginia. They have two married sons and three grandchildren.

#### **Michael R. Danis, Executive Director**

Before joining the U.S.-China Commission, Michael Danis served as an intelligence officer with the Defense Intelligence Agency for 25 years. Mr. Danis managed the agency's technology transfer division. This division is the U.S. government's sole analytical entity tasked with producing intelligence assessments regarding all aspects of foreign acquisition of U.S.-controlled technology and high-technology corporations. Mr. Danis also established and led a unique team of China technology specialists producing assessments on China's military-industrial complex and the impact of U.S. export-controlled and other foreign technology on Chinese weapons development programs. While serving in the U.S. Air Force, Mr. Danis was twice temporarily assigned to the Office of the Defense Attaché in Beijing.

### **APPENDIX III**

#### **PUBLIC HEARINGS OF THE COMMISSION**

Full transcripts and written testimonies are available online at the Commission's website: [www.uscc.gov](http://www.uscc.gov).

##### **January 27, 2011: Public Hearing on "China's Active Defense Strategy and its Regional Impact"** **Washington, DC**

Commissioners present: Hon. William A. Reinsch, Chairman; Daniel M. Slane, Vice Chairman; Carolyn Bartholomew (Hearing Co-Chair); Hon. C. Richard D'Amato; Hon. Patrick A. Mulloy; Hon. Dennis C. Shea; Larry M. Wortzel (Hearing Co-Chair).

Congressional Perspectives: Hon. Rob Wittman, U.S. Representative from the state of Virginia; Hon. Daniel Inouye,\* U.S. Senator from the state of Hawaii.

Witnesses: Oriana Skylar Mastro, Princeton University; Roger Cliff, The RAND Corporation; Cortez A. Cooper, The RAND Corporation; Martin C. Libicki, The RAND Corporation; Dean Cheng, The Heritage Foundation; Balbina Y. Hwang, Georgetown University; Stacy A. Pedrozo, Council on Foreign Relations; Jim Thomas, Center for Strategic and Budgetary Assessments; David A. Deptula,\* The Deptula Group, LLC.

##### **February 25, 2011: Public Hearing on "China's Internal Dilemmas" and Roundtable on "China's Internal Dilemmas and Implications for the United States"** **Washington, DC**

Commissioners present: Hon. William A. Reinsch, Chairman (Hearing Co-Chair); Daniel M. Slane, Vice Chairman; Daniel A. Blumenthal; Peter T.R. Brookes; Robin Cleveland (Hearing Co-Chair); Hon. C. Richard D'Amato; Jeffrey L. Fiedler; Hon. Patrick A. Mulloy; Hon. Dennis C. Shea; Michael R. Wessel.

Witnesses: Elizabeth Economy, Council on Foreign Relations; Martin K. Whyte, Harvard University; Murray Scot Tanner, CNA; Yukon Huang, Carnegie Endowment for International Peace; Steven Dunaway, Council on Foreign Relations.

Roundtable Participants: James Mann, The Johns Hopkins University, SAIS; Martin K. Whyte, Harvard University; Murray Scot Tanner, CNA; Yukon Huang, Carnegie Endowment for International Peace; Steven Dunaway, Council on Foreign Relations.



**March 10, 2011: Public Hearing on “China’s Narratives  
Regarding National Security Policy”  
Washington, DC**

Commissioners present: Hon. William A. Reinsch, Chairman; Daniel M. Slane, Vice Chairman; Carolyn Bartholomew; Daniel A. Blumenthal; Peter T.R. Brookes; Hon. C. Richard D’Amato; Jeffrey L. Fiedler (Hearing Co-Chair); Hon. Patrick A. Mulloy; Hon. Dennis C. Shea (Hearing Co-Chair); Michael R. Wessel; Larry M. Wortzel.

Witnesses: David M. Lampton, The Johns Hopkins University, SAIS; Gilbert Rozman, Princeton University and Woodrow Wilson Center; Christopher A. Ford, The Hudson Institute; Jacqueline A. Newmyer Deal, Long Term Strategy Group and Foreign Policy Research Institute; Ashley Esarey, Whitman College, Harvard University, and University of Washington; Mark A. Stokes, Project 2049 Institute; John S. Park, U.S. Institute of Peace; Abraham M. Denmark, Center for a New American Security; Alison Kaufman,\* CNA; Gary D. Rawnsley,\* University of Leeds (UK); Andrew Scobell,\* The RAND Corporation.

**March 30, 2011: Public Hearing on “Chinese State-Owned  
Enterprises and U.S.-China Bilateral Investment”  
Washington, DC**

Commissioners present: Hon. William A. Reinsch, Chairman; Daniel M. Slane, Vice Chairman (Hearing Co-Chair); Carolyn Bartholomew; Daniel A. Blumenthal; Peter T.R. Brookes; Robin Cleveland; Hon. C. Richard D’Amato; Hon. Patrick A. Mulloy; Hon. Dennis C. Shea; Michael R. Wessel (Hearing Co-Chair); Larry M. Wortzel.

Congressional Perspectives: Hon. Rosa L. DeLauro, U.S. Representative from the state of Connecticut; Hon. Maurice Hinchey, U.S. Representative from the state of New York; Hon. Michael A. Michaud,\* U.S. Representative from the state of Maine.

Witnesses: Barry J. Naughton, University of California; Derek Scissors, The Heritage Foundation; Theodore H. Moran, Georgetown University and Peterson Institute for International Economics; Robert E. Scott, Economic Policy Institute; K.C. Fung, University of California at Santa Cruz; Daniel H. Rosen, Rhodium Group and Peterson Institute for International Economics; Karl P. Sauviant, Columbia University.

**April 13, 2011: Public Hearing on “China’s Foreign Policy:  
Challenges and Players”  
Washington, DC**

Commissioners present: Hon. William A. Reinsch, Chairman; Daniel M. Slane, Vice Chairman; Carolyn Bartholomew (Hearing Co-Chair); Daniel A. Blumenthal; Peter T.R. Brookes (Hearing Co-Chair); Robin Cleveland; Hon. C. Richard D’Amato; Jeffrey L. Fiedler; Hon. Patrick A. Mulloy; Hon. Dennis C. Shea; Michael R. Wessel; Larry M. Wortzel.

Congressional Perspectives: Hon. Dana Rohrabacher, U.S. Representative from the state of California; Hon. Bill Johnson,\* U.S. Representative from the state of Ohio.

Witnesses: Daniel J. Kritenbrink, U.S. Department of State; David Helvey, U.S. Department of Defense; J. Peter Pham, Atlantic Council; Alan M. Wachman, Tufts University; Andrew Small, German Marshall Fund of the United States; Victor D. Cha, Georgetown University and Center for Strategic and International Studies; John W. Garver, Georgia Institute of Technology; Richard Weitz, The Hudson Institute; Yu-Wen Julie Chen, University of Virginia; Erica S. Downs, The Brookings Institution; Susan V. Lawrence, Congressional Research Service.

**May 4, 2011: Public Hearing on “China’s Intellectual Property Rights and Indigenous Innovation Policy”  
Washington, DC**

Commissioners present: Hon. William A. Reinsch, Chairman; Daniel M. Slane, Vice Chairman; Carolyn Bartholomew, Peter T.R. Brookes; Hon. C. Richard D’Amato (Hearing Co-Chair); Jeffrey L. Fiedler; Hon. Patrick A. Mulloy; Hon. Dennis C. Shea (Hearing Co-Chair); Michael R. Wessel.

Congressional Perspectives: Hon. Thomas Slade Gorton, former U.S. Senator from the state of Washington; Hon. Brad Sherman, U.S. Representative from the state of California.

Witnesses: Michael Schlesinger, International Intellectual Property Alliance; Ken Wasch, Software & Information Industry Association; Thea Mei Lee, AFL-CIO; Alan Wm. Wolff, Dewey & LeBoeuf, LLP.

**May 11, 2011: Public Hearing on “The Implications of China’s Military and Civil Space Programs”  
Washington, DC**

Commissioners present: Hon. William A. Reinsch, Chairman; Daniel M. Slane, Vice Chairman; Carolyn Bartholomew; Daniel A. Blumenthal (Hearing Co-Chair); Robin Cleveland; Hon. C. Richard D’Amato; Jeffrey L. Fiedler; Hon. Patrick A. Mulloy; Hon. Dennis C. Shea; Michael R. Wessel (Hearing Co-Chair); Larry M. Wortzel.

Congressional Perspective: Hon. Frank Wolf, U.S. Representative from the state of Virginia.

Witnesses: Gregory L. Schulte, U.S. Department of Defense; Mark A. Stokes, Project 2049 Institute; Bruce W. MacDonald, U.S. Institute of Peace; Barry Watts, Center for Strategic and Budgetary Assessments; Scott Pace, The George Washington University; James Clay Moltz, Naval Postgraduate School; Alanna Krolikowski, The George Washington University Space Policy Institute and University of Toronto; Dean Cheng,\* The Heritage Foundation.

**June 15, 2011: Public Hearing on “China’s Five-Year Plan,  
Indigenous Innovation and Technology Transfers,  
and Outsourcing”  
Washington, DC**

Commissioners present: Hon. William A. Reinsch, Chairman; Daniel M. Slane, Vice Chairman (Hearing Co-Chair); Carolyn Bartholomew; Daniel A. Blumenthal; Peter T.R. Brookes; Robin Cleveland; Hon. C. Richard D’Amato; Hon. Patrick A. Mulloy (Hearing Co-Chair); Hon. Dennis C. Shea; Michael R. Wessel.

Witnesses: Willy C. Shih, Harvard Business School; Eswar S. Prasad, Cornell University and The Brookings Institution; Adam Segal, Council on Foreign Relations; John Neuffer, Information Technology Industry Council; Dieter Ernst, East-West Center; Ralph E. Gomory, NYU Stern School of Business and Alfred P. Sloan Foundation; Leo Hindery, Jr., New America Foundation; Philip I. Levy, American Enterprise Institute.

---

\*Submitted material for the record.

**APPENDIX IIIA**

**LIST OF WITNESSES TESTIFYING BEFORE  
THE COMMISSION**

**2011 Hearings**

Full transcripts and written testimonies are available online at  
the Commission's website: [www.uscc.gov](http://www.uscc.gov).

**Alphabetical Listing of Panelists Testifying before the USCC**

<b>Panelist Name</b>	<b>Panelist Affiliation</b>	<b>USCC Hearing</b>
Cha, Victor D.	Georgetown University and Center for Strategic and International Studies	April 13, 2011
Chen, Yu-Wen Julie	University of Virginia	April 13, 2011
Cheng, Dean	The Heritage Foundation	January 27, 2011 May 11, 2011 *
Cliff, Roger	The RAND Corporation	January 27, 2011
Cooper, Cortez A.	The RAND Corporation	January 27, 2011
DeLauro, Rosa L.	U.S. Representative from the state of Connecticut	March 30, 2011
Denmark, Abraham M.	Center for a New American Security	March 10, 2011
Deptula, David A.*	The Deptula Group, LLC	January 27, 2011
Downs, Erica S.	The Brookings Institution	April 13, 2011
Dunaway, Steven	Council on Foreign Relations	February 25, 2011
Economy, Elizabeth	Council on Foreign Relations	February 25, 2011
Ernst, Dieter	East-West Center	June 15, 2011
Esarey, Ashley	Whitman College, Harvard University, and University of Washington	March 10, 2011
Ford, Christopher A.	The Hudson Institute	March 10, 2011
Fung, K.C.	University of California at Santa Cruz	March 30, 2011

**Alphabetical Listing of Panelists Testifying before the USCC**  
***Continued***

<b>Panelist Name</b>	<b>Panelist Affiliation</b>	<b>USCC Hearing</b>
Garver, John W.	Georgia Institute of Technology	April 13, 2011
Gomory, Ralph E.	NYU Stern School of Business and Alfred P. Sloan Foundation	June 15, 2011
Gorton, Thomas Slade	Former U.S. Senator from the state of Washington	May 4, 2011
Helvey, David	U.S. Department of Defense	April 13, 2011
Hinchey, Maurice	U.S. Representative from the state of New York	March 30, 2011
Hindery Jr., Leo	New America Foundation	June 15, 2011
Huang, Yukon	Carnegie Endowment for International Peace	February 25, 2011
Hwang, Balbina Y.	Georgetown University	January 27, 2011
Inouye, Daniel *	U.S. Senator from the state of Hawaii	January 27, 2011
Johnson, Bill *	U.S. Representative from the state of Ohio	April 13, 2011
Kaufman, Alison *	CNA	March 10, 2011
Kritenbrink, Daniel J.	U.S. Department of State	April 13, 2011
Krolikowski, Alanna	The George Washington University Space Policy Institute and University of Toronto	May 11, 2011
Lampton, David M.	The Johns Hopkins University, SAIS	March 10, 2011
Lawrence, Susan V.	Congressional Research Service	April 13, 2011
Lee, Thea Mei	AFL-CIO	May 4, 2011
Levy, Philip I.	American Enterprise Institute	June 15, 2011
Libicki, Martin C.	The RAND Corporation	January 27, 2011
MacDonald, Bruce W.	U.S. Institute of Peace	May 11, 2011
Mann, James	The Johns Hopkins University, SAIS	February 25, 2011
Mastro, Oriana Skylar	Princeton University	January 27, 2011
Michaud, Michael A.*	U.S. Representative from the state of Maine	March 30, 2011
Moltz, James Clay	Naval Postgraduate School	May 11, 2011



**Alphabetical Listing of Panelists Testifying before the USCC**  
***Continued***

<b>Panelist Name</b>	<b>Panelist Affiliation</b>	<b>USCC Hearing</b>
Moran, Theodore H.	Georgetown University and Peterson Institute for International Economics	March 30, 2011
Naughton, Barry J.	University of California	March 30, 2011
Neuffer, John	Information Technology Industry Council	June 15, 2011
Newmyer Deal, Jacqueline A.	Long Term Strategy Group and Foreign Policy Research Institute	March 10, 2011
Pace, Scott	The George Washington University	May 11, 2011
Park, John S.	U.S. Institute of Peace	March 10, 2011
Pedrozo, Stacy A.	Council on Foreign Relations	January 27, 2011
Pham, J. Peter	Atlantic Council	April 13, 2011
Prasad, Eswar S.	Cornell University and The Brookings Institution	June 15, 2011
Rawnsley, Gary D.*	University of Leeds (UK)	March 10, 2011
Rohrabacher, Dana	U.S. Representative from the state of California	April 13, 2011
Rosen, Daniel H.	Rhodium Group and Peterson Institute for International Economics	March 30, 2011
Rozman, Gilbert	Princeton University and Woodrow Wilson Center	March 10, 2011
Sauvant, Karl P.	Columbia University	March 30, 2011
Schlesinger, Michael	International Intellectual Property Alliance	May 4, 2011
Schulte, Gregory L.	U.S. Department of Defense	May 11, 2011
Scissors, Derek	The Heritage Foundation	March 30, 2011
Scobell, Andrew *	The RAND Corporation	March 10, 2011
Scott, Robert E.	Economic Policy Institute	March 30, 2011
Segal, Adam	Council on Foreign Relations	June 15, 2011
Sherman, Brad	U.S. Representative from the state of California	May 4, 2011
Shih, Willy C.	Harvard Business School	June 15, 2011
Small, Andrew	German Marshall Fund of the United States	April 13, 2011

**Alphabetical Listing of Panelists Testifying before the USCC**  
***Continued***

<b>Panelist Name</b>	<b>Panelist Affiliation</b>	<b>USCC Hearing</b>
Stokes, Mark A.	Project 2049 Institute	March 10, 2011 May 11, 2011
Tanner, Murray Scot	CNA	February 25, 2011
Thomas, Jim	Center for Strategic and Budgetary Assessments	January 27, 2011
Wachman, Alan M.	Tufts University	April 13, 2011
Wasch, Ken	Software & Information Industry Association	May 4, 2011
Watts, Barry	Center for Strategic and Budgetary Assessments	May 11, 2011
Weitz, Richard	The Hudson Institute	April 13, 2011
Whyte, Martin K.	Harvard University	February 25, 2011
Wittman, Rob	U.S. Representative from the state of Virginia	January 27, 2011
Wolf, Frank	U.S. Representative from the state of Virginia	May 11, 2011
Wolff, Alan Wm.	Dewey & LeBoeuf, LLP	May 4, 2011

\* Submitted material for the record.

## **APPENDIX IV INTERLOCUTORS' ORGANIZATIONS**

### **Asia Fact Finding Trips December 2010 and August 2011**

#### **SINGAPORE AND INDONESIA, DECEMBER 10–18, 2010**

**During the visit of a U.S.-China Commission delegation to Singapore and Indonesia in December 2010, the delegation met with representatives of the following organizations:**

##### ***In Singapore***

###### **U.S. Government**

- U.S. Embassy in Singapore

###### **Government of Singapore**

- Ministry of Foreign Affairs
- Ministry of Defense
- Republic of Singapore Navy
- Economic Development Board

###### **Research Organizations**

- Rajaratnam School of International Studies
- East Asian Institute

##### ***In Indonesia***

###### **U.S. Government**

- U.S. Embassy in Jakarta

###### **Government of Indonesia**

- Indonesia Investment Coordinating Board (BKPM)
- Ministry of Foreign Affairs (KEMLU)
- National Economic Committee
- Ministry of Trade (KEMDAG)
- Ministry of Defense (KEMHAN)
- National Resilience Institute of Indonesia (LEMHANAS)

###### **Universities and Research Organizations**

- Center for Strategic and International Studies, Jakarta
- University of Indonesia

###### **Private Enterprise**

- PT Indika Energy
- Van Zorge, Heffernan & Associates

###### **Intergovernmental Institutions**

- ASEAN Secretariat
- World Bank Office Jakarta

**CHINA, HONG KONG, AND TAIWAN, AUGUST 6–18, 2011**

**During the visit of a U.S.-China Commission delegation to China, Hong Kong, and Taiwan in August 2011, the delegation met with representatives of the following organizations:**

***In China*****U.S. Government**

- U.S. Embassy in Beijing
- U.S. Consulate in Shanghai

**Government of the People's Republic of China**

- China Investment Corporation
- China Institute of International Studies
- The Chinese People's Institute of Foreign Affairs

**Research and University Organizations**

- Shanghai Scholar Roundtable
- Fudan University
- Shanghai Jiaotong University
- Shanghai Institute for International Studies
- Tongji University

**Private Enterprise**

- China Aerospace Science and Technology Corporation
- China Great Wall Industry Corporation
- Shanghai Academy of Spaceflight Technology
- American Chamber of Commerce Beijing
- American Chamber of Commerce Shanghai
- U.S.-China Business Council
- Korea Business Consultants
- Koryo Tours
- Pan Asia Technical Automotive Center (Shanghai)

***In Hong Kong*****U.S. Government**

- U.S. Consulate in Hong Kong

**Government of the Hong Kong Special Administrative Region**

- Hong Kong Economic and Trade Office

**Private Enterprise**

- American Chamber of Commerce Hong Kong
- Goldman Sachs

**Political Enterprise**

- Hong Kong Pan-Democrats

***In Taiwan***

**U.S. Government**

- American Institute in Taiwan

**Government of Taiwan**

- President Ma Ying-Jeou
- Legislative Yuan
- Ministry of Foreign Affairs
- Ministry of Defense
- Ministry of Economic Affairs
- National Security Council
- Mainland Affairs Council

**Political Enterprise**

- Taiwan Democratic Progressive Party





**APPENDIX V**  
**LIST OF RESEARCH MATERIAL**  
**Contracted and Staff Research Reports**  
**Released in 2011**

*Disclaimer*

The reports in this section were prepared at the request of the Commission to support its deliberations. They have been posted to the Commission's website in order to promote greater public understanding of the issues addressed by the Commission in its ongoing assessment of U.S.-China economic relations and their implications for U.S. security, as mandated by P.L. 106-398 and P.L. 108-7. The posting of these reports to the Commission's website does not imply an endorsement by the Commission or any individual Commissioner of the views or conclusions expressed therein.

**Contracted Research Reports**

***An Analysis of State-owned Enterprises and State Capitalism in China***

Prepared for the USCC by Andrew Szamosszegi and Cole Kyle/  
Capital Trade, Inc.

October 2011

[http://www.uscc.gov/researchpapers/2011/10\\_26\\_11\\_CapitalTradeSOEStudy.pdf](http://www.uscc.gov/researchpapers/2011/10_26_11_CapitalTradeSOEStudy.pdf)

***China's Program for Science and Technology Modernization: Implications for American Competitiveness***

Prepared for the USCC by Micah Springut, Stephen Schlaikjer, and  
David Chen/CENTRA Technology, Inc.

April 2011

[http://www.uscc.gov/researchpapers/2011/USCC\\_REPORT\\_China%27s\\_Program\\_forScience\\_and\\_Technology\\_Modernization.pdf](http://www.uscc.gov/researchpapers/2011/USCC_REPORT_China%27s_Program_forScience_and_Technology_Modernization.pdf)

***Ready for Takeoff: China's Advancing Aerospace Industry***

Prepared for the USCC by Roger Cliff, Chad J.R. Ohlandt, and  
David Yang/RAND Corporation

March 2011

[http://www.uscc.gov/researchpapers/2011/RAND\\_Aerospace\\_Report%5b1%5d.pdf](http://www.uscc.gov/researchpapers/2011/RAND_Aerospace_Report%5b1%5d.pdf)

***The Evolving Role of China in International Institutions***

Prepared for the USCC by Stephen Olson and Clyde Prestowitz/

The Economic Strategy Institute

January 2011

<http://www.uscc.gov/researchpapers/2011/TheEvolvingRoleofChinainInternationalInstitutions.pdf>

**Staff Research Reports and Backgrounders**

***China's Foreign Assistance in Review***

Written by USCC staff members Jonathan Weston,

Caitlin Campbell, and Katherine Koleski

September 2011

[http://www.uscc.gov/researchpapers/2011/9\\_1\\_%202011\\_ChinasForeignAssistanceinReview.pdf](http://www.uscc.gov/researchpapers/2011/9_1_%202011_ChinasForeignAssistanceinReview.pdf)

***The Confucian Revival in the Propaganda Narratives of the Chinese Government***

Written by USCC Research Coordinator John Dotson

July 2011

[http://www.uscc.gov/researchpapers/2011/Confucian\\_Revival\\_Paper.pdf](http://www.uscc.gov/researchpapers/2011/Confucian_Revival_Paper.pdf)

***The Chinese People's Liberation Army Delegation Visit to the United States, May 2011: A Summary of Key Actors and Issues***

Written by USCC Research Fellow Amy Chang

June 2011

[http://www.uscc.gov/PLA\\_Delegation\\_Visit\\_to\\_U.S.\\_May\\_2011\\_Background.pdf](http://www.uscc.gov/PLA_Delegation_Visit_to_U.S._May_2011_Background.pdf)

***Backgrounder: China's 12th Five-Year Plan***

Written by USCC Research Assistant Katherine Koleski and

Research Fellow Joseph Casey

June 2011

[http://www.uscc.gov/researchpapers/2011/12th-FiveYearPlan\\_062811.pdf](http://www.uscc.gov/researchpapers/2011/12th-FiveYearPlan_062811.pdf)

***Backgrounder: China in Latin America***

Written by USCC Research Assistant Katherine Koleski

May 2011

[http://www.uscc.gov/Backgrounder\\_China\\_in\\_Latin\\_America.pdf](http://www.uscc.gov/Backgrounder_China_in_Latin_America.pdf)

***Going Out: An Overview of China's Outward Foreign Direct Investment***

Written by USCC Policy Analyst Nargiza Salidjanova

March 2011

<http://www.uscc.gov/researchpapers/2011/GoingOut.pdf>

401

***The National Security Implications of Investments and  
Products from the People's Republic of China in the  
Telecommunications Sector***

Prepared by USCC staff with the support of Reperi LLC  
January 2011

*<http://www.uscc.gov/RFP/2011/FINALREPORT> TheNational  
SecurityImplicationsofInvestmentsandProductsfromThePRC  
intheTelecommunicationsSector.pdf*





## APPENDIX VI

### ACRONYMS AND ABBREVIATIONS

AFL–CIO	American Federation of Labor–Congress of Industrial Organizations
ASEAN	Association of Southeast Asian Nations
CAIFC	China Association for International Friendly Contact
CBRC	China Banking Regulatory Commission
CCTV 7	China Central Television 7
CFIUS	Committee on Foreign Investment in the United States
CIC	China Investment Corporation
CIRC	China Insurance Regulatory Commission
CNOOC	China National Offshore Oil Corporation
CNPC	China National Petroleum Corporation
CCP	Chinese Communist Party
CRS	Congressional Research Service
CPD	Center for Peace and Development
CSRC	China Securities Regulatory Commission
CZ	Chang Zheng (family of rockets)
DoD	Department of Defense
EEZ	Exclusive economic zone
EOS	Earth observation system
EU	European Union
FDI	Foreign direct investment
GDP	Gross domestic product
GPA	WTO Agreement on Government Procurement
Km	Kilometer
MLP	Medium- and Long-Term Plan for the Development of Science and Technology
NDRC	National Development and Reform Commission
OECD	Organization for Economic Cooperation and Development
PLA	People’s Liberation Army
PRC	People’s Republic of China
R&D	Research and development
RMB	Renminbi
SASAC	State-owned Assets Supervision and Administration Commission
SCO	Shanghai Cooperation Organization
SEI	Strategic Emerging Industry
Sinopec	China Petroleum and Chemical Corporation
SOE	State-owned enterprise
UN	United Nations
USTR	United States Trade Representative
VAT	Value-added tax

404

WAPI	Wired Authentication and Privacy Infrastructure Standard
WTO	World Trade Organization

**2011 COMMISSION STAFF**

MICHAEL R. DANIS, *Executive Director*  
 KATHLEEN J. MICHELS, *Associate Director*  
 DANIEL M. HARTNETT, *Senior Policy Analyst Military and Security Issues*  
 PAUL C. MAGNUSSON, *Senior Policy Analyst Economics and Trade Issues*  
 JOHN D. DOTSON, *Research Coordinator*  
 JONATHAN G. WESTON, *Congressional and Public Affairs Coordinator*

CAITLIN E. CAMPBELL, *Policy Analyst for Energy and Foreign Affairs*  
 DOUGLAS G. FEHRER, *Human Resources Coordinator*  
 CHRISTOPHER P. FIORAVANTE, *Travel and Procurement Assistant*  
 M.L. FAUNCE, *Administrative-Program Specialist*  
 RICHARD KOMAIKO, *Senior Staff Research Fellow, Economics and Trade Issues*  
 TIMOTHY L. LIPKA, *Administrative-Program Assistant*  
 NARGIZA SALIDJANOVA, *Policy Analyst for Economics and Trade Issues Policy*  
 ROBERT G. SHELDON, *Policy Analyst for Military and Security Issues Policy*  
 KATHLEEN WILSON, *Budget and Accounting Specialist*

**ACKNOWLEDGEMENTS**

The Commission would like to express its deep appreciation to those who testified before the Commission as expert witnesses, the researchers and analysts who prepared research papers under contract to the Commission, and others who assisted with the Commission's work by briefing the Commissioners on a wide array of economic and security issues. All these efforts helped inform the Commission's and the public's debate on issues vital to ongoing U.S.-China relations.

The Commission offers its special thanks to The Honorable Kurt M. Campbell, Assistant Secretary of State for East Asian and Pacific Affairs and staff for their outstanding support of the Commission's fact-finding trip to China, Hong Kong, and Taiwan in August 2011. The Members of the Commission also owe a deep debt of gratitude and thanks to the following officials of the State Department, U.S. Embassies and Consulates: U.S. Embassy Beijing Deputy Chief of Mission Robert S. Wang, and staff for their outstanding support during the Commission's delegation visit to Beijing and Shanghai, including Carl T. Watson and Amanda H. King in Beijing, and David C. Ng in Shanghai, who were instrumental in arranging and helping the Commission to meet its schedule of meetings with officials in Beijing and Shanghai. The Honorable Stephen M. Young, U.S. Consul Hong Kong, and staff, including Kim Liao and Stephanie Boven for their technical assistance and logistical support in setting up meetings with government officials and political and opinion leaders. Their advice and assistance were instrumental in the success of the Commission's visit to Hong Kong. And finally, a special thanks to The Honorable William A. Stanton, American Institute-Taiwan, and staff members Jennifer Health and Justin G. Miller, for the outstanding assistance and technical support provided during the Commission's delegation visit to Taiwan, which was instrumental in the Commission's ability to meet with government officials and political leaders.

The Commissioners also wish to thank Admiral Robert F. Willard, Commander U.S. Pacific Command; and other key officials, including Rear Admiral Thomas K. Shannon, Deputy Chief of Staff for Operations, Training and Readiness, U.S. Pacific Fleet; Brigadier General Michael A. Keltz, Deputy Director of Operations, Plans, Programs and Requirements, Headquarters Pacific Air Forces; Colonel James Reilly, Chief of Staff, U.S. Marine Corps Forces Pacific; and staff members James Seatris, Charlie Johnson, William Chambliss, and Tim Roy for their outstanding assistance, which was instrumental in the success of the Commission's visit to Hawaii. The Commissioners are also grateful to the agencies of the intelligence community that briefed Commissioners on key issues of importance to the U.S.-China relationship.

The Commissioners also express their special thanks to former program staff members Lee Levkowitz, Foreign Affairs and Energy Analyst; Katherine Koleski, Research Assistant; and Daniel Neumann, Economics and Trade Analyst. A special thanks also to current and former interns and fellows, who assisted the Commissioners and staff during this Report cycle by preparing research material and background information and by providing administrative and program support for the 2011 briefings and public hearings. They include Nathan Beauchamp-Mustafaga, Joseph Casey, Wilfred Chan, Amy Chang, Jeffrey Chivers, Benjamin Cmejla, Brendan Cooley, Kathleen Crowe, Elizabeth Flora, Ashley Johnson, Cory Johnson, Lauren Sprott, Jesse Walter, Olivia Wang, Gavin Williams, Lisa Zhang, and Shelly Zhao.

The Commissioners are especially grateful to Michael R. Danis, executive director, for his efforts in organizing the work of the Commission and in the preparation of the final Report to Congress, and offer special thanks to Senior Policy Analysts Daniel M. Hartnett, Paul C. Magnusson, and John D. Dotson for their exceptional expertise and guidance provided to the staff analysts during the drafting of the Report, and to Rona Mendelsohn, who served as technical editor. They also express their thanks to the policy analyst staff for their exemplary assistance in framing the debate and assisting in the writing and editing of the final report.

# EXHIBIT 5

# **ANNUAL REPORT TO CONGRESS**

## **Military and Security Developments Involving the People's Republic of China 2011**



Office of the Secretary of Defense

Preparation of this report cost the Department of Defense a total of approximately \$73,212 in Fiscal Years 2010-2011.

Generated on 2011

May06 RefID: 1-4AE81FF



*(This page left intentionally blank)*

# **Military and Security Developments Involving the People's Republic of China 2011**

**A Report to Congress  
Pursuant to the National Defense Authorization Act for  
Fiscal Year 2000**

---

*Section 1246, "Annual Report on Military and Security Developments Involving the People's Republic of China," of the National Defense Authorization Act for Fiscal Year 2010, Public Law 111-84, which amends the National Defense Authorization Act for Fiscal Year 2000, Section 1202, Public Law 106-65, provides that the Secretary of Defense shall submit a report "in both classified and unclassified form, on military and security developments involving the People's Republic of China. The report shall address the current and probable future course of military-technological development of the People's Liberation Army and the tenets and probable development of Chinese security strategy and military strategy, and of the military organizations and operational concepts supporting such development over the next 20 years. The report shall also address United States-China engagement and cooperation on security matters during the period covered by the report, including through United States-China military-to-military contacts, and the United States strategy for such engagement and cooperation in the future."*

---

*(This page left intentionally blank)*

## EXECUTIVE SUMMARY

---

China's rise as a major international actor is likely to stand out as a defining feature of the strategic landscape of the early 21<sup>st</sup> century. Sustained economic development has raised the standard of living for China's citizens and elevated China's international profile. This development, coupled with an expanding science and technology base, has also facilitated a comprehensive and ongoing military modernization program. The United States welcomes a strong, prosperous, and successful China that reinforces international rules and norms and enhances security and peace both regionally and globally.

China is steadily assuming new roles and responsibilities in the international community. In 2004, Chinese President Hu Jintao articulated new guidance for the People's Liberation Army (PLA), including missions extending beyond China's immediate territorial interests. This catalyzed China's growing involvement in international peacekeeping efforts, counter-piracy operations, humanitarian assistance and disaster relief, and the evacuation of Chinese citizens from overseas trouble spots. China's 2010 Defense White Paper asserts that China's "future and destiny have never been more closely connected with those of the international community." Nonetheless, China's modernized military could be put to use in ways that increase China's ability to gain diplomatic advantage or resolve disputes in its favor.

Although the PLA is contending with a growing array of missions, Taiwan remains its "main strategic direction." China continued modernizing its military in 2010, with a focus on Taiwan contingencies, even as cross-Straits relations improved. The PLA seeks the capability to deter Taiwan independence and influence Taiwan to settle the dispute on Beijing's terms. In pursuit of this objective, Beijing is developing capabilities intended to deter, delay, or deny possible U.S. support for the island in the event of conflict. The balance of cross-Straits military forces and capabilities continues to shift in the mainland's favor.

Over the past decade, China's military has benefitted from robust investment in modern hardware and technology. Many modern systems have reached maturity and others will become operational in the next few years. Following this period of ambitious acquisition, the decade from 2011 through 2020 will prove critical to the PLA as it attempts to integrate many new and complex platforms, and to adopt modern operational concepts, including joint operations and network-centric warfare.

China has made modest, but incremental, improvements in the transparency of its military and security affairs. However, there remains uncertainty about how China will use its growing capabilities.

The United States recognizes and welcomes PRC contributions that support a safe and secure global environment. China's steady integration into the global economy creates new incentives for partnership and cooperation, particularly in the maritime domain. Although China's expanding military capabilities can facilitate cooperation in pursuit of shared objectives, they can also increase the risk of misunderstanding and miscalculation. Strengthening our military-to-military relationship is a critical part of our strategy to shape China's choices as we seek to capitalize on opportunities for cooperation while mitigating risks. To support this strategy, the United States must continue monitoring PRC force development and strategy. In concert with our friends and Allies, the United States will also continue adapting our forces, posture, and operational concepts to maintain a stable and secure East Asian environment.

*(This page left intentionally blank)*

# Table of Contents

<b>Executive Summary</b>	<b>I</b>
<b>Chapter One: Annual Update</b>	<b>1</b>
China's Challenges and Opportunities in 2010	1
Developments in China's National Security Leadership	1
Developments in the Security Situation in the Taiwan Strait	2
Developments in the Size, Location, and Capabilities of PRC Military Forces	2
Developments in China's Space and Cyber Capabilities	5
Developments in China's Defense Technology Acquisition	6
Challenges to Taiwan's Deterrent Forces	7
China's Foreign Military Engagement	7
<b>Chapter Two: Understanding China's Strategy</b>	<b>9</b>
Overview	9
Understanding Chinese Strategy	9
China's Strategic Priorities	13
The New Historic Missions	16
Debates on Future Strategy	17
China's Military Strategy	22
Secrecy and Deception	25
<b>Chapter Three: Force Modernization Goals and Trends</b>	<b>27</b>
Overview	27
Anti-Access/Area Denial Capability Developments	28
Ballistic Missile Defense	32
Extended Operational Reach	32
Strategic Capabilities	33
Power Projection Beyond Taiwan	37
<b>Chapter Four: Resources for Force Modernization</b>	<b>41</b>
Overview	41
Military Expenditure Trends	41
China's Advancing Defense Industries	41
Trends and Projections	45



<b>Chapter Five: Force Modernization and Security in the Taiwan Strait</b>	<b>47</b>
Overview	47
Beijing’s Taiwan Strategy	48
Beijing’s Courses of Action Against Taiwan	49
<b>Chapter Six: U.S.-China Military-To-Military Contacts</b>	<b>53</b>
Overview	53
Military Relations in 2010	53
U.S. Strategy for Military Engagement	54
Opportunities and Challenges in U.S.-China Military-To-Military Relations	55
<b>Special Topic: China’s Evolving Maritime Strategy</b>	<b>57</b>
The Rise of China’s Maritime Security Interests	57
The Evolution in “Maritime Consciousness”	57
Evolving Naval Strategy	57
New Security Interests Driving Requirements	58
New “Firsts” for the PLA Navy	59
China’s Maritime Interests	59
Sea Lane Protection	61
Great Power Status	61
Sea-Based Nuclear Forces	62
Overcoming Key Challenges	62
Assessing the Future	62
<b>Special Topic: China’s Military Engagement</b>	<b>65</b>
Traditional Military Diplomacy	65
Combined Exercises	65
Peacekeeping Operations	66
Humanitarian Assistance/Disaster Relief	67
Arms Sales	67
Conclusion	69
<b>Appendix I:</b>	<b>71</b>
<b>China and Taiwan Forces Data</b>	<b>71</b>
<b>Appendix II:</b>	<b>79</b>
<b>Military-To-Military Exchanges</b>	<b>79</b>

## Glossary of Acronyms

AAV: Amphibious Assault Vehicle	MIRV: Multiple Independently Targeted Re-entry Vehicles
AEW&C: Airborne Early Warning and Control	MMCA: Military Maritime Consultative Agreement
APCSS: Asia Pacific Center for Security Studies	MND: Ministry of National Defense
ASAT: Anti-Satellite	MR: Military Region
ASBM: Anti-Ship Ballistic Missile	MRBM: Medium-Range Ballistic Missile
ASCM: Anti-Ship Cruise Missile	MRL: Multiple Rocket Launcher
bcm: billion cubic meters	NCO: Non-Commissioned Officer
b/d: barrels per day	NDU: National Defense University
C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance	NFU: No First Use
CCP: Chinese Communist Party	OMTE: Outline of Military Training and Evaluation
CMC: Central Military Commission	OTH: Over-the-Horizon
CNO: Computer Network Operations	PLA: People's Liberation Army
COMSAT: Communications Satellite	PLAAF: People's Liberation Army Air Force
CONUS: Continental United States	PRC: People's Republic of China
DCT: Defense Consultative Talks	R&D: Research and Development
DDG: Guided-Missile Destroyer	S&ED: Strategic and Economic Dialogue
DPCT: Defense Policy Coordination Talks	SAM: Surface-to-Air Missile
DSS: Defense Security Service	SCO: Shanghai Cooperation Organization
DSTL: Developing Sciences and Technologies List	SLBM: Submarine-Launched Ballistic Missile
EEZ: Exclusive Economic Zone	SLOC: Sea Lines of Communication
EU: European Union	SRBM: Short-Range Ballistic Missile
FAO: Foreign Affairs Office	SS: Diesel-Electric Attack Submarine
FFG: Guided-Missile Frigate	SSBN: Nuclear-Powered Ballistic Missile Submarine
GDP: Gross Domestic Product	SSN: Nuclear-Powered Attack Submarine
GPS: Global Positioning System	UAV: Unmanned Aerial Vehicle
HA/DR: Humanitarian Assistance/Disaster Relief	UCAV: Unmanned Combat Aerial Vehicle
ICBM: Intercontinental-Range Ballistic Missile	UN: United Nations
IJO: Integrated Joint Operations	UNCLOS: UN Convention on the Law of the Sea
LACM: Land Attack Cruise Missile	USCG: United States Coast Guard
	USMC: United States Marine Corps

*(This page left intentionally blank)*

## CHAPTER ONE: ANNUAL UPDATE

---

*“In the next five years, our economy and society will develop faster, boosting comprehensive national power. The developments will provide an even more stable material base to our defense and military buildup.”*

– PRC Defense Minister Liang Guanglie

Several significant developments in China over the past year relate to the questions Congress posed in Section 1246 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111-84).

### CHINA’S CHALLENGES AND OPPORTUNITIES IN 2010

The government of China remained focused on maintaining economic development and enhancing China’s security interests in 2010. The Chinese Communist Party (CCP) has built its legitimacy on the promise of economic growth, stability, and national unity. To ensure its position, the CCP closely monitors potential sources of domestic unrest, from unemployment and rising income disparities to pro-democracy movements and ethnic tensions. Additionally, Beijing is seeking to balance a more confident assertion of its growing interests in the international community with a desire to avoid generating opposition and countervailing responses from regional and major powers. An example of this could be seen in Beijing’s recalibrated rhetorical approach to regional territorial disputes such as the South China Sea following the June 2010 Association of Southeast Asian Nations Regional Forum (ARF).

The 11<sup>th</sup> Five Year Plan concluded in 2010 and was marked by new milestones in PLA force development and technology acquisition. Motivated by expanding economic and security interests, the PLA is now venturing into the global maritime domain, a sphere long dominated by the U.S. Navy. Relations with Taiwan have continued to improve, but the PLA shows no sign of slowing its efforts to develop plans and capabilities for a cross-Strait contingency.

Much of the PLA’s success over the next decade will be determined by how effectively it integrates emerging capabilities and platforms into the force. By most accounts, the PLA is on track to achieve its goal of building a modern, regionally-focused military by 2020.

In tandem with the PLA’s improved capacities for regional military operations, PRC officials in recent years have emphasized China’s sovereignty and territorial interests with greater frequency. Citing a violation of these “core interests,” the PLA suspended military-to-military relations with the United States in January 2010, following U.S. approval of arms sales to Taiwan.

### DEVELOPMENTS IN CHINA’S NATIONAL SECURITY LEADERSHIP

Vice President Xi Jinping became a vice chairman of the CCP Central Military Commission (CMC) at the 5<sup>th</sup> Plenum of the 17<sup>th</sup> Central Committee in October 2010. Based on historical precedent, this move could be the penultimate step to Xi becoming the General Secretary of the CCP and Chairman of the Central Military Commission (CMC). During the leadership transition process that is expected to unfold around the 18<sup>th</sup> Party Congress in the fall of 2012, it is not clear if President Hu Jintao will relinquish

the Party General Secretary and CMC Chairman positions, or if he will follow the precedent set by Jiang Zemin in 2002 and retain the CMC Chairmanship for a number of months, or even years, to facilitate the power transition.

## **DEVELOPMENTS IN THE SECURITY SITUATION IN THE TAIWAN STRAIT**

Since the election in Taiwan of President Ma Ying-jeou in March 2008, Beijing and Taipei have made significant progress in improving cross-Strait relations. Both Beijing and Taipei have emphasized expanding economic and cultural ties as a means of reducing tension and sustaining the current positive cross-Strait atmosphere.

Beijing and Taipei signed the Economic Cooperation Framework Agreement (ECFA) in 2010. Beijing has at times demonstrated flexibility on the issue of Taiwan's participation in international forums, but has also continued to pressure players in the international community to restrict this participation.

Despite the warming of cross-Strait ties, China continued its military modernization in 2010, including specific efforts to provide a credible range of military options in a Taiwan contingency. In the current decade to 2020, the PLA is likely to steadily expand its military options for Taiwan, including those to deter, delay, or deny third party intervention.

## **DEVELOPMENTS IN THE SIZE, LOCATION, AND CAPABILITIES OF PRC MILITARY FORCES**

China's long-term, comprehensive military modernization is improving the PLA's capacity to conduct high-intensity, regional military operations, including "anti-access and area denial" (A2AD) operations. The terms "anti-access and area denial" refer to capabilities that could be employed to deter or counter adversary forces from deploying to, or operating within, a defined space.

Consistent with a near-term focus on preparing for Taiwan Strait contingencies, China continues to base many of its most advanced systems in the military regions (MRs) opposite Taiwan. Although these capabilities could be employed for a variety of regional crisis or conflict scenarios, China has made less progress on capabilities that extend global reach or power projection. Outside of peacetime counter-piracy missions, for example, China's Navy has little operational experience beyond regional waters. Although the PLA's new roles and missions in the international domain reflect China's expanding set of interests, regional contingencies continue to dominate resources and planning.

**Ballistic and Cruise Missiles.** China has prioritized land-based ballistic and cruise missile programs. It is developing and testing several new classes and variants of offensive missiles, forming additional missile units, upgrading older missile systems, and developing methods to counter ballistic missile defenses.

- The PLA is acquiring large numbers of highly accurate cruise missiles, many of which have ranges in excess of 185 km. This includes the domestically-produced, ground-launched DH-10 land-attack cruise missile (LACM); the domestically produced ground- and ship-launched YJ-62 anti-ship cruise missile (ASCM); the Russian SS-N-22/SUNBURN supersonic ASCM, which is fitted on China's SOVREMENNY-class DDGs acquired from Russia; and, the Russian SS-N-27B/SIZZLER supersonic ASCM on China's Russian-built, KILO-class diesel-electric attack submarines.
- By December 2010, the PLA had deployed between 1,000 and 1,200 short-range ballistic missiles (SRBM) to units opposite Taiwan. To improve the lethality of this force, the PLA is introducing variants of missiles with improved ranges, accuracies, and payloads.

- China is developing an anti-ship ballistic missile (ASBM) based on a variant of the CSS-5 medium-range ballistic missile (MRBM). Known as the DF-21D, this missile is intended to provide the PLA the capability to attack large ships, including aircraft carriers, in the western Pacific Ocean. The DF-21D has a range exceeding 1,500 km and is armed with a maneuverable warhead.
- China is modernizing its nuclear forces by adding more survivable delivery systems. In recent years, the road mobile, solid propellant CSS-10 Mod 1 and CSS-10 Mod 2 (DF-31 and DF-31A) intercontinental-range ballistic missiles (ICBMs) have entered service. The CSS-10 Mod 2, with a range in excess of 11,200 km, can reach most locations within the continental United States.
- China may also be developing a new road-mobile ICBM, possibly capable of carrying a multiple independently targetable re-entry vehicle (MIRV).

**Naval Forces.** Since the 1990s, the PLA Navy has rapidly transformed from a large fleet of low-capability, single-mission platforms, to a leaner force equipped with more modern, multi-mission platforms. In contrast to the fleet just a decade ago, many PLA Navy combatants are equipped with advanced air-defense systems and modern ASCMs, with ranges in excess of 185 km. These capabilities not only increase the lethality of PLA Navy platforms, particularly in the area of anti-surface warfare (ASuW), but also enable them to operate beyond the range of land-based air defenses.

The PLA Navy possesses some 75 principal surface combatants, more than 60 submarines, 55 medium and large amphibious ships, and roughly 85 missile-equipped small combatants. The PLA has now completed construction of a major naval base at Yulin, on the southernmost tip of Hainan Island. The base is large enough to accommodate a mix of attack and ballistic missile submarines

and advanced surface combatants, including aircraft carriers. Submarine tunnel facilities at the base could also enable deployments from this facility with reduced risk of detection.

- China's aircraft carrier research and development program includes renovation of the ex-VARYAG, which could begin sea trials in 2011, although without aircraft. It will likely serve initially as a training and evaluation platform, and eventually offer a limited operational capability. China could begin construction of a fully indigenous carrier in 2011, which could achieve operational capability after 2015. China likely will build multiple aircraft carriers with support ships over the next decade.
- China currently has a land-based training program for carrier pilots; however, it will still take several additional years for China to achieve a minimal level of combat capability on an aircraft carrier.
- The PLA Navy is improving its over-the-horizon (OTH) targeting capability with sky wave and surface wave OTH radars. In combination with early-warning aircraft, unmanned aerial vehicles (UAVs), and other surveillance and reconnaissance equipment, the sky wave OTH radar allows the PRC to carry out surveillance and reconnaissance over the western Pacific. The OTH radars can be used in conjunction with reconnaissance satellites to locate targets at great distances from the PRC, thereby supporting long-range precision strikes, including employment of ASBMs.
- China continues to produce a new class of nuclear-powered ballistic missile submarine (SSBN). JIN-class (Type 094) SSBNs will eventually carry the JL-2 submarine-launched ballistic missile with an estimated range of some 7,400 km. The JIN and the JL-2 will give the PLA Navy its first credible sea-based nuclear capability. Although DoD initially



forecast the JL-2 would reach IOC by 2010, the program has faced repeated delays.

- China has expanded its force of nuclear-powered attack submarines (SSN). Two second-generation SHANG-class (Type 093) SSNs are already in service and as many as five third-generation Type 095 SSNs will be added in the coming years. When complete, the Type 095 will incorporate better quieting technology, improving its capability to conduct a range of missions from surveillance to the interdiction of surface vessels with torpedoes and ASCMs.
- The current mainstay modern diesel powered attack submarines (SS) in the PLA Navy's submarine force are the 13 SONG-class (Type 039) units. Each can carry the YJ-82 ASCM. The follow-on to the SONG is the YUAN-class SS; as many as four of which are already in service. The YUAN-class SS might also include an air-independent power system. The SONG, YUAN, SHANG and the still-to-be-deployed Type 095 all will be capable of launching the long-range CH-SS-NX-13 ASCM, once the missile completes development and testing.
- China has deployed some 60 of its new HOUBEI-class (Type 022) wave-piercing catamaran hull missile patrol boats. Each boat can carry up to eight YJ-83 ASCMs. These ships have increased the PLA Navy's littoral warfare capabilities.
- The PLA Navy has acquired a new generation of domestically produced surface combatants. These include at least two LUYANG II-class (Type 052C) DDGs fitted with the indigenous HHQ-9 long-range surface-to-air missile (SAM) with additional hulls under construction; two LUZHOU-class (Type 051C) DDGs equipped with the Russian SA-N-20 long-range SAM; and as many as eight JIANGKAI II-class (Type 054A) guided-missile frigates (FFG) fitted with the

medium-range HHQ-16 vertically launched naval SAM. These ships significantly improve the PLA Navy's area air defense capability, which will be critical as the PLA Navy expands its operations into "distant seas," beyond the range of shore-based air defense.

**Air and Air Defense Forces.** China bases 490 combat aircraft within unrefueled operational range of Taiwan and has the airfield capacity to expand that number by hundreds. Newer and more advanced aircraft make up a growing percentage of the inventory.

- The January 2011 flight test of China's next generation fighter prototype, the J-20, highlights China's ambition to produce a fighter aircraft that incorporates stealth attributes, advanced avionics, and super-cruise capable engines over the next several years.
- China is upgrading its B-6 bomber fleet (originally adapted from the Soviet Tu-16) with a new, longer-range variant that will be armed with a new long-range cruise missile.
- The PLA Air Force has continued expanding its inventory of long-range, advanced SAM systems and now possesses one of the largest such forces in the world. Over the past five years, China has acquired multiple SA-20 PMU2 battalions, the most advanced SAM system Russia exports. It has also introduced the indigenously designed HQ-9.
- China's aviation industry is developing several types of airborne early warning and control system (AWACS) aircraft. These include the KJ-200, based on the Y-8 airframe, for AWACS as well as intelligence collection and maritime surveillance, and the KJ-2000, based on a modified Russian IL-76 airframe.

**Ground Forces.** The PLA has about 1.25 million ground force personnel,

approximately 400,000 of whom are based in the three military regions (MRs) opposite Taiwan. China continues to gradually modernize its large ground force. Much of the observed upgrade activity has occurred in units with the potential to be involved in a Taiwan contingency. Examples of ground unit modernization include the Type 99 third-generation main battle tank, a new-generation amphibious assault vehicle, and a series of multiple rocket launch systems.

In October 2010, the PLA conducted its first Group Army-level exercise, which it called “MISSION ACTION (SHIMING XINGDONG).” The primary participants from the Beijing, Lanzhou, and Chengdu Military Regions practiced maneuver, ground-air coordination, and long-distance mobilization via military and commercial assets as they transited between MRs. Given that these MRs are located along China’s land borders, the exercise scenario was likely based on border conflict scenarios. In addition to providing large-scale mobility and joint experience, the exercise allowed PLA command staff to test their ability to plan and execute a large joint campaign while practicing communication between command elements across dispersed forces. This skill is critical to responding to crises along China’s periphery.

## DEVELOPMENTS IN CHINA’S SPACE AND CYBER CAPABILITIES

**Space and Counterspace Capabilities.** In 2010, China conducted a national record 15 space launches. It also expanded its space-based intelligence, surveillance, reconnaissance, navigation, meteorological, and communications satellite constellations. In parallel, China is developing a multi-dimensional program to improve its capabilities to limit or prevent the use of space-based assets by adversaries during times of crisis or conflict.

- During 2010, Beijing launched five BeiDou navigation satellites. China plans

to complete a regional network by 2012 and a global network by 2020.

- China launched nine new remote sensing satellites in 2010, which can perform both civil and military applications.
- In 2010, Beijing also launched two communications satellites (one military and one civil), a meteorological satellite, two experimental small satellites, and its second lunar mission during the year.
- China continues to develop the Long March V (LM-V) rocket, which is intended to lift heavy payloads into space. LM-V will more than double the size of the Low Earth Orbit and Geosynchronous Orbit payloads China is capable of placing into orbit. To support these rockets, China began constructing the Wenchang Satellite Launch Center in 2008. Located on Hainan Island, this launch facility is expected to be complete by 2012, with the initial LM-V launch scheduled for 2014.

**Cyberwarfare Capabilities.** In 2010, numerous computer systems around the world, including those owned by the U.S. Government, were the target of intrusions, some of which appear to have originated within the PRC. These intrusions were focused on exfiltrating information. Although this alone is a serious concern, the accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks. China’s 2010 Defense White Paper notes China’s own concern over foreign cyberwarfare efforts and highlighted the importance of cyber-security in China’s national defense.

Cyberwarfare capabilities could serve PRC military operations in three key areas. First and foremost, they allow data collection through exfiltration. Second, they can be employed to constrain an adversary’s actions or slow response time by targeting network-based logistics, communications, and commercial activities. Third, they can serve as a force multiplier when coupled with

kinetic attacks during times of crisis or conflict.

Developing capabilities for cyberwarfare is consistent with authoritative PLA military writings. Two military doctrinal writings, *Science of Strategy*, and *Science of Campaigns* identify information warfare (IW) as integral to achieving information superiority and an effective means for countering a stronger foe. Although neither document identifies the specific criteria for employing computer network attack against an adversary, both advocate developing capabilities to compete in this medium.

*The Science of Strategy* and *Science of Campaigns* detail the effectiveness of IW and computer network operations in conflicts and advocate targeting adversary command and control and logistics networks to impact their ability to operate during the early stages of conflict. As the *Science of Strategy* explains, “In the information war, the command and control system is the heart of information collection, control, and application on the battlefield. It is also the nerve center of the entire battlefield.”

In parallel with its military preparations, China has increased diplomatic engagement and advocacy in multilateral and international forums where cyber issues are discussed and debated. Beijing’s agenda is frequently in line with the Russian Federation’s efforts to promote more international control over cyber activities. China has not yet agreed with the U.S. position that existing mechanisms, such as International Humanitarian Law and the Law of Armed Conflict, apply in cyberspace. China’s thinking in this area is evolving as it becomes more engaged.

#### **DEVELOPMENTS IN CHINA’S DEFENSE TECHNOLOGY ACQUISITION**

China relies on foreign technology, acquisition of key dual-use components, and focused indigenous research and development (R&D) to advance military modernization.

The PRC also utilizes a large, well-organized network of enterprises, defense factories, affiliated research institutes, and computer network operations to facilitate the collection of sensitive information and export-controlled technology, as well as basic research and science that supports U.S. defense system modernization.

Many of the organizations comprising China’s military-industrial complex have both military and civilian research and development functions. This network of government-affiliated companies and research institutes often enables the PLA to access sensitive and dual-use technologies or knowledgeable experts under the guise of civilian research and development. The enterprises and institutes accomplish this through technology conferences and symposia; legitimate contracts and joint commercial ventures; partnerships with foreign firms; and joint development of specific technologies.

In the case of key national security technologies, controlled equipment, and other materials not readily obtainable through commercial means or academia, the PRC has utilized its intelligence services and employed other illicit approaches that violate U.S. laws and export controls.

- In August 2010, Noshir Gowadia was convicted of providing the PRC with classified U.S. defense technology. Gowadia assisted the PRC in developing a low-signature cruise missile exhaust system capable of rendering a cruise missile resistant to detection by infrared missiles.
- In September 2010, Chi Tong Kuok was convicted for conspiracy to illegally export U.S. military encryption technology and smuggle it to Macau and Hong Kong. The relevant technology included encryption, communications equipment, and Global Positioning System (GPS) equipment used by U.S. and NATO forces.

## CHALLENGES TO TAIWAN'S DETERRENT FORCES

There were no armed incidents in the vicinity of the Taiwan Strait in 2010 and the overall situation remained stable. However, the PRC's military modernization and the deployment of advanced capabilities opposite the island have not eased, and the balance of military force continues to shift in Beijing's favor.

Taiwan President Ma Ying-jeou's defense reforms designed to streamline and professionalize the military continue, but budget shortfalls and escalating costs will lengthen the time necessary for implementation.

Taiwan plans to cut its military force to 215,000 troops and transition to an all-volunteer military by 2015, but recruitment and cost challenges may require a reevaluation of the scope or implementation schedule. It will also reorganize several support commands and looks to civilianize its key defense research and development facilities to improve efficiency and productivity.

Consistent with the provisions of the Taiwan Relations Act, Public Law 96-8 (1979), the United States continues to make available defense articles and defense services to enable Taiwan to maintain a sufficient self-defense capability. Toward this end, in January 2010, the Obama Administration announced its intent to sell to Taiwan \$6.4 billion in defensive arms and equipment, including UH-60 utility helicopters; PATRIOT PAC-3 air and missile defense systems; HARPOON training missiles; Multifunctional Information Distribution Systems technical support for Taiwan's Syun An command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) system; and OSPREY-class minehunting ships.

## CHINA'S FOREIGN MILITARY ENGAGEMENT

China's military engages with foreign militaries to build relationships, improve functional capabilities, and shape foreign perceptions of China. PLA engagement activities support China's military modernization goals through acquisition of advanced weapons systems; increased operational experience both within and beyond Asia; and access to foreign military practices, operational doctrine, and training methods.

- China continues to conduct counter-piracy operations in the Gulf of Aden. PLA Navy ships have remained in the Gulf of Aden since January 2009. In July 2011 the PLA Navy deployed its ninth escort formation. Outside of foreign "goodwill cruises," this represents the PLA Navy's only series of operational deployments beyond the immediate western Pacific region.
- China's Ministry of National Defense (MND) announced that by December 2010, it had comprehensively expanded foreign military relations through establishment of military relations with over 150 countries, including attaché offices in 112 countries. 102 countries have military attaché offices in China. The PLA continues sending over 170 military delegations overseas every year and receiving over 200 foreign military delegations as part of high-level strategic consultations and professional and technical exchanges.
- In April 2010, China introduced its "August First" aerial demonstration team to the international media and discussed the PLA Air Force's intention for the team to perform in foreign countries.

**Combined Exercises.** PLA participation in bilateral and multilateral exercises is increasing. The PLA derives political benefit through increased influence and enhanced ties



with partner states and organizations. Such exercises provide the PLA opportunities to improve capabilities and gain operational insights by observing tactics, command decision-making, and equipment used by more advanced militaries.

- During the recently completed 11<sup>th</sup> Five-Year Plan, the PLA held 32 joint exercise and training events with foreign militaries. These activities covered issues such as counter-terrorism, maritime drills, ground forces training, peacekeeping, and search and rescue.
- In July, PLA and Brazilian special operations forces conducted FRIENDSHIP-2010, a joint counter-terrorism exercise, which included live fire exercises supported by fighter/bombers, transport aircraft, and attack and transport helicopters.
- China and Peru conducted “PEACE ANGEL 2010,” a humanitarian medical rescue exercise in November.
- In early November, the PLA conducted FRIENDSHIP ACTION-2010 with Albanian forces. This marked the PLA’s third exercise with foreign troops within China and the first with a European military.
- The PLA Air Force participated in two major international events in 2010; a bilateral air exercise with Turkey and subsequently, PEACE MISSION 2010, which was conducted under the auspices of the Shanghai Cooperation Organization. This latter exercise involved launching air operations from PRC bases to fly missions over Kazakhstan.

**Peacekeeping and Humanitarian Assistance/Disaster Relief Operations.** China’s participation in UN peacekeeping operations increased six-fold during the six-year period from January 2004 to January 2010. China is now the leading contributor of peacekeeping personnel among the five permanent members

of the UN Security Council. China’s contributions have included engineering, logistics, medical troops, civilian police, and observers. In January 2004, China had 359 peacekeepers deployed to eight UN peacekeeping missions, with no single contingent larger than 70 troops. As of January 2010, China had 2,131 peacekeepers supporting 10 UN missions, with five separate contingents larger than 200 troops.

- In September 2010, China co-hosted its first UN peacekeeping senior commanders training course at the PRC MND Peacekeeping Center.
- China has maintained a force of 125 riot police in Haiti, in support of the UN stabilization force. After Haiti suffered a devastating earthquake in January 2010, these riot police provided escorts to the PRC medical team Beijing dispatched to the country for humanitarian support.

China’s civilian and military leaders have identified humanitarian assistance and disaster relief as an area for China to cooperate with foreign partners and advance PRC interests.

- As of early 2011, China had pledged 250 million U.S. dollars to Pakistan for flood relief. This pledge of aid, which came after international criticism of China’s initial response, constituted China’s largest-ever humanitarian aid package to a foreign nation. Beijing dispatched two of its international search-and-rescue teams to aid Pakistan, and the PLA sent a medical team. In another first for China, the PLA deployed four military helicopters out of China to support the relief effort.
- In July 2010, China’s Ministry of National Defense announced that the PLA had participated in at least 20 international humanitarian rescue missions since 2002, and that its international rescue team had joined six international rescue missions since its creation in 2001.

## CHAPTER TWO: UNDERSTANDING CHINA'S STRATEGY

---

### OVERVIEW

China's leaders characterize the initial two decades of the 21<sup>st</sup> century as a "strategic window of opportunity." They assess that during this period, both domestic and international conditions will be conducive to expanding China's "comprehensive national power" (*zonghe guoli*—综合国力), a term that encapsulates all elements of state power including economic capacity, military might, and diplomacy. Speaking in December 2010, PRC Defense Minister Liang Guanglie asserted that "making the country prosperous and making the armed forces strong are two major cornerstones for realizing the great rejuvenation of the Chinese nation." China's leaders anticipate that a successful expansion of comprehensive national power will serve China's overriding strategic objectives, which include perpetuating CCP rule; sustaining economic growth and development; maintaining domestic political stability; defending national sovereignty and territorial integrity; and securing China's status as a great power.

In the near term, the PRC regards stable relations with the U.S. and China's neighbors as essential to stability and critical to maximizing this window of opportunity. At the same time, China's growing economic and military confidence and capabilities occasionally manifest in more assertive rhetoric and behavior when Beijing perceives threats to its national interests or feels compelled to respond to public expectations.

The PRC is particularly concerned that regional actors might counterbalance China's rise through military development and coalitions. China publicly states that its rise is "peaceful" and that it harbors no "hegemonic" designs or aspirations for territorial expansion. However, China's lack of transparency surrounding these growing

capabilities has increased concerns in the region about China's intentions.

### UNDERSTANDING CHINESE STRATEGY

China uses white papers, speeches, and articles as the principal mechanisms to publicly communicate policy and strategy. Published on March 31, 2011, China's Defense White Paper for 2010 summarizes four national defense "goals" as:

- safeguarding national sovereignty, security and interests of national development;
- maintaining social harmony and stability;
- accelerating the modernization of national defense and the armed forces; and,
- maintaining world peace and stability.

The Defense White Paper for 2010 notes that China continues to implement the military strategy of "Active Defense" and is enhancing "national strategic capabilities" while maintaining China's "no first use" policy on nuclear weapons. China's stated defense strategy is focused on fostering a security environment conducive to China's comprehensive development.

While addressing many of the themes presented in previous PRC Defense White Papers, the latest version conveys some important differences. The new document expresses confidence that the China's position relative to other major powers has improved substantially. Relations with the United States are portrayed with a degree of concern, while the current state of cross-Strait relations is presented in a favorable light. The latest version highlights the PLA's growing focus on military operations other than war, but



overall, the document presents only incremental new insights into the PLA's structure, doctrine and capabilities. Overall, the transparency of China's military and security affairs has improved gradually in recent years, highlighted by its publication of

Defense White Papers, establishment of a MND spokesperson, the launch of an official MND website, wider media coverage of military issues, and growing availability of books and professional journals on military and security topics.

### **Military Decision Making Structures and Processes in China**

The PLA is the armed instrument of the Chinese Communist Party (CCP) and organizationally, is subordinate to the Party apparatus. Career military officers are CCP members, and units at the company level and above have political officers responsible for personnel decisions, propaganda, and counterintelligence. Major decisions at all levels are made by CCP committees, also led by the political officers and commanders.

The PLA's highest decision-making body, the Central Military Commission (CMC), is technically a department of the CCP Central Committee, but is staffed primarily by military officers. The Chairman is a civilian, usually the General Secretary of the CCP and the President. Other members include the commanders of the service arms and the four general headquarters departments, and a number of Vice Chairmen.

Vice President Xi Jinping, the anticipated successor to PRC President Hu Jintao, is one of three Vice Chairmen and the only other civilian on the CMC. China's Ministry of National Defense is a relatively small office specializing in military-related tasks that are the responsibility of the civilian government rather than the armed forces, including foreign military relations, mobilization, recruitment, and civil support to military operations. The Minister of Defense is a uniformed military officer and CMC member.

The PLA currently has less representation in key party decision-making bodies than in the mid-1990s or even the mid-2000s. With the passing of China's revolutionary generation, fewer national leaders hail from a military background. However, PLA leaders are increasingly inclined to voice their thoughts and opinions on international affairs in the public domain.

# The Chinese High Command



*The PRC Military Structure*

### **China's Upcoming Military Leadership Transition**

China's civilian and military leadership are expected to undergo extensive changes during the 18<sup>th</sup> Party Congress, likely to be held in the fall of 2012. Vice President Xi Jinping was appointed Vice Chairman of the Central Military Commission (CMC) in October 2010. It is unclear whether Hu will follow in the footsteps of his predecessor Jiang Zemin and remain CMC chairman for some period of time after relinquishing his other leadership roles.

The uniformed CMC membership is also expected to experience a major transition during the 18<sup>th</sup> Party Congress. Seven of the ten uniformed CMC members will almost certainly retire based on age limits. In December 2010, Defense Minister Liang highlighted the PLA's shift towards a "more rational" force structure as the Navy, Air Force, and Second Artillery Corps take on a larger and more prominent place in the PLA.

#### **The three uniformed members expected to retain their CMC posts beyond 2012 are:**

**General Chang Wanquan**, Director of the General Armament Department (GAD), is the only ground forces officer eligible by age to serve an additional term. A former commander of the Shenyang Military Region (MR) and chief of staff of the Beijing MR, General Chang spent most of his career in operations and training posts in the Lanzhou MR. He also served as director of the campaign teaching and research office at the National Defense University in the late 1990s. In his current post as GAD director, Chang oversees foreign weapon procurement and domestic production, military testing, and the space and satellite programs. Two current senior CMC members, Chief of the General Staff Chen Bingde and director of the General Political Department Li Jinai, are also former GAD chiefs, underscoring the emphasis the Party has placed on these elements of the PLA's modernization program.

**Admiral Wu Shengli**, the Commander of the PLA Navy, has presided over a substantial increase in the Navy's international engagement, including its ongoing counter-piracy deployment to the Gulf of Aden. A former destroyer captain in China's East Sea Fleet and later commandant of the Dalian Naval Vessels Academy who rose to become commander of the South Sea Fleet, Wu also served as a deputy chief of the general staff in the mid-2000s. He is the second naval officer to serve on the CMC since the Navy, Air Force and 2<sup>nd</sup> Artillery Corps commanders were added to its membership in 2004.

**General Xu Qiliang**, the Commander of the PLA Air Force is a former pilot who served much of his career in the Nanjing MR opposite Taiwan. He rose to Chief of Staff of the Beijing MR Air Force and then Commander of the Shenyang MR Air Force. Along with Wu Shengli, his promotion to Commander of his service followed a tour as a Deputy Chief of the General Staff in the mid-2000s.

## CHINA'S STRATEGIC PRIORITIES

Since China launched its “reform and opening,” in 1978, the essential elements of China’s strategy have remained relatively constant. Rather than challenge the existing global order, China has adopted a pragmatic approach to international relations and economic development that seeks to strengthen the economy, modernize the military, and solidify the CCP’s hold on power. This approach reflects Beijing’s assumption that great power status over the long-term is best achieved by avoiding confrontation in the near-term. China’s leaders routinely emphasize the goal of reaching critical economic and military benchmarks by 2020 and eventually becoming a world-class economic and military power by 2050.

China’s leaders appear to make decisions based on an array of interrelated and sometimes competing strategic priorities, which include perpetuating CCP rule; sustaining economic growth and development; maintaining domestic political stability; defending national sovereignty and territorial integrity; and securing China’s status as a great power. Although evolving security challenges and growing capabilities have prompted adjustments over the past three decades, the overarching strategic vision has remained largely intact.

During 2010, China continued on a path toward its long-term strategic objectives. Despite domestic concerns over inflation, growing income disparities, and a possible housing bubble, to date China’s economy appears to have weathered the global economic turmoil with relative success. In 2010, the PRC economy surpassed that of Japan to become the world’s second largest. Although PRC leaders remain concerned over a number of economic challenges, many analysts have suggested that China’s economic performance in recent years has endowed Beijing with greater confidence in its economic model and in its relative strength.

Militarily, China’s sustained modernization program is paying visible dividends. During 2010, China made strides toward fielding an operational anti-ship ballistic missile, continued work on its aircraft carrier program, and finalized the prototype of its first stealth aircraft. Despite continued gaps in some key areas, large quantities of antiquated hardware, and a lack of operational experience, the PLA is steadily closing the technological gap with modern armed forces.

China’s leaders speak about their strategic priorities in terms of what they call China’s “core interests.” In a December 2010 exposition on China’s foreign policy, State Councilor Dai Bingguo enumerated China’s core interests as:

- The state system, political system, and political stability of China; that is the leadership of the CCP, the socialist system, and the path of socialism with Chinese characteristics.
- The sovereignty and security, territorial integrity, and national unity of China.
- The basic guarantee for the sustained development of the economy and society of China.

The PRC leadership is also focused on the many potential problems that could complicate or derail China’s growth trajectory or its strategy of “peaceful development.” These include the following:

- Economics: Continued economic development remains the bedrock of social stability and underwrites China’s military power. A wide range of economic factors could disrupt this trajectory, including the rapid contraction of a potentially overheated economy. China’s leaders have already scaled back GDP targets for 2011-2015 to mitigate risk of overheating and to manage expectations. Other potential economic risks for China include shifting global trade patterns, resource constraints, or attempts to challenge access to resources.

- **Nationalism:** Communist Party leaders and military officials continue to exploit nationalism to bolster the legitimacy of the Party and deflect domestic criticism. However, this approach is inherently risk-laden, as these forces could easily turn against the state or complicate China's policy process. Nationalistic appeals for a more muscular PRC posture, particularly during times of crisis, effectively constrain more moderate, pragmatic elites in China's foreign policy establishment. Alternatively, PRC elites may point to nationalism as a justification for their own inflexibility in dialogues with foreign interlocutors.
- **Growing Expectations:** China's development has translated into greater expectations both at home and abroad for involvement in the international arena. Other nations have called on Beijing to shoulder a greater role in solving international problems, to a point at which some Chinese leaders worry about taking on more than they can handle. At the same time, the domestic perception of China's growing status is producing popular demands for a more assertive pursuit of China's international interests.
- **Regional Balancing:** China's growing economic, diplomatic and military presence and influence in Asia and globally is raising concerns among many countries about China's ultimate aims – and the threats this could present to them. These regional concerns could catalyze regional or global balancing efforts.
- **Domestic Political Pressures:** Regime survival shapes the strategic outlook of China's leaders and drives decision making. The Communist Party continues to face long-term popular demands for improved government responsiveness, transparency and accountability. If unmet, these factors weaken CCP legitimacy.
- **Demographic Pressures:** Demographic stresses will increase in the future, creating a structural constraint on China's ability to sustain high economic growth rates as well as a social challenge for the CCP.
- **Environment:** China's economic development has come at a high environmental cost. China's leaders are increasingly concerned that environmental degradation could undermine regime legitimacy by threatening economic development, public health, social stability, and China's international image.
- **Cross-Strait Dynamics:** Despite a reduction in tensions following the March 2008 election of Taiwan President Ma Ying-jeou, the possibility of a military conflict with Taiwan, including U.S. military intervention, remains a pressing, long-term focus for the PLA. In the absence of a peaceful cross-Strait resolution or long-term non-aggression pact, the Taiwan mission will likely continue to dominate PLA modernization and operational planning.

### **China's Territorial Disputes**

China faces extensive territorial disputes along its land and maritime periphery. Next to the status of Taiwan, these disputes play a central role in PLA planning. Although China has generally adopted a less confrontational posture towards its regional disputes since the late 1990s (China has settled eleven land disputes with six of its neighbors since 1998), some regional actors fear China's growing military and economic weight is beginning to produce a more assertive posture, particularly in the maritime domain.

In addition to a longstanding and contentious border dispute with India, China has maritime boundary disputes with Japan over the East China Sea and throughout the South China Sea with Vietnam, Malaysia, the Philippines, Brunei, and Taiwan. These have sparked occasional armed conflict, including a 1962 border conflict with India and a 1979 ground invasion of Vietnam. In the South China Sea, China fought Vietnamese forces in the Paracel Islands in 1974 and near Fiery Cross Reef in 1988. In 1995, China occupied Mischief Reef, also in the Spratly Islands, amid protest from the Philippines. In 2002, Beijing and ASEAN brokered a Declaration on Conduct in the South China Sea. While non-binding, the declaration was followed by a period of relative stability.

China's broad claim to potentially all of the South China Sea remains a source of regional contention. Beginning in the 1930s and 1940s, the Republic of China began publishing regional maps with a dashed line around the perimeter of South China Sea. After taking power in 1949, the CCP maintained this claim. Both the PRC and Taiwan continue to base their South China Sea claims on that broad delineation. China increasingly regards the South China Sea as a vital commercial and security corridor for East and Southeast Asia.

In recent years, some of China's neighbors have questioned Beijing's long-term commitment to peacefully and cooperatively resolve the remainder of its disputes. PLA Navy assets have repeatedly circumnavigated the South China Sea since 2005, and civilian enforcement ships, sometimes supported by the PLA Navy, have occasionally harassed foreign vessels. Underscoring the volatility of these various disputes, a PRC-flagged fishing boat collided with Japanese Coast Guard vessels near the disputed Senkaku Islands in the East China Sea, triggering a highly charged political standoff between Tokyo and Beijing in September 2010.





**China's Disputed Territories.** This map is an approximate presentation of PRC and other regional claims. China has remained ambiguous on the extent and legal justification for these regional claims. Three of China's major ongoing territorial disputes are based on claims along its shared border with India and Bhutan, the South China Sea, and with Japan in the East China Sea.

## THE NEW HISTORIC MISSIONS

In 2004, Hu Jintao articulated a mission statement for the armed forces titled, the “Historic Missions of the Armed Forces in the New Period of the New Century” (*xin shiji xin jieduan wojun lishi shiming*—). These “new historic missions” focus primarily on adjustments in the PRC leadership’s assessment of the international security environment and the expanding definition of national security. These missions were further codified in a 2007 amendment to the CCP Constitution. The missions, as currently defined, include:

- Provide an important guarantee of strength for the party to consolidate its ruling position.

- Provide a strong security guarantee for safeguarding the period of strategic opportunity for national development.
- Provide a powerful strategic support for safeguarding national interests.
- Play an important role in safeguarding world peace and promoting common development.

According to official writings, the driving factors behind the articulation of these missions were: changes in China’s security situation, challenges and priorities regarding China’s national development, and a desire to realign the tasks of the PLA with the CCP’s objectives. Politburo member and CMC Vice Chairman Xu Caihou in 2005 asserted “the historic missions embody the new requirements imposed on the military by the Party’s historic tasks, accommodate new

changes in our national development strategy, and conform to the new trends in global military development.”

In a point reiterated in the latest PRC Defense White Paper, economic development remains a central task and the PLA is expected to support China’s economic interests and security. This poses new challenges for a military that, until recently had virtually no operational experience outside of its region.

President Hu Jintao’s strategic guidance to the military reflects this view, calling on the PLA to play a broader role in securing China’s strategic interests, including those beyond its territorial boundaries. In a March 2009 speech to military delegates to China’s National People’s Congress, President Hu urged the military to concentrate on “building core military capabilities,” but also “the ability to carry out military operations other than war” (*fei zhanzheng junshi xingdong*—非战争军事行动). Hu maintained, “with the prerequisite of satisfactorily completing all missions—taking preparation for military struggle as the lead—the armed forces must participate actively in and support national economic construction and public welfare.”

China’s 2010 Defense White Paper highlights the PLA’s evolving roles and missions, noting that:

*They organize preparations for military operations other than war (MOOTW) in a scientific way, work out pre-designed strategic programs against non-traditional security threats, reinforce the building of specialized forces for emergency response, and enhance capabilities in counter-terrorism and stability maintenance, emergency rescue, and the protection of security.*

Authoritative PRC media describe these “military operations other than war” as including: counter-terrorism, maintaining social stability, disaster relief and rescue, and international peacekeeping operations. China’s leaders have mentioned other “non-war military” activities including protecting

sea lanes, cyber warfare, security of space-based assets, conducting military diplomacy, and preparing for unexpected conditions and events.

- The PLA Navy’s ongoing deployment to conduct counter-piracy escort missions in the Gulf of Aden is one example of China’s pursuit of its new historic missions.
- Another example was the 2010 voyage of China’s first large hospital ship, which made stops in Asia and Africa. The ship is able to support combat operations, but PRC official press reporting stresses the humanitarian aspects of the ship’s mission.
- Most recently, the PLA employed lift assets to assist in the evacuation of PRC citizens from Libya. This marked the PLA’s first noncombatant evacuation operation (NEO).

## DEBATES ON FUTURE STRATEGY

China’s current strategy remains one of managing the external environment to ensure conditions are conducive to China’s economic development and military modernization. This approach serves the paramount goal of preserving the survival and leadership of the CCP. Although this strategy appears to enjoy widespread acceptance among Beijing’s foreign and security policy establishment, military and academic writings reveal differences of opinion concerning the means of achieving China’s broad national objectives.

Although the view is increasingly articulated that the time has come for China to discuss more candidly and pursue its national interests, the prevailing voices within China’s leadership have supported former paramount leader Deng Xiaoping’s dictum from the early 1990s that China should, “observe calmly; secure our position; cope with affairs calmly; hide our capabilities and bide our time; be good at maintaining a low profile; and never claim leadership.” This guidance reflected

Deng's belief that PRC interests are best served by focusing on internal development and stability while steering clear of direct confrontation or antagonism with major powers. In December 2010, State Councilor Dai Bingguo specifically cited Deng's guidance, insisting China adhered to a "path of peaceful development" and would not seek expansion or hegemony. He asserted that the "hide and hide" rhetoric was not a "smokescreen" employed while China builds its strength, but rather an admonition to be patient and not stand out.

Some PRC scholars question whether Deng's policy approach will continue to win support as China's interests and power expand. China's perceived security interests have changed considerably since Deng's era to include a heavy reliance on maritime commerce. China's improving naval capabilities enable roles and missions that

would have been impossible for the PLA to pursue just a decade ago. Proponents of a more active and assertive PRC role on the world stage have suggested that China would be better served by a firm stance in the face of U.S. or other regional pressure.

There has also been an active debate among military and civilian theorists in China concerning future capabilities the PLA should develop to advance China's interests beyond traditional requirements. Some senior officers and civilian theorists advocate an expansion of the PLA's power projection capabilities to facilitate missions well beyond Taiwan and regional disputes. Publicly, PRC officials contend that increasing the scope of China's maritime capabilities is intended to build capacity for international peacekeeping, humanitarian assistance, disaster relief, and protection of sea lanes.

### **China Debates its National Security Strategy in 2010**

Throughout 2010, a line of commentary in Western and Chinese media and academic circles, suggested that China has grown stronger relative to the United States, particularly as a result of the global financial crisis. Some commentators asserted that a more powerful China should more proactively pursue its national interests. While this increasingly public debate indicates the CCP is allowing discussion of competing strategic priorities, there is little indication that its senior leaders are abandoning Deng Xiaoping's foreign policy legacy in the near term.

The tension between managing China's image and advancing China's interests was revealed on several occasions in 2010. This included discussions of how Beijing should respond to South China Sea tensions and U.S.-South Korea joint exercises in the Yellow Sea. Much of the resulting commentary hailed perceptions that Beijing had taken a stronger stand on these issues in line with its growing international weight. Some commentators argued that China needed to take a still stronger stand or asserted that on the contrary, Beijing lacked sufficient power to sustain a more assertive position, despite a relative U.S. decline.

An increasingly public debate in China regarding the exercise of national power reflects the fact that both assertive and accommodating behaviors come with a set of costs for Beijing. Many in China feel that the steady expansion of comprehensive national power entitles China to greater respect and deference. However, during the current "strategic window of opportunity," the Chinese leadership remains wary of undermining their long-term objectives.

By autumn 2010, commentary on security relations with the United States had moderated, probably due to efforts to smooth the way for President Hu Jintao's planned early 2011 visit to the United States. The official communiqué of the 5<sup>th</sup> Plenum of the 17<sup>th</sup> CCP Central Committee held from October 15-18, 2010: "stressed that our country is still in the important strategic opportunity period." We judge this to be a re-affirmation of Deng's strategy of carefully preserving a stable environment for China's development as opposed to a call for Beijing to take a more assertive stance.



### Military and Security Aspects of Beijing's Regional Energy Strategy

China's engagement, investment, and foreign construction related to energy continue to grow. Beijing has constructed or invested in energy projects in more than 50 countries, spanning nearly every continent. This ambitious investment in energy assets is driven primarily by two factors. First, Beijing is increasingly dependent upon imported energy to sustain its economy. A net oil exporter until 1993, China still lacks trust in international energy markets. Second, energy projects present a viable option for investing China's vast foreign currency holdings.

In addition to ensuring reliable energy sources, Beijing hopes to diversify both producers and transport options. Although energy independence is no longer realistic for China, given population growth and increasing per capita energy consumption, Beijing still seeks to maintain a supply chain less susceptible to external disruption.

In 2009, China imported approximately 56 percent of its oil and conservative estimates project that China will import almost two-thirds of its oil by 2015 and three-quarters by 2030. Beijing looks primarily to the Persian Gulf, Central Asia, and Africa to satisfy its growing demand for oil. Imported oil contributes to approximately 10% of China's total energy consumption.

A second goal of Beijing's foreign energy strategy is to alleviate China's heavy dependence on Sea Lines of Communication (SLOCs), particularly the South China Sea and Strait of Malacca. In 2010, over 80 percent of China's oil imports transited the South China Sea and Strait of Malacca. A crude oil pipeline from Kazakhstan to China illustrates efforts to increase overland supply. In January 2011, a 300,000 b/d spur pipeline from Siberia to Daqing began delivering crude to China. China also commenced construction on a pipeline designed to transport crude oil and natural gas from Kyuakpya, Burma, to Kunming, China, bypassing the Strait of Malacca.

China's Top Crude Oil Suppliers 2009

Country	Volume	%
Saudi Arabia	843	21
Angola	646	16
Iran	465	11
Russia	307	8
Sudan	245	6
Oman	234	6
Iraq	144	4
Kuwait	142	3
Libya	127	3
Kazakhstan	121	3
Other	818	19
<b>TOTAL</b>	<b>4,092</b>	

Volumes are in 1,000 barrels per day  
Figures have been rounded





*China's import transit routes/critical chokepoints and proposed/under construction SLOC bypass routes.*

Given China's growing energy demand, new pipelines will only slightly alleviate China's maritime dependency in either the Strait of Malacca or the Strait of Hormuz. The sheer volume of oil and liquefied natural gas imports to China from the Middle East will make strategic SLOCs increasingly important to Beijing.

In 2009 a pipeline that will deliver up to 40 billion cubic meters (bcm) of natural gas per year from Turkmenistan to China via Kazakhstan and Uzbekistan commenced operation. Another natural gas pipeline designed to deliver 14 bcm per year from Burma is in the initial stages of construction and estimated for completion in 2013. Additionally Beijing is negotiating with Moscow for two pipelines that could supply China with up to 69 bcm of gas.



## CHINA'S MILITARY STRATEGY

PLA theorists have developed a framework for doctrine-driven reform with the long-term goal of building a force capable of fighting and winning “local wars under conditions of informatization.” Drawing upon foreign military experiences, particularly U.S.-led campaigns up to and including Operation ENDURING FREEDOM and Operation IRAQI FREEDOM, Soviet and Russian military theory, and the PLA’s own combat history, China is transforming across the whole of its armed forces.

China relies on a body of overall principles and guidance known as the “National Military Strategic Guidelines for the New Period” (*xin shiqi guojia junshi zhanlue fangzhen*—**期国家军事战略方针**) to plan and manage the development and use of the armed forces. This is the closest equivalent in China of the U.S. “National Military Strategy.”

The current operational component of China’s National Military Strategic Guidelines for the New Period is known as “Active Defense” (*jiji fangyu*—**积极防御**). Active Defense is the highest-level strategic guidance for all PLA activities and applies to all services. Tenets of Active Defense include the following:

- “Overall, our military strategy is defensive. We attack only after being attacked. But our operations are offensive.”
- “Space or time will not limit our counter-offensive.”
- “We will not put boundaries on the limits of our offenses.”
- “We will wait for the time and conditions that favor our forces when we do initiate offensive operations.”
- “We will focus on the opposing force’s weaknesses.”

Academic research suggests that the current guidelines most likely date to 1993, reflecting the impact of the 1991 Persian Gulf War and the collapse of the Soviet Union on PRC military-strategic thinking. The guidelines were revised in 2002 and 2004, likely reflecting China’s perceptions of its evolving security environment and the changing character of modern warfare.

In practice, this strategic evolution has prompted a major shift toward investments in asymmetric, network-centric warfare and A2AD capabilities that are intended to deny elements of the modern battle space to potential enemies. According to the 2008 Defense White Paper, these guidelines emphasize fighting and winning local wars under conditions of informatization and building toward integrated joint operations, with a stress on asymmetric warfare to “make the best use of our strong points to attack the enemy’s weak points.”

Citing the need to ensure “close coordination between military struggle and political, diplomatic, economic, cultural, and legal endeavors,” the guidelines also emphasize the importance of integrating multiple instruments of state power to ensure deterrence and prevent conflict.

**Naval Warfare.** During the mid 1980s, the CMC approved a specific naval component of “Active Defense” called “Offshore Defense” (*jinhai fangyu*—**近海防御**), which is sometimes translated more literally as, “Near Seas Defense.” Offshore Defense is an overarching strategic concept that directs the PLA Navy to prepare for three essential missions including:

- keeping the enemy within limits and resisting invasion from the sea;
- protecting the nation’s territorial sovereignty; and,
- safeguarding the motherland’s unity and maritime rights.

The so-called “near seas,” which remain a primary focus for the Navy, include the

Yellow Sea, East China Sea, and South China Sea. Increasingly, the PLA is taking on missions that reflect China's expanding commercial and diplomatic interests beyond the near seas, into the "far seas" which include the Philippine Sea and beyond. PLA Navy doctrine for maritime operations focuses on six offensive and defensive campaigns: blockade, anti-sea lines of communication, maritime-land attack, anti-ship, maritime transportation protection, and naval base defense.

Senior civilian officials and PLA officers have argued that China's economic and political power is contingent upon access to, and use of the sea, and that a strong Navy is required to safeguard such access. Despite an increasingly public discussion concerning missions farther from China, the Navy appears primarily focused on contingencies within the "first and second island chains" (see map), with emphasis on a potential conflict with U.S. forces over Taiwan or a territorial dispute.



**The First and Second Island Chains.** PRC military theorists refer to two "island chains" along China's maritime perimeter. The First Island Chain includes Taiwan and the Ryuku Islands, the Second Island Chain extends from Japan to Guam.

**Ground Warfare.** Under “Active Defense,” ground forces are tasked with defending China’s borders, ensuring domestic stability, and exercising regional power projection. PLA ground forces are transitioning from a static defensive force allocated across seven internal MRs, oriented for positional, mobile, urban, and mountain offensive campaigns; coastal defense campaigns; and landing campaigns, to a more offensive and maneuver-oriented force organized and equipped for operations along China’s periphery.

The 2010 Defense White Paper asserts that the ground force has:

*emphasized the development of new types of combat forces, optimized its organization and structure, strengthened military training in conditions of informatization, accelerated the digitized upgrading and retrofitting of main battle weaponry, organically deployed new types of weapon platforms, and significantly boosted its capabilities in long-distance maneuvers and integrated assaults.*

The ground forces appear to be leading the PLA’s effort to experiment with *ad hoc*, multi-service, joint tactical formations to execute integrated joint operations.

**Air Warfare.** The PLA Air Force continues its conversion from a force for limited territorial defense to a more flexible and agile force able to operate off-shore in both offensive and defensive roles, using the U.S. and Russian air forces as models. Mission focus areas include: strike, air and missile defense, early warning and reconnaissance, and strategic mobility. The PLA Air Force also has a leading role in China’s planning for anti-access and area denial operations.

The PLA’s new missions are also driving discussions about the future of the PLA Air Force, where a general consensus has emerged that protecting China’s global interests requires an increase in the Air Force’s long-range transportation and

logistics capabilities. In September 2010, the PLA Air Force conducted an unprecedented deployment of Su-27 fighter aircraft to Turkey to participate in joint air exercises with the Turkish Air Force. China has also been investing in stealth technology, as evidenced by the appearance of its first stealth aircraft prototype in January 2011. However, as with the Navy, it is likely that the Air Force’s primary focus for the coming decade will remain on building the capabilities required to pose a credible military threat to Taiwan and U.S. forces in East Asia, deter Taiwan independence, or influence Taiwan to settle the dispute on Beijing’s terms.

**Space Warfare.** PLA strategists regard the ability to utilize space and deny adversaries access to space as central to enabling modern, informatized warfare. Although PLA doctrine does not appear to address space operations as a unique operational “campaign,” space operations form an integral component of other PLA campaigns. Publicly, Beijing attempts to dispel any skepticism over its military intentions for space. In 2009, the commander of the PLA Air Force, General Xu Qiliang, publically retracted his earlier assertion that the militarization of space was a “historic inevitability” after President Hu Jintao swiftly contradicted him.

The PLA is acquiring a range of technologies to improve China’s space and counterspace capabilities. A PLA analysis of U.S. and Coalition military operations reinforced the importance of operations in space to enable informatized warfare, claiming that “space is the commanding point for the information battlefield.”

PLA writings emphasize the necessity of “destroying, damaging, and interfering with the enemy’s reconnaissance... and communications satellites,” suggesting that such systems, as well as navigation and early warning satellites, could be among initial targets of attack to “blind and deafen the enemy.” The same PLA analysis of U.S. and



### Offense as Defense

PRC military strategists characterize “Active Defense” as inherently defensive, suggesting that China strikes only “after the enemy has struck.” Taken alone, this statement, which was reiterated in China’s 2010 Defense White Paper, seems clear. However, more detailed Chinese writings leave the actual significance far more ambiguous. In particular, it remains unclear what actions taken by an adversary might cross the threshold of an initial strike.

The *Science of Military Strategy*, which is published by the PLA’s Academy of Military Science, asserts that the definition of an enemy strike is not limited to conventional, kinetic military operations. Rather, an enemy “strike” may also be defined in political terms. Thus:

*Striking only after the enemy has struck does not mean waiting for the enemy’s strike passively... It doesn’t mean to give up the “advantageous chances” in campaign or tactical operations, for the “first shot” on the plane of politics must be differentiated from the “first shot” on that of tactics.*

[This section continues] *if any country or organization violates the other country’s sovereignty and territorial integrity, the other side will have the right to „fire the first shot” on the plane of tactics.*

If China loosely defines a “strike” to encompass some political action, this significantly alters the purportedly “defensive” nature of this strategic construct. This implies that PLA forces might be employed preemptively in the name of defense.

Coalition military operations also states that “destroying or capturing satellites and other sensors... will deprive an opponent of initiative on the battlefield and [make it difficult] for them to bring their precision guided weapons into full play.”

### Integrated Network Electronic Warfare.

PRC military writings highlight the seizure of electromagnetic dominance in the early phases of a campaign as among the foremost tasks to ensure battlefield success. PLA theorists have coined the term “integrated network electronic warfare” (*wangdian yitizhan*—网电一体战) to describe the use of electronic warfare, computer network operations, and kinetic strikes to disrupt battlefield information systems that support an adversary’s warfighting and power projection capabilities. PLA writings identify “integrated network electronic warfare” as one of the basic forms of “integrated joint operations,” suggesting the centrality of seizing and dominating the electromagnetic spectrum in PLA campaign theory.

### SECRECY AND DECEPTION

PRC military writings point to a working definition of strategic deception as “[luring] the other side into developing misperceptions... and [establishing for oneself] a strategically advantageous position by producing various kinds of false phenomena in an organized and planned manner with the smallest cost in manpower and materials.” In addition to information operations and conventional camouflage, concealment, and denial, the PLA draws from China’s historical experience and the traditional role that stratagem and deception have played in Chinese statecraft.

There is an inherent tension in Chinese strategic culture today, pitting a deep-seated tendency to conceal military capabilities and force development against a partial acceptance that excessive secrecy inflames regional and global anxiety about China’s rising power. For over a decade PRC leaders have identified the so called “China threat theory” as a serious hazard to the country’s international standing and reputation, threatening the development of a persistent alignment of regional and global

powers in opposition to China. In addition, extreme secrecy is increasingly difficult to reconcile with China's role in the integrated global economy, which depends upon transparency and the free flow of information for success.

There is perhaps another source of tension between the emerging reality of Chinese military power and China's tradition of secrecy, and that is the fact that many of China's new military capabilities are difficult

or impossible to hide. Examples of such capabilities include advanced aircraft, long range missiles, and modern naval assets. Furthermore, missiles, space-based, and counterspace systems must be tested and exercised before being operationally deployed with confidence. The PLA's growing inventory of these new assets and the ranges at which they operate effectively prevents their concealment.

### “Three Warfares”

The Chinese concept of "three warfares" (*san zhong zhanfa*— ) refers specifically to psychological warfare, media warfare, and legal warfare. It reflects China's desire to effectively exploit these force enablers in the run up to and during hostilities. During military training and exercises, PLA troops employ the “three warfares” to undermine the spirit and ideological commitment of the adversary. In essence, it is a non-military tool used to advance or catalyze a military objective.

- **Psychological Warfare** seeks to undermine an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing enemy military personnel and supporting civilian populations.
- **Media Warfare** is aimed at influencing domestic and international public opinion to build support for China's military actions and dissuade an adversary from pursuing actions contrary to China's interests.
- **Legal Warfare** uses international and domestic law to claim the legal high ground or assert Chinese interests. It can be employed to hamstring an adversary's operational freedom and shape the operational space. Legal warfare is also intended to build international support and manage possible political repercussions of China's military actions. China has attempted to employ legal warfare in the maritime domain and in international airspace in pursuit of a security buffer zone.

In 2003, the CCP Central Committee and the CMC endorsed the “three warfares” concept, reflecting China's recognition that as a global actor, it will benefit from learning to effectively utilize the tools of public opinion, messaging, and influence. China likely hopes to employ these three concepts in unison, particularly during the early stages of a crisis, as they have a tendency to bolster one another.

## CHAPTER THREE: FORCE MODERNIZATION GOALS AND TRENDS

---

### OVERVIEW

Since the early 1990s PRC leaders have sustained an ambitious and broad-based military modernization program intended to transform the PLA into a modern force. Although the PLA currently retains a large number of legacy platforms and weapons, the percentage of modern equipment in the force is growing rapidly. China has closed important technological gaps and achieved some capabilities that are on par with or exceed global standards. Motivated by a growing set of economic and security interests, China's leaders have given the PLA a new and more externally focused direction, as evidenced by China's growing naval presence on the global maritime domain.

For the PLA, this modernization effort remains a work in progress. The first decade of the 21<sup>st</sup> century can be characterized as a period of ambitious PLA acquisition and development. Although this trend will continue in the years ahead, the more dominant theme of the 2010-2020 decade is likely to be training and integration. Senior PRC leaders recognize that this period will prove critical to meeting the PLA's modernization objectives, and they have demanded that the military engage in more realistic training and organizational reform.

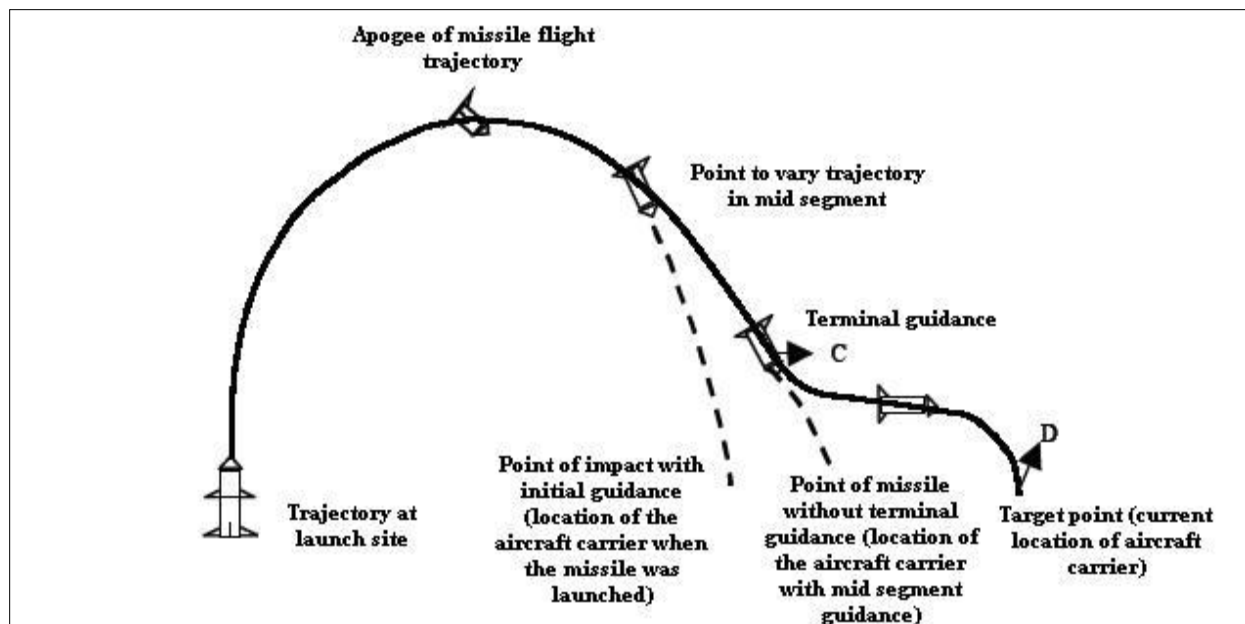
Throughout the PLA's modernization drive, Taiwan contingency planning has largely dominated the agenda. Even though cross-strait tensions have subsided since 2008, Taiwan remains a critical mission, and the

PLA continues building capabilities aimed not only at Taiwan, but also to deter, delay or deny possible U.S. or allied intervention in a cross-strait conflict. At the same time, a diminished sense of urgency over Taiwan has enabled the PLA to devote attention to an expanding set of regional and global missions. This includes a focus on "safeguarding China's expanding national interests" and protecting "sovereignty" as outlined in the New Historic Missions, described in the previous chapter

By the latter half of the current decade, China will likely be able to project and sustain a modest-sized force, perhaps several battalions of ground forces or a naval flotilla of up to a dozen ships, in low-intensity operations far from China. This evolution will lay the foundation for a force able to accomplish a broader set of regional and global objectives. However, it is unlikely that China will be able to project and sustain large forces in high-intensity combat operations far from China prior to 2020.

Despite significant improvements, the PLA continues to face deficiencies in inter-service cooperation and actual experience in joint exercises and combat operations. Recognizing these shortcomings, China's leaders continue to stress asymmetric strategies to leverage China's advantages while exploiting the perceived vulnerabilities of potential opponents. The PLA has also embarked on human capital reform, intended to attract and retain talented personnel.





**Missile Flight Trajectory with Terminal Guidance.** This graphic of an anti-ship ballistic missile's use of mid-course and terminal guidance to strike an aircraft carrier appeared in a 2006 article from the Second Artillery Engineering College.

## ANTI-ACCESS/AREA DENIAL CAPABILITY DEVELOPMENTS

As part of its planning for a regional contingency, China is developing measures to deter or counter third-party intervention, including by the United States. Although many of these capabilities were developed with a focus on Taiwan, they have broad applications and implications extending beyond a Taiwan scenario. China's approach to this challenge, which it refers to as "counter-intervention," is manifested in a sustained effort to develop the capability to attack, at long ranges, military forces that might deploy or operate within the western Pacific. The U.S. Department of Defense characterizes these as "anti-access" and "area denial" capabilities. China is pursuing a variety of air, sea, undersea, space, counterspace, information warfare systems, and operational concepts to achieve this capability, moving toward an array of overlapping, multilayered offensive capabilities extending from China's coast into the western Pacific.

An essential element of China's emerging A2AD regime is the ability to control and dominate the information spectrum in all dimensions of the modern battlespace. PLA authors often cite the need in modern warfare to control information, sometimes termed "information blockade" or "information dominance," and gain an information advantage in the early phases of a campaign to achieve air and sea superiority. China is improving information and operational security to protect its own information structures, and is also developing electronic and information warfare capabilities, including denial and deception, to defeat those of its adversaries. China's "information blockade" likely envisions employment of military and non-military instruments of state power across the battlespace, including in cyberspace and outer space. China's investments in advanced electronic warfare systems, counterspace weapons, and computer network operations, combined with more traditional forms of control historically associated with the PLA and CCP systems, such as propaganda, deception, and denial through opacity, reflect the emphasis and

priority China's leaders place on building capability for information advantage.

In more traditional domains, China's A2AD focus appears oriented toward restricting or controlling access to the land, sea, and air spaces along China's periphery, including the western Pacific. For example, China's current and projected force structure improvements will provide the PLA with systems that can engage adversary surface ships up to 1,850 km from the PRC coast. These include:

- Anti-Ship Ballistic Missiles: Medium Range Ballistic Missiles (MRBMs) designed to target forces at sea, combined with overhead and over-the-horizon targeting systems to locate and track moving ships.
- Conventional and nuclear-powered attack submarines: KILO, SONG, YUAN, and SHANG-class attack submarines capable of firing advanced ASCMs.
- Surface combatants: LUZHOU, LUYANG I/II, SOVREMENNY-II-class

guided missile destroyers with advanced long-range anti-air and anti-ship missiles.

- Maritime Strike Aircraft: FB-7 and FB-7A, B-6G, and the SU-30 MK2, armed with ASCMs to engage surface combatants.

Similarly, current and projected systems such as the J-20 stealth fighter and longer-range conventional ballistic missiles could improve the PLA's ability to strike regional air bases, logistical facilities, and other ground-based infrastructure. PRC military analysts have concluded that logistics and power projection are potential vulnerabilities in modern warfare, given the requirements for precision in coordinating transportation, communications, and logistics networks. China is fielding an array of conventionally armed ballistic missiles, modern aircraft, UAVs, ground- and air-launched land-attack cruise missiles, special operations forces, and cyber-warfare capabilities to hold targets at risk throughout the region.

### **Building Capacity for Conventional Precision Strike**

**Short-Range Ballistic Missiles (< 1,000 km).** As of December 2010, the PLA had somewhere between 1,000-1,200 SRBMs. The total number of SRBMs represents little to no change over the past year. However, the PLA continues to field advanced variants with improved ranges and more sophisticated payloads that are gradually replacing earlier generations that do not possess true “precision strike” capability.

**Medium-Range Ballistic Missiles (1,000-3,000 km).** The PLA is acquiring and fielding conventional MRBMs to increase the range at which it can conduct precision strikes against land targets and naval ships, including aircraft carriers, operating far from China’s shores out to the first island chain.

**Land-Attack Cruise Missiles.** The PLA continues to field air- and ground-launched LACMs, such as the YJ-63, KD-88, and DH-10 systems for stand-off, precision strikes.

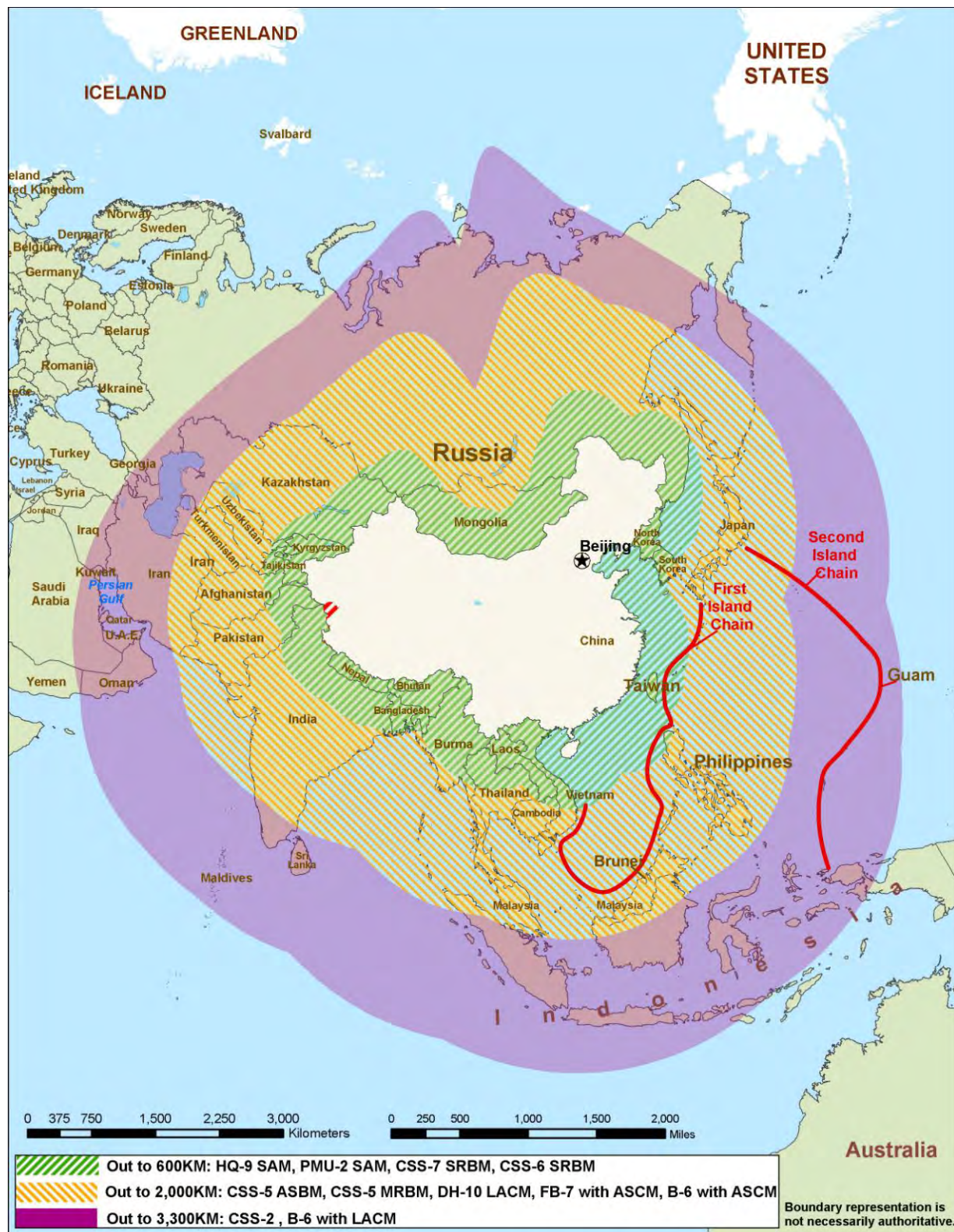
**Ground Attack Munitions.** The PLA Air Force has a small number of tactical air-to-surface missiles as well as precision-guided munitions including all-weather, satellite-guided bombs, anti-radiation missiles, and laser-guided bombs.

**Anti-Ship Cruise Missiles.** The PLA Navy has or is acquiring nearly a dozen ASCM variants, ranging from the 1950s-era CSS-N-2 to the modern Russian-made SS-N-22 and SS-N-27B. The pace of ASCM research, development, and production within China has accelerated over the past decade.

**Anti-Radiation Weapons.** The PLA imported Israeli-made HARPY unmanned combat aerial vehicles (UCAVs) during the 1990s and Russian-made anti-radiation missiles. China continues development of an indigenous version of the Russian Kh-31P (AS-17) known as the YJ-91 and is starting to integrate this system into its fighter-bomber force.

**Artillery-Delivered High Precision Munitions.** The PLA is developing or deploying artillery systems with the range to strike targets within or even across the Taiwan Strait, including the PHL-03 300 mm multiple-rocket launcher (MRL) (100+ km range) and the WS-2 400 mm MRL (200 km range).





**Conventional Anti-Access Capabilities.** *The PLA's conventional forces are currently capable of striking targets well beyond China's immediate periphery. Not included are ranges for naval surface- and sub-surface-based weapons, whose employment at distances from China would be determined by doctrine and the scenario in which they are employed.*

The air and air defense component of China's regional strategy includes long-range, advanced SAMs, such as the Russian SA-10 and SA-20 PMU1/PMU2, as well as the indigenous HQ-9. Beijing will also use Russian-built and domestically produced fourth-generation aircraft (e.g., Su-27/F-11 and Su-30 variants) as well as the indigenous F-10 to compete for local air dominance. The PLA Navy would employ Russian Su-30MK2 fighters, armed with AS-17/Kh-31A anti-ship missiles, B-6G bombers, and FB-7 fighter-bombers for maritime interdiction. Additionally, acquisition and development of longer-range UAVs and UCAVs will expand China's options for long-range reconnaissance and strike.

In January 2011, initial images of China's 5<sup>th</sup> generation J-20 stealth fighter were posted on the Internet. Although the appearance of this prototype underscores the level of PRC investment in advanced defense systems, the Defense Department does not expect the J-20 to achieve an effective operational capability prior to 2018. China faces several hurdles as it moves toward J-20 production, including the mastery of high performance jet engine production.

## **BALLISTIC MISSILE DEFENSE**

China's existing long-range advanced SAM inventory offers limited capability against ballistic missiles, but advertises a capability against cruise missiles. The SA-10 was originally designed to counter low-flying cruise missiles, a capability enhanced in the later model SA-20 systems. The SA-20 PMU2, the most advanced SAM Russia offers for export, also has the advertised capability to engage ballistic missiles with ranges of 1000km and speeds of 2,800 m/s.

China's HQ-9 long-range SAM system is also advertised (through its export variant FD-2000) to protect against low-altitude cruise missiles and is expected to have a limited capability to provide point defense against tactical ballistic missiles with ranges up to

500 km. China is proceeding with the research and development of a missile defense "umbrella" consisting of kinetic energy intercept at exo-atmospheric altitudes (>80 km), as well as intercepts of ballistic missiles and other aerospace vehicles within the upper atmosphere. In January 2010, China successfully intercepted a ballistic missile at mid-course, using a ground-based missile.

## **EXTENDED OPERATIONAL REACH**

In addition to preparing for a Taiwan contingency, the PLA has been developing new platforms and capabilities that will extend its operational reach to address other concerns within the East and South China Seas, and possibly to the Indian Ocean and beyond the second island chain in the western Pacific.

In describing the modernization tasks for each of the service arms, China's Defense White Papers in 2008 and 2010 emphasized mobility and operations at greater distances from China's mainland. The main avenues for the PLA to realize these capabilities are through its naval, ballistic missile, and air forces.

**The PLA Navy:** The PLA Navy is at the forefront of efforts to extend operational reach beyond China's regional waters. China's 2010 Defense White paper asserts that "recent emergency rescue and disaster relief operations, counter-terrorism exercises, and... training [demonstrate]... a notable improvement in the PLA's capabilities of equipment support in long-distance and trans-regional maneuvers, escort operations in distant waters, and complex battlefield environments."

The PLA Navy has demonstrated the capability to conduct limited deployments of modern surface platforms outside the second island chain, including nine separate deployments to the Gulf of Aden to support sustained counter-piracy operations from 2009 through mid 2011. The PLA Navy also has acquired new classes of ships to support



conventional military operations as well as humanitarian assistance and disaster relief missions, including the Type 071 amphibious transport dock and the hospital ship, which the Chinese call the “Peace Ark.”

The PLA Navy’s investment in platforms such as nuclear-powered submarines and its first aircraft carrier suggest China is seeking to support additional military missions beyond a Taiwan contingency.

China has invested in several civilian port projects throughout Asia and along the Indian Ocean. Although such investments may improve peacetime logistical support options for the PLA Navy, not to mention enhancing PRC soft power in the region, they are not a substitute for military bases. Without overseas military bases, China will be constrained in its ability to project and sustain power beyond the immediate region. A decision in Beijing to abandon its longstanding and self-imposed policy against overseas basing would signal that China seeks a greater blue water combat capability.

**Second Artillery Corps:** As detailed elsewhere in this report, China’s ballistic missile force is acquiring conventional medium-range and intermediate-range ballistic missiles, extending the distance from which it can threaten other countries with conventional precision or near-precision strikes.

**The PLA Air Force:** The PLA Air Force is developing longer-range versions of the B-6/BADGER bomber that, when equipped with a long-range land-attack cruise missile, will enable strikes as far as the second island chain. The J-20 will eventually give the PLA Air Force a platform capable of long range, penetrating strikes into complex air defense environments.

During the Shanghai Cooperation Organization’s Peace Mission exercise in September 2010, PLA Air Force B-6s conducted long-range bombing missions in Kazakhstan while operating out of Urumqi in western China. The PLA Air Force reached

another milestone in out-of-area operations in 2010 by deploying Su-27 fighter aircraft to Turkey for joint exercises. Although the PLA Air Force has encountered some difficulty in expanding its fleet of long-range heavy transport aircraft, it marked a new milestone in February 2011, when it employed four IL-76 long-haul transport aircraft to assist with evacuating Chinese citizens from Libya. This mission marked the PLA Air Force’s first overseas deployment to evacuate PRC citizens.

**PLA Ground Force.** Although the PLA’s large ground force has not experienced the same dramatic modernization as other branches of the PLA, it has steadily improved capabilities in certain areas. Much, but not all, of this effort has focused on units garrisoned nearest Taiwan. For example, a new amphibious assault vehicle has entered service in key units, improving the PLA’s capability to conduct amphibious attacks. Throughout the PLA, small numbers of modern main battle tanks, armored vehicles, self-propelled artillery, and air defense weapons have entered service in selected units. Concurrent with this modernization, PLA ground force training has begun to emphasize combined arms operations and long-range mobility.

## STRATEGIC CAPABILITIES

China has made steady progress in recent years to develop offensive nuclear, space, and cyber warfare capabilities—the only aspects of China’s armed forces that are currently global in nature. In the case of cyber and space weapons, however, there is little evidence that China’s military and civilian leaders have fully thought through the global and systemic effects that would be associated with the employment of these strategic capabilities. Additionally, China is both qualitatively and quantitatively improving its strategic missile forces.



**Nuclear Forces.** China's nuclear arsenal currently consists of approximately 55-65 intercontinental ballistic missiles (ICBMs), including the silo-based CSS-4 (DF-5); the solid-fueled, road-mobile CSS-10 Mods 1 and 2 (DF-31 and DF-31A); and the more limited range CSS-3 (DF-3). This force is complemented by liquid-fueled CSS-2 intermediate-range ballistic missiles and road-mobile, solid-fueled CSS-5 (DF-21D) MRBMs for regional deterrence missions. The operational status of China's single XIA-class ballistic missile submarine (SSBN) and medium-range JL-1 submarine-launched ballistic missiles (SLBM) remain questionable.

By 2015, China's nuclear forces will include additional CSS-10 Mod 2s and enhanced CSS-4s. The first of the new JIN-class (Type 094) SSBN appears ready, but the associated JL-2 SLBM has faced a number of problems and will likely continue flight tests. The date when the JIN-class SSBN/JL-2 SLBM combination will be fully operational is uncertain.

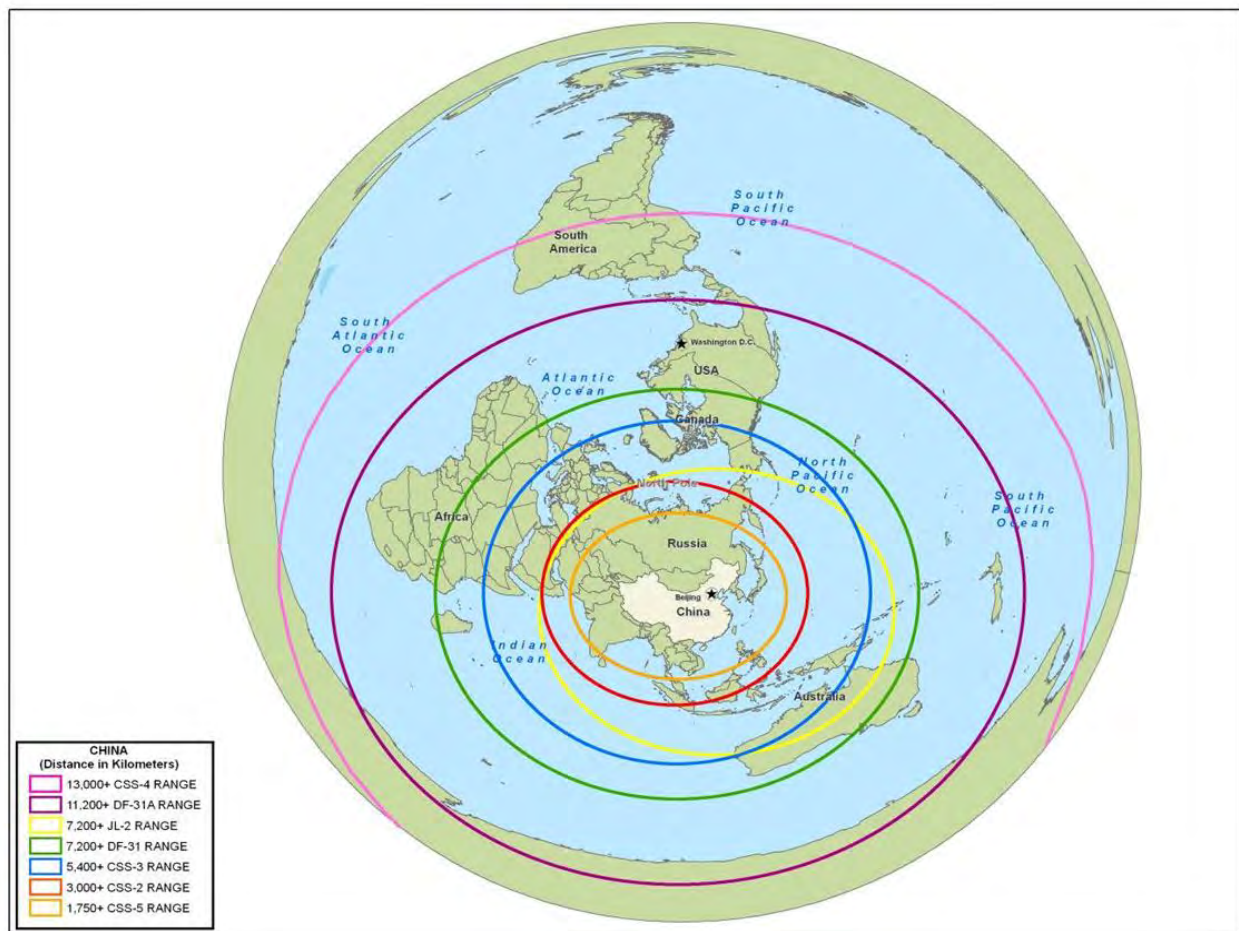
China is also currently working on a range of technologies to attempt to counter U.S. and other countries' ballistic missile defense systems, including maneuvering re-entry vehicles, MIRVs, decoys, chaff, jamming, thermal shielding, and anti-satellite (ASAT) weapons. PRC official media also cites numerous Second Artillery Corps training exercises featuring maneuver, camouflage, and launch operations under simulated combat conditions, which are intended to increase survivability. Together with the increased mobility and survivability of the new generation of missiles, these technologies and training enhancements strengthen China's nuclear force and enhance its strategic strike capabilities.

The introduction of more mobile systems will create new command and control challenges for China's leadership, which now confronts a different set of variables related to deployment and release authorities. For example, the PLA has only a limited capacity

to communicate with submarines at sea, and the PLA Navy has no experience in managing a SSBN fleet that performs strategic patrols with live nuclear warheads mated to missiles. Land-based mobile missiles may face similar command and control challenges in wartime, although probably not as extreme as with submarines.

Beijing's official policy towards the role of nuclear weapons continues to focus on maintaining a nuclear force structure able to survive an attack, and respond with sufficient strength to inflict unacceptable damage on the enemy. The new generation of mobile missiles, maneuvering and MIRV warheads, and penetration aids are intended to ensure the viability of China's strategic deterrent in the face of continued advances in U.S. and, to a lesser extent, Russian strategic intelligence, surveillance, and reconnaissance; precision strike; and missile defense capabilities.

Beijing has consistently asserted that it adheres to a ~~no~~ "no first use" (NFU) policy, stating it would use nuclear forces only in response to a nuclear strike against China. China's NFU pledge consists of two stated commitments: China will never use nuclear weapons first against any nuclear-weapon state, and China will never use or threaten to use nuclear weapons against any non-nuclear-weapon state or nuclear-weapon-free zone. However, there is some ambiguity over the conditions under which China's NFU policy would apply, including whether strikes on what China considers its own territory, demonstration strikes, or high altitude bursts would constitute a first use. Moreover, some PLA officers have written publicly of the need to spell out conditions under which China might need to use nuclear weapons first; for example, if an enemy's conventional attack threatened the survival of China's nuclear force, or of the regime itself. However, there has been no indication that national leaders are willing to attach such nuances and caveats to China's ~~no~~ "no first use" doctrine.



**Medium and Intercontinental Range Ballistic Missiles.** China is capable of targeting its nuclear forces throughout the region and most of the world, including the continental United States. Newer systems, such as the DF-31, DF-31A, and JL-2, will give China a more survivable nuclear force.

Beijing will likely continue to invest considerable resources to maintain a limited nuclear force, also referred to by some PRC writers as “sufficient and effective,” to ensure the PLA can deliver a damaging retaliatory nuclear strike.

**Space and Counterspace.** China’s space activities and capabilities, including ASAT programs, have significant implications for anti-access/area denial efforts in Taiwan Strait contingencies and beyond.

**Reconnaissance:** China is deploying imagery, reconnaissance, and Earth resource systems with military utility. Examples include the Yaogan satellites, the Haiyang-1B, and the Huanjing disaster/environmental monitoring satellite constellation. China is planning eight satellites in the Huanjing program that are capable of visible, infrared, multi-spectral,

and synthetic aperture radar imaging. In the next decade, even as Beijing fields a larger and more capable array of reconnaissance satellites, it probably will continue to employ commercial satellite imagery to supplement its coverage. China currently accesses high-resolution, commercial electro-optical and synthetic aperture radar imagery from all of the major providers including Spot Image (Europe), Infoterra (Europe), MDA (Canada), Antrix (India), GeoEye (United States), and Digital Globe (United States).

**Manned Space:** China’s most recent manned mission, Shenzhou-7, concluded in September 2008. Shenzhou-7 included China’s first spacewalk as well as the launch and rendezvous with an autonomous microsatellite. China will continue its manned space program, including both manned and unmanned docking, with the

goals of establishing a permanently manned space station by 2020 and landing a human on the moon by 2030.

**Position, Navigation, and Timing (PNT):** Since the 1990s, China has used the U.S. Global Positioning System (GPS) for a wide variety of military, civil, and commercial applications. Building on this foundation, China is pursuing several avenues to reduce its dependence on GPS and become a major supplier of PNT services and user equipment. Currently, the PRC is increasing its use of Russia's GLONASS, deploying its own BeiDou-2 (Compass) system as well as a second independent satellite system called CAPS, while augmenting these overhead systems with a variety of ground-based signals.

The experimental BeiDou-1 system consisted of just three satellites, providing both civil and military services to China. China is replacing BeiDou-1 with the much larger

BeiDou-2 constellation, intended to eventually provide a worldwide PNT service, independent of foreign control. By 2012, the BeiDou 2 constellation is expected to provide regional services with approximately 10 satellites. The PRC plans to complete the BeiDou-2 system by 2020, with 35 a satellite constellation offering global coverage.

**Communications:** China uses communications satellites for both regional and international telecommunications in support of civil and military users, including satellite television, Internet, and telephony. China also maintains a single data-relay satellite launched in mid-2008, the TianLian-1. China has recently entered the world market by exporting satellites and infrastructure to Venezuela and Nigeria. Although the satellite built and launched for Nigeria failed, China continues to market its services worldwide, to customers such as Pakistan, Bolivia, Laos, and Vietnam.

### PLA Underground Facilities

Since the early 1950s, the PLA has employed underground facilities (UGFs) to protect and conceal its vital assets. China's strategic missile force, the Second Artillery Corps (SAC), has developed and utilized UGFs since deploying its oldest liquid-fueled missile systems and continues to utilize them to protect and conceal their newest and most modern solid-fueled mobile missiles. As early as the mid 1990's Chinese media vaguely acknowledged the existence of UGFs that support the SAC. Since December 2009, several PRC and foreign media reports offered additional insight into this obscure tunnel network, which reportedly stretches for over 5,000 km.

Given China's nuclear policy of "no first use" and until recently its limited ballistic missile early warning capability, Beijing had assumed it might have to absorb an initial nuclear blow prior to engaging in "nuclear counterattack." Nuclear survivability was particularly critical given China's relatively small number of nuclear weapons and the development by potential adversaries of modern, precision munitions. In recent years, advanced construction design has allowed militaries to go deeper underground to complicate adversarial targeting.

Although secrecy and ambiguity remain China's predominant approach in the nuclear realm, occasional disclosure of information on some missile-related UGFs is consistent with an effort to send strategic signals on the credibility of its limited nuclear arsenal. These public disclosures include images of tunnels, modern network-based security and control centers, and advanced camouflage measures. Categories of military facilities which make good candidates for UGFs include: command posts; communications sites; storage for important weapons and equipment; and protection for personnel.

**ASAT Weapons:** In January 2007, China successfully tested a direct-ascent ASAT weapon against a PRC weather satellite, demonstrating its ability to attack satellites in low-Earth orbit. China continues to develop and refine this system, which is one component of a multi-dimensional program to limit or prevent the use of space-based assets by potential adversaries during times of crisis or conflict.

In addition to the direct-ascent ASAT program, China is developing other kinetic and directed-energy (e.g., lasers, high-powered microwave, and particle beam weapons) technologies for ASAT missions. Foreign and indigenous systems give China the capability to jam common satellite communications bands and GPS receivers. China's nuclear arsenal has long provided Beijing with an inherent ASAT capability, although a nuclear explosion in space would also damage China's own space assets, along with those of whomever it was trying to target.

Citing the requirements of its manned and lunar space programs, China is improving its ability to track and identify satellites—a prerequisite for effective, precise counterspace operations.

**Information Warfare.** PRC military thinkers have written extensively on information warfare, reflecting a strong conceptual understanding of its methodology and potential utility. For example, a November 2006 Liberation Army Daily commentary outlines:

*[The] mechanism to get the upper hand of the enemy in a war under conditions of informatization finds prominent expression in whether or not we are capable of using various means to obtain information and of ensuring the effective circulation of information; whether or not we are capable of making full use of the permeability, sharable property, and connection of information to realize the organic merging of materials, energy,*

*and information to form a combined fighting strength; [and,] whether or not we are capable of applying effective means to weaken the enemy side's information superiority and lower the operational efficiency of enemy information equipment.*

The PLA is investing in electronic countermeasures, defenses against electronic attack (e.g., electronic and infrared decoys, angle reflectors, and false target generators), and computer network operations (CNO). China's CNO concepts include computer network attack, computer network exploitation, and computer network defense. The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, as well as tactics and measures to protect friendly computer systems and networks. These units include elements of the militia, creating a linkage between PLA network operators and China's civilian information technology professionals. Under the rubric of Integrated Network Electronic Warfare, the PLA seeks to employ both computer network operations and electronic warfare to deny an adversary access to information essential to conduct combat operations.

## **POWER PROJECTION BEYOND TAIWAN**

China continues to invest in military programs designed to improve extended-range operations. Current trends in China's military capabilities could provide China with a force capable of conducting a range of military operations in Asia well beyond Taiwan.

China's political leaders have also charged the PLA with developing capabilities for military operations other than war such as peacekeeping, disaster relief, and counter-terrorism operations. These capabilities hold the potential to make positive contributions in the delivery of international public goods, but also increase Beijing's options for military



coercion to gain diplomatic advantage, advance interests, or resolve disputes in its favor.

Analysis of China's weapons development and deployment patterns suggests Beijing is already looking at contingencies beyond Taiwan as it builds its force. For example, new missile units outfitted with conventional, theater-range missiles at various locations in China could be used in a variety of non-Taiwan contingencies. Given the fact that Taiwan can be reached by land-based aviation, China's aircraft carrier program would offer very limited value in a Taiwan scenario and would require additional naval resources for protection. However, it would enable China to extend its naval air capabilities elsewhere. Airborne Early Warning and Control (AEW&C) and aerial-refueling programs would also facilitate extended air operations. Advanced destroyers and submarines could protect and advance China's maritime interests up to and beyond the second island chain. China's expeditionary forces (three airborne divisions, two amphibious infantry divisions, two marine brigades, and about seven special operations groups) are improving with the introduction of new equipment, better unit-level tactics, and greater coordination of joint operations. Over the long-term, improvements in China's C4ISR, including space-based and over-the-horizon sensors, could enable Beijing to identify, track, and target military activities deep into the western Pacific Ocean.

China's increasing focus on humanitarian assistance and disaster relief (HA/DR) missions will require a unique set of technological developments, including large ships and strategic airlift, to support these missions. Of course, many of these HA/DR capabilities would also enhance the PLA ability to support military operations along and beyond China's borders.

**India.** China deepened its ties with India through increased trade and high-level dialogues in 2010, though border tensions

remained an irritant in the bilateral relationship. Bilateral trade in 2010 reached nearly \$60 billion. The two neighbors have held several rounds of dialogue over disputed territorial claims. Sino-Indian defense ties were institutionalized in 2007 with the establishment of an Annual Defense Dialogue. Though India cancelled high-level military exchanges following China's denial of a visa to a senior Indian general in 2010, both sides agreed to resume exchanges in April 2011. During his December 2010 trip to New Delhi, Premier Wen Jiabao attempted to smooth over differences following a year of uneasy relations, but he did not address serious irritants. A high degree of mistrust continues to strain the bilateral relationship. To strengthen its deterrent posture relative to India, the PLA has replaced liquid-fueled, nuclear-capable CSS-2 IRBMs with more advanced and survivable solid-fueled CSS-5 MRBM systems. China is also investing in road development along the Sino-Indian border. Although this construction is primarily aimed at facilitating economic development in western China, improved roads could also support PLA border defense operations. India is also improving infrastructure along its northeastern border. New Delhi remains concerned by China's close military relationship with Pakistan and Beijing's growing footprint in the Indian Ocean, Central Asia, and Africa.

**Russia.** Beijing continues to view Moscow as a useful international partner. Despite awareness that some Russian interests are not consistent with those of China, Moscow and Beijing share many overlapping interests, and China benefits greatly from a more stable and peaceful northern border. Sino-Russia bilateral cooperation continues on a range of international issues, especially in Central Asia where the two jointly manage the Shanghai Cooperation Organization (SCO).

Despite this cooperation, Russia has concerns about China's rise, while PLA strategists continue to regard Russia as a potential long-term security challenge. China shifted its



strategic orientation to the south and east following the collapse of the Soviet Union, but Beijing retains significant force structure in the Lanzhou, Beijing, and Shenyang Military Regions, in addition to its conventional and strategic missile forces, to maintain deterrence.

**Central Asia.** China has several important interests in Central Asia. Most notably, China is interested in acquiring energy and natural resources. Beijing has pursued multiple agreements with energy-rich Central Asian states. This includes a pipeline deal that will extend from Turkmenistan through Uzbekistan and Kazakhstan into China.

Beijing is also interested in Central Asia from a domestic security perspective. From the domestic security standpoint, Beijing hopes to undermine support for China's Uighur separatists, who share religious, ethnic, and linguistic connections to groups in Central Asia. Beijing believes that Islamic radicalism and competing political ideologies could destabilize an already fragile security situation in Western China.

China has used the multilateral Shanghai Cooperation Organization, which it co-founded, to address border security, counter-terrorism, and regional security. Beijing has also conducted bilateral and multilateral exercises with SCO member states to enhance China's regional influence and build cohesive opposition to Uighur activities.

**South China Sea.** Before the CCP took power in 1949, the Chinese government regarded the South China Sea as a region of geostrategic interest and a part of China's "historical waters." As early as the 1930's, the Republic of China was considering a broad line delineating the South China Sea as Chinese territory. The "U-shaped" dashed line that began appearing on Chinese maps in 1947 continues to define PRC claims to the South China Sea. Until recently, however, the PLA Navy's limited operational reach constrained Beijing's military options in the South China Sea.

Over the past five years, China has begun demonstrating a more routine naval and civilian enforcement presence in the South China Sea. In several instances, particularly in 2009, China's use of force and coercion to push its disputed maritime territorial claims elicited concern among many of its Asian neighbors.

Although the PRC remains wary of triggering regional opposition and may have adjusted certain tactics, Beijing appears eager to strengthen its claim to the disputed region over the long-term. This includes legal efforts as well as the deployment of more capable naval and civilian law enforcement ships. A more robust presence would position China for force projection, blockade, and surveillance operations to influence the critical sea lanes in the region, through which some 50 percent of global merchant traffic passes.

Competition for resources, including oil, gas, and fishing rights, coupled with strong nationalistic sentiments continues to drive territorial disputes among several South China Sea claimants. Although tensions in this hotly disputed region subsided after the-1990s, signs of friction re-emerged in 2007, particularly between China and Vietnam.

In response to the 2004 articulation of the PLA's "New Historic Missions," China's senior military leaders began developing concepts for an expanded regional maritime strategy and presence. For example, in 2006, PLA Navy Commander Wu Shengli called for a "powerful navy to protect fishing, resource development and strategic passageways for energy." Many of these ideas echo the debates in the late 1980s and early 1990s over building PLA naval capabilities. However, the rise of Taiwan contingency planning as the dominant driver of PLA force modernization in the mid-1990s, and especially after 2001, largely sidelined these discussions. The 2008 and 2010 Defense White Papers reflect greater attention to the PLA's expanding mission set.

As part of its military modernization effort, China has increasingly shifted resources away from the PLAN's North Sea Fleet to the South Sea Fleet, greatly expanding the latter's

capabilities. China's ability to deploy a more robust strategic and conventional military presence off its southern coast is having a growing impact on regional rivalries and power dynamics.

## CHAPTER FOUR: RESOURCES FOR FORCE MODERNIZATION

---

### OVERVIEW

The PLA has decreased reliance on foreign weapons acquisitions as China's defense-industrial and research bases mature. However, the PLA still looks to foreign assistance to fill some critical near-term capability gaps. China continues to leverage foreign investments, commercial joint ventures, academic exchanges, the experience of repatriated PRC students and researchers, and state-sponsored industrial/technical espionage to increase the level of technologies and expertise available to support military research, development, and acquisition. Beijing's long-term goal is to create a wholly indigenous defense industrial sector, augmented by a strong commercial sector, to meet the needs of PLA modernization and to compete as a top-tier producer in the global arms market. China's leaders can draw from diverse sources to support PLA modernization, including: domestic defense investments, indigenous defense industrial development, a growing research and development and science and technology base, dual-use technologies, and foreign technology acquisition.

### MILITARY EXPENDITURE TRENDS

On March 4, 2011, Beijing announced a 12.7 percent increase in its military budget to approximately \$91.5 billion. This increase continues more than two decades of sustained annual increases in China's announced military budget. Analysis of 2000-2010 data indicates China's officially disclosed military budget grew at an average of 12.1 percent in inflation-adjusted terms over the period. Although the military budget increases are slightly larger than the percentage increases of its overall economic growth of 10.2 percent over the same period, the actual change in the implied burden of the official defense budget on the economy appears negligible.

### *Estimating China's Actual Military Expenditures.*

The Department of Defense estimates China's total military-related spending for 2010 was over \$160 billion, using 2010 prices and exchange rates.

Estimating actual PLA military expenditures is a difficult process due to the lack of accounting transparency and China's still incomplete transition from a command economy. Moreover, China's published military budget does not include major categories of expenditure, such as foreign procurement. China's legislature has not made public any details of the role, if any, that it plays in exercising oversight of the PLA budget. However, public calls within China for greater budget transparency, generally in response to sustained and systemic official corruption, suggest that improvement in government transparency as a whole could develop over time.

The United States and other countries continue to urge China to increase transparency in military spending. In August 2010, China submitted a report on its military expenditures to the UN Secretary General, the third such report in as many years. China's report was submitted in the UN Simplified Reporting Form, which provides minimal information on major budget categories, in contrast to the more detailed Standardized Reporting Form used by countries practicing greater defense transparency.

### CHINA'S ADVANCING DEFENSE INDUSTRIES

Since the late 1990s, China's state-owned defense and defense-related companies have undergone a broad-based transformation. Beijing continues to improve its business

practices, streamline bureaucracy, broaden incentives for its factory workers, shorten developmental timelines, improve quality control, and increase overall defense industrial production capacity. Beijing is also emphasizing integration of defense and non-defense sectors to leverage the latest dual-use technologies and the output from China's expanding science and technology base. Augmented in part by direct acquisition of foreign weapons and technology, these reforms have enabled China to incorporate mid-1990s technology into the development and production of most of its advanced weapon systems. Some systems, particularly ballistic missiles, incorporate cutting-edge technologies in a manner that rivals even the world's most modern systems.

**Civil-Military Integration.** Developing innovative dual-use technology and an industrial base that serves both military and civilian needs is a high priority for China's leadership. President Hu expressed in his political report to the CCP's 17th Party Congress in October 2007:

*We must establish sound systems of weapons and equipment research and manufacturing... and combine military efforts with civilian support, build the armed forces through diligence and thrift, and blaze a path of development with Chinese characteristics featuring military and civilian integration.*

China's defense industry has benefited from integration with a rapidly expanding civilian economy and science and technology sector, particularly elements that have access to foreign technology. Progress within individual defense sectors appears linked to the relative integration of each, through China's civilian economy, into the global production and research and development (R&D) chain. For example, the shipbuilding and defense electronics sectors, benefiting from China's leading role in producing commercial shipping and information technologies, have witnessed the greatest progress over the last decade. Information

technology companies in particular, including Huawei, Datang, and Zhongxing, maintain close ties to the PLA.

In contrast, enterprises producing high-performance computers, advanced applications software, and specialized top-end semiconductors/microprocessors—key to the evolution of increasingly advanced and capable defense microelectronics and applications, but with limited counterparts in the PRC civil-industrial sector—have experienced slower progress. The aviation and ordnance sectors have similarly suffered from a limited number of spin-off benefits, despite partnerships between foreign multinational corporations and domestic industry.

**Sector-by-Sector Analysis.** Progress across China's defense industry sectors has been uneven. Production trends and resource allocation appear to favor missile and space systems, followed by maritime assets (both surface and sub-surface), aircraft, and ground force materiel. In all areas, China is increasing the quality of its output and surge production capabilities, if not capacities. However, many of China's most advanced systems are still based heavily on foreign designs copied through reverse engineering, highlighting a persistent weakness in China's capability for overall system design and integration.

**Missile and Space Industry:** China produces a broad range of sophisticated ballistic, cruise, air-to-air, and surface-to-air missiles. Many of China's primary final assembly and rocket motor production facilities have received upgrades over the past few years, likely increasing production capacity. In addition to supplying China's military, complete systems and missile technologies could also be marketed for export. Surge production for these systems could result in a significantly higher output of SRBMs and perhaps double the number of MRBMs per year. China's space launch vehicle industry is expanding to support satellite launch services and the manned space program.

**Shipbuilding Industry:** China operates a vibrant and globally competitive shipbuilding

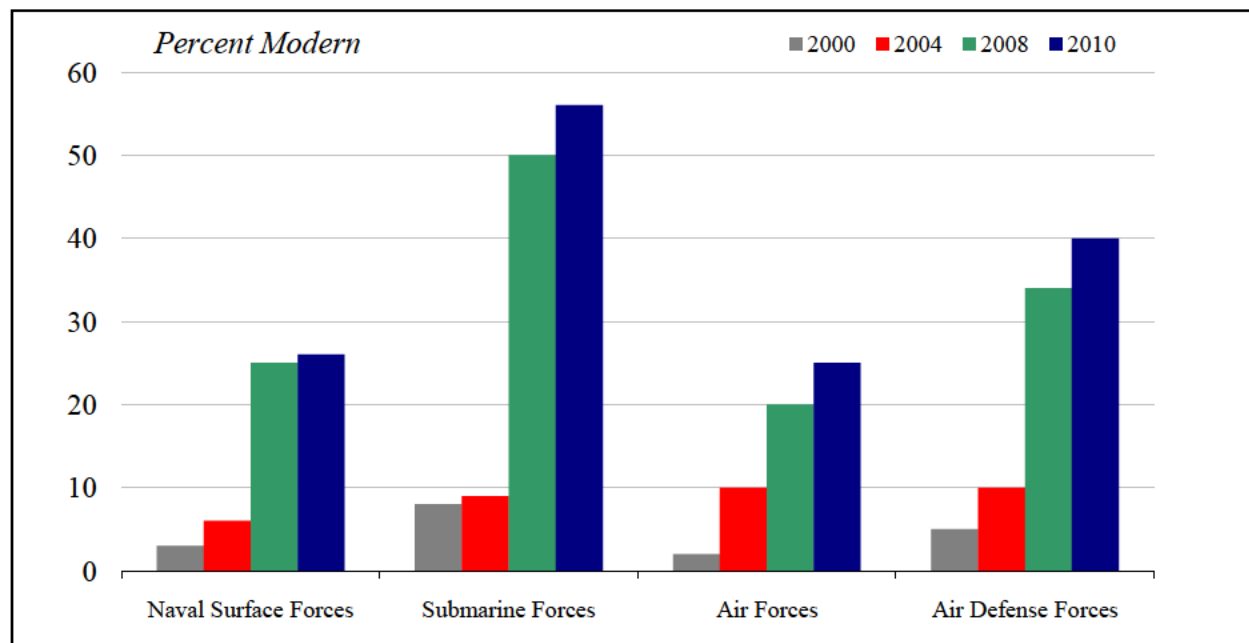
industry. By some measures, China is the largest shipbuilder in the world. Shipyard expansion and modernization have increased China's shipbuilding capacity and capability, generating benefits for all types of military projects, including: submarines; surface combatants; naval aviation, including aircraft carriers; and lift assets. China continues relying on foreign suppliers for some propulsion units and to a much lesser degree, fire control systems, cruise missiles, surface-to-air missiles, torpedo systems, sensors, and other advanced electronics. Modular shipbuilding techniques will allow China to spread production across multiple locations, increasing both efficiency and output. China has already demonstrated an ability to surge submarine and amphibious production.

**Armament Industry:** China's ground force modernization includes production of new tanks, armored personnel carriers, and artillery pieces. There have been advances in almost every area of PLA ground forces with new production capacity to accommodate surge requests. China's reliance on foreign

partners to fill gaps in critical technical capabilities could still limit actual surge output.

**Aviation Industry:** China's commercial and military aviation industries have advanced from producing direct copies of early Soviet models to developing and producing indigenous aircraft. These include improved versions of older aircraft and modern fourth generation fighters. China's commercial aircraft industry has imported high-precision and technologically advanced machine tools, electronics, and other components that can also be used in the production of military aircraft. However, China's ability to surge production in the aircraft industry will be limited by its reliance on foreign sourcing for aircraft engines and avionics, as well as the lack of skilled personnel and facilities.

**Foreign Technology Acquisition.** Key areas where China continues to rely most heavily on foreign technologies include: guidance and control systems, engine technology, and



**PLA Modernization Areas, 2000 – 2010.** This graphic compares the expansion of modern operational systems within the PLA in 2000, 2004, 2008, and 2010.

Footnote: For surface combatants “modern” is defined as multi-mission platforms with significant capabilities in at least two warfare areas. “Modern” for submarines is defined as those platforms capable of firing an anti-ship cruise missile. For air forces, “modern” is defined as 4th generation platforms (Su-27, Su-30, F-10) and platforms with 4th generation-like capabilities (FB-7). “Modern” SAMs are defined as advanced, long-range Russian systems (SA-10, SA-20), and their PRC indigenous equivalents (HQ-9).



enabling technologies such as precision machine tools, advanced diagnostic and forensic equipment, applications and processes essential to rapid prototyping, and computer-assisted design/manufacturing. China often pursues these foreign technologies for the purpose of reverse engineering or to supplement indigenous military modernization efforts.

Russia has been China's primary weapons and materiel provider, selling Beijing advanced fighter aircraft, helicopters, missile systems, submarines, and destroyers. Relying on Russian components for several of its production programs, China purchased production rights to Russian weapon designs. However, this trend is changing as China becomes more self-sufficient in development and production.

Israel previously supplied advanced military technology to China, but has reformed its export control regime through the passage of a Defense Export Control Act in July 2007 and the adoption of implementing regulations in December 2007.

Since 2003, China has pressured European Union (EU) Member States to lift the embargo on lethal military sales to China that the EU imposed in response to China's 1989 crackdown on demonstrators. In their Joint Statement following the 2004 EU-China Summit, European and PRC leaders committed to work towards lifting the Tiananmen embargo. Although the issue remains on the EU agenda, there is no consensus among the EU Member States on lifting the embargo in the near future.

In addition, economic espionage, supported by extensive open source research, computer network exploitation, and targeted intelligence operations also enables China to obtain technologies to supplement indigenous military modernization efforts.

In its 2008 report, *Targeting U.S. Technologies: A Trend Analysis of Reporting From Defense Industry*, the Defense Security Service (DSS) found that in the previous year,

foreign collectors, including the PRC, attempted to obtain information and technologies from each of the 20 categories of the Developing Sciences and Technologies List (DSTL). The DSTL is a compendium of scientific and technological capabilities being developed worldwide that have the potential to enhance or degrade U.S. military capabilities significantly in the future.

The DSS report described China's science and technology collection priorities as: guidance and control systems, advanced energy technologies, nanotechnology, space and counterspace systems, nuclear forces, innovative materials, aeronautics and astronautic mechanisms, computer-aided manufacturing and design, and information technologies. The PRC continues to target these technologies.

The U.S. Department of Commerce's Bureau of Industry and Security and the Department of Justice identified at least 26 major cases since 2006 linking China to the acquisition of technologies and applications cited above, as well as to current and future warship technology, electronic propulsion systems, controlled power amplifiers with military applications, space launch technical data and services, C-17 aircraft, Delta IV rockets, infrared cameras, information related to cruise missile design, and military-grade accelerometers. Additional technologies cited in these cases consisted of microwave integrated circuits; weapon scopes; restricted night-vision equipment and data; satellite/missile thermal insulation blankets; controlled electronic components; traveling wave tubes used with satellite and radar systems; microwave amplifiers with radar applications; export controlled technical data related to plasma technology for UAVs; carbon fiber material for aircraft, rockets, spacecraft, and the uranium enrichment process; and, extended range programmable logic devices.

The PRC's continuing efforts to acquire U.S. military and dual-use technologies are enabling the PRC science and technology

base to diminish the U.S. technological edge in areas critical to the development of military weapons and communications systems. Additionally, the technologies China has acquired could be used to develop more advanced technologies by shortening PRC R&D cycles.

## TRENDS AND PROJECTIONS

China's *National Medium- and Long-Term Program for Science and Technology Development* (2006-2020), issued by the State Council in February 2006, seeks to transform China into an "innovation-oriented society by 2020." The plan defines China's science and technology focus in terms of "basic research," "leading-edge technologies," "key fields and priority subjects," and "major special items," all of which have military applications.

**Basic Research.** As part of a broad effort to expand basic research capabilities, China identified five areas that have military applications as major strategic needs or science research plans requiring active government involvement and funding:

- material design and preparation;
- manufacturing in extreme environmental conditions;
- aeronautic and astronautic mechanics;
- information technology development; and,
- nanotechnology research.

In nanotechnology, China has progressed from virtually no research or funding in 2002 to being a close second to the United States in total government investment.

**Leading-edge Technologies.** China is focusing on the following technologies for rapid development:

- ***Information Technology:*** Priorities include intelligent perception technologies, ad hoc networks, and virtual reality technologies;
- ***New Materials:*** Priorities include smart materials and structures, high-temperature

superconducting technologies, and highly efficient energy materials technologies;

- ***Advanced Manufacturing:*** Priorities include extreme manufacturing technologies and intelligent service advanced machine tools;
- ***Advanced Energy Technologies:*** Priorities include hydrogen energy and fuel cell technologies, alternative fuels, and advanced vehicle technologies;
- ***Marine Technologies:*** Priorities include three-dimensional maritime environmental monitoring technologies, fast, multi-parameter ocean floor survey technologies, and deep-sea operations technologies; and,
- ***Laser and Aerospace Technologies*** are also high priorities.

**Key Fields and Priority Subjects.** China has identified certain industries and technology groups with potential to provide technological breakthroughs, remove technical obstacles across industries, and improve international competitiveness. Specifically, China's defense industries are pursuing advanced manufacturing, information technology, and defense technologies. Examples include radar, counterspace capabilities, secure C4ISR, smart materials, and low-observable technologies.

**Major Special Items.** China has also identified 16 "major special items" for which it plans to develop or expand indigenous capabilities. These include core electronic components, high-end universal chips and operating system software, very large-scale integrated circuit manufacturing, next-generation broadband wireless mobile communications, high-grade numerically controlled machine tools, large aircraft, high-resolution satellites, manned spaceflight, and lunar exploration.

### **Status of Aircraft Carrier Developments**

During the next decade China is likely to fulfill its carrier ambitions, becoming the last permanent member of the UN Security Council to obtain a carrier capability. In April 2011, China's Xinhua state news agency posted the newspaper's first pictures of the former Soviet carrier (Kuznetsov-class Hull-2) under renovation in Dalian, proclaiming that China will soon fulfill its 70-year aircraft carrier dreams." In June 2011, PLA Chief of the General Staff, Chen Bingde, finally confirmed China's carrier program.

Throughout 2010, the PRC continued refurbishing Kuznetsov Hull-2 (the ex-VARYAG), which China purchased from Ukraine in 1998. This carrier will likely begin sea trials in 2011, and the ship could become operationally available, although without aircraft, by the end of 2012. However, it will take several years for an operationally viable air group of fixed and rotary wing aircraft to achieve even a minimal level of combat capability. The PLA Navy has initiated a land-based program to begin training navy pilots to operate fixed-wing aircraft from an aircraft carrier. This program will probably be followed in about three years by full-scale ship-borne training aboard Kuznetsov Hull-2.

China has demonstrated an interest in foreign carrier-borne fighters and carrier aviation, but it appears that a domestic carrier aircraft production program is progressing. Currently in flight testing, the carrier aircraft, known as the J-15, is reportedly an unlicensed copy of a Russian Su-33, which China obtained from Ukraine in 2004. China is also looking abroad for operational expertise. In May 2009, Brazilian Defense Minister Nelson Jobim announced that the Brazilian Navy would provide training to PLA Navy officers in aircraft carrier operations. However, Brazil's limited capabilities in this area and the extensive problems associated with Brazil's own carrier program raise some questions as to the implications of the offer.

In addition to the Kuznetsov-class carrier, the PLA Navy will likely build several additional carriers in Chinese shipyards. In March 2009, PLA Navy Admiral Wu Huayang affirmed, "China is capable of building aircraft carriers... Given the level of development in our country, I think we have such strength." Construction of China's first indigenous carrier, which would likely have a similar displacement and design of the Kuznetsov Hull-2, could begin as early as 2011. If China commences construction in 2011, the PLA Navy could have its first indigenous carrier achieving operational capability as early as 2015.

## CHAPTER FIVE: FORCE MODERNIZATION AND SECURITY IN THE TAIWAN STRAIT

---

### OVERVIEW

China's acute focus on Taiwan has served for two decades as the dominant force shaping PLA modernization. Although China's other emerging interests increasingly compete for attention and resources, defense planners continue to regard Taiwan as the PLA's primary mission. Beijing seeks the military capability to deter Taiwan moves toward independence. This mission has catalyzed efforts to deter, delay, or deny the possible intervention of U.S. forces in a cross-Strait conflict. Although cross-Strait ties have improved steadily since 2008 and the prospect of a near-term crisis appears low, the PRC remains focused on developing the prerequisite military capabilities to eventually settle the dispute on Beijing's terms.

Since the election of Taiwan President Ma Ying-jeou in March 2008, China and Taiwan have embarked on a period of improved economic and political ties. The two sides have expanded trade and economic links, such as direct shipping, flights, and mail across the Strait. The United States welcomes and encourages this trend as a means to reduce tensions and bridge differences between the two sides. Nevertheless, there is no indication that China's long-term objectives have changed.

In October 2010, senior PRC officials indicated that the two sides were in no rush to address thorny political or military issues, but would focus on improving economic cooperation. Consistent with that statement, the PRC has not taken steps to reduce its military forces facing Taiwan. China has continued to develop a wide range of weapons and capabilities designed to provide credible military options in a Taiwan contingency. This includes efforts to deter or limit the effectiveness of potential U.S. intervention.

Security in the Taiwan Strait is largely a function of dynamic interactions between and among mainland China, Taiwan, and the United States. Although the PLA probably lacks the necessary military power to successfully conduct a full-scale amphibious invasion of Taiwan, it is working to close perceived capability gaps in the coming years. Furthermore, Taiwan's relatively modest defense spending has failed to keep pace with ambitious military developments on the mainland.

Taiwan has historically relied upon multiple factors to deter PLA aggression: the PLA's inability to project sufficient power across the 185 km Taiwan Strait; the Taiwan military's technological superiority; the inherent geographic advantages of island defense; and the possibility of U.S. intervention. China's increasingly modern weapons and platforms (over a thousand ballistic missiles, an anti-ship ballistic missile program, increasingly modern ships and submarines, combat aircraft, and improved C4ISR capabilities) threaten to negate many of those factors upon which Taiwan has depended.

Taiwan has taken important steps to build its war reserve stocks, grow its defense industrial base, improve joint operations and crisis response capabilities, and increase its officer and noncommissioned officer (NCO) corps. These improvements have partially addressed Taiwan's eroding defensive advantages. Taiwan released its first Quadrennial Defense Review in March 2009, and is following through on that report by creating an all-volunteer military and reducing its active military end-strength from 275,000 to 215,000 personnel to create a "small but smart and strong force." Under this plan, which is slated for completion by December

2014, the cost savings from a smaller force will free up resources to increase volunteer salaries and benefits. However, the additional personnel costs needed to initially attract and retain personnel under the volunteer system could divert funds from foreign and indigenous acquisition programs, as well as near-term training and readiness.

U.S. policy toward Taiwan is based on our one China policy, based on the three Joint Communiqués and the Taiwan Relations Act [Public Law 96-8 (1979)]. U.S. policy opposes any unilateral changes to the status quo in the Taiwan Strait by either side. The United States continues to support peaceful resolution of cross-Strait differences in a manner acceptable to the people on both sides.

Consistent with the Taiwan Relations Act, the United States has helped to maintain peace, security, and stability in the Taiwan Strait by providing defense articles and services to enable Taiwan to maintain a sufficient self defense capability. To this end, the Obama Administration announced in January 2010 its intent to sell to Taiwan US\$6.4 billion worth of defensive arms and equipment, including:

- UH-60 utility helicopters;
- PATRIOT PAC-3 air and missile defense systems;
- HARPOON anti-ship cruise missile training;
- Multifunctional Information Distribution Systems technical support for Taiwan's *Syun An* C4ISR system; and,
- OSPREY-class minehunting ships.

In addition, the U.S. Department of Defense, through transformation of the U.S. Armed Forces and global force posture realignments, is maintaining the capability and capacity of the United States to defend against Beijing's use of force or coercion against Taiwan.

## BEIJING'S TAIWAN STRATEGY

Through the employment of both “carrots and sticks” Beijing apparently seeks to deter Taiwan moves toward independence and achieve eventual unification. The PRC strives to integrate the two economies while advancing cultural and historic ties. Politically, China has sought to expand ties with the KMT Party on Taiwan while attempting to isolate political entities with more overtly pro-independence leanings. The PRC employs economic enticement, propaganda, and political engagement in pursuit of these objectives.

The military component of China's Taiwan strategy is likely intended to create an impression on Taiwan that accommodation with China is ultimately in the island's best interest. This approach appears to include a heavy focus on amphibious operations, long range strike, and anti-access and area denial capabilities, which are intended to alter Taiwan's threat calculus as well as that of any party considering intervention in a cross-Strait crisis.

Beijing appears prepared to defer the use of force as long as it believes long term reunification remains possible and the costs of conflict outweigh the benefits. Although Beijing often emphasizes its preference for “peaceful unification” under the principle of “one country, two systems,” it has never renounced the possibility of using force to achieve this end. Beijing likely calculates that the prospect of employing military force is an important point of leverage in this relationship.

Historically, the PRC has alluded to several events or conditions that might prompt it to employ military force in pursuit of its Taiwan policy. These conditions have evolved over time in response to political developments on Taiwan, the evolution of PLA capabilities, and Beijing's perception of Taiwan's foreign relations. These circumstances have included:



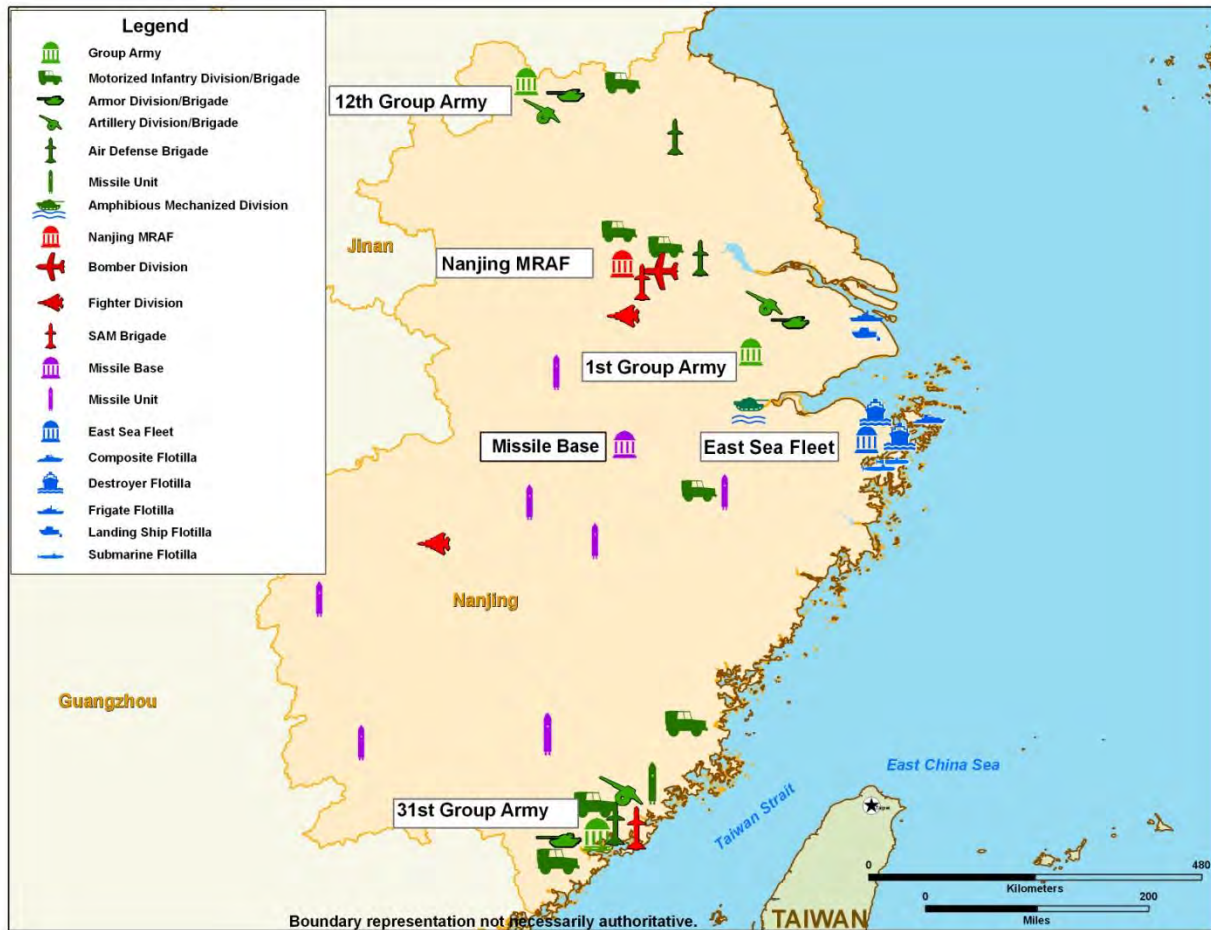
- formal declaration of Taiwan independence;
- undefined moves toward Taiwan independence;
- internal unrest on Taiwan;
- Taiwan's acquisition of nuclear weapons;
- indefinite delays in the resumption of cross-Straits dialogue on unification;
- foreign intervention in Taiwan's internal affairs; and,
- foreign troops stationed on Taiwan.

Article 8 of China's March 2005 "Anti-Secession Law" states that Beijing may use "non-peaceful means" if "secessionist forces... cause the fact of Taiwan's secession from China;" if "major incidents entailing Taiwan's secession" occur; or, if "possibilities for peaceful reunification" are exhausted. The ambiguity of these "redlines" preserves Beijing's flexibility.

## BEIJING'S COURSES OF ACTION AGAINST TAIWAN

The PLA is capable of increasingly sophisticated military action against Taiwan. Should Beijing resolve to employ military force against Taiwan, some analysts assert the PLA would mobilize forces in a manner that optimizes speed of engagement over strategic deception. Others contend that Beijing would sacrifice preparations in favor of tactical surprise, with the goal of forcing rapid military and/or political resolution before other countries could respond. If a quick resolution is not possible, Beijing would seek to:

- deter potential U.S. intervention by highlighting the potential cost to the U.S. and targeting the resolve of the U.S. public and leadership;
- failing that, delay intervention and seek victory in an asymmetric, limited, quick war; or,
- fight to a standstill and pursue a political settlement after a protracted conflict.

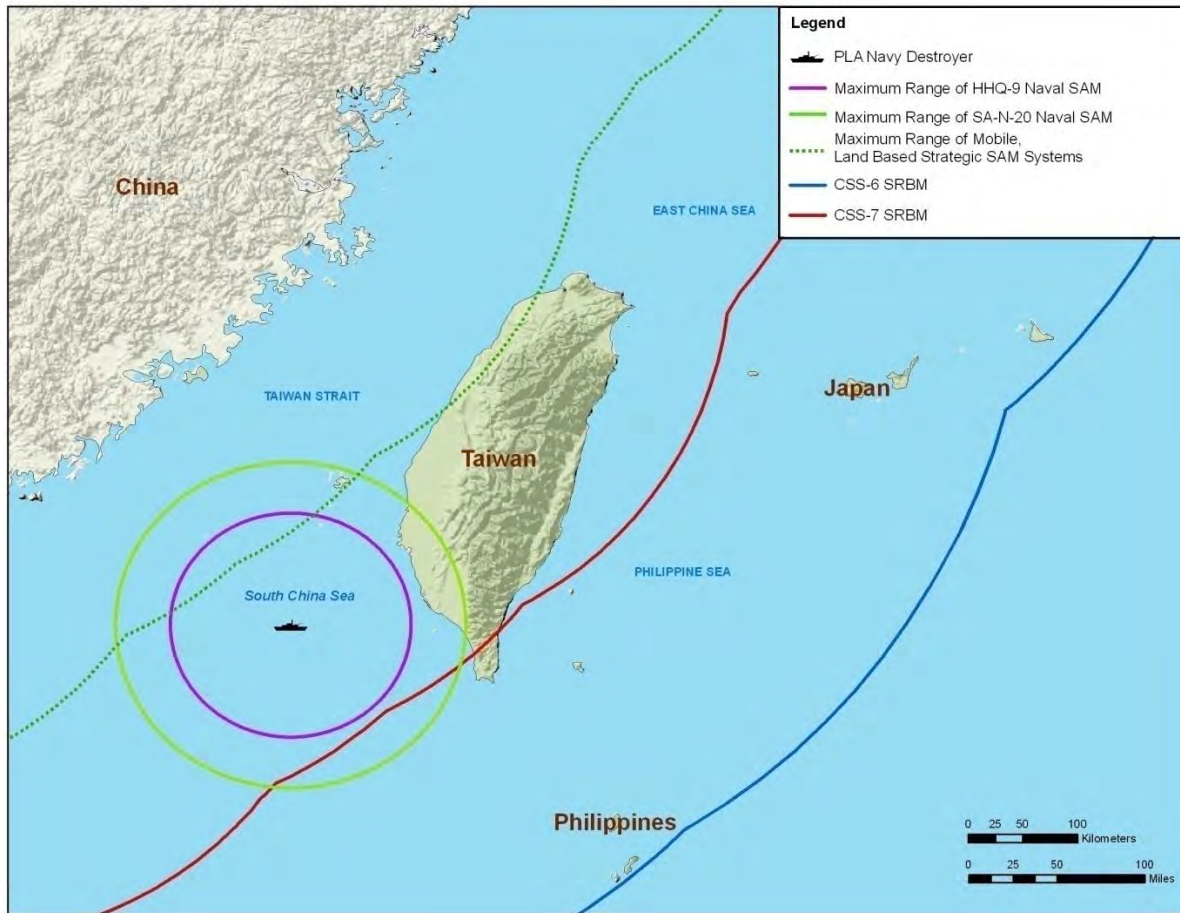


*Disposition of PLA Forces in Nanjing Military Region.*

### **Maritime Quarantine or Blockade.**

Although a traditional maritime quarantine or blockade would have a short-term impact on Taiwan, such an operation would tax PLA Navy capabilities. PRC military writings describe potential alternative solutions including air blockades, missile attacks, and mining to obstruct harbors and approaches. Beijing could declare that ships en route to Taiwan must stop in mainland ports for inspection prior to transiting to Taiwan ports. Beijing could also attempt the equivalent of a blockade by declaring exercise or missile closure areas in approaches to ports, effectively closing port access and diverting

merchant traffic. The PLA employed this method during the 1995-96 missile firings and live-fire exercises. However, there is a risk that Beijing would underestimate the degree to which any attempt to limit maritime traffic to and from Taiwan would trigger countervailing international pressure and military escalation. Currently, China probably could not effectively enforce a full military blockade, particularly in the face of intervention by a major naval power. However, its ability to execute a blockade will improve steadily through 2020.



**Taiwan Strait SAM & SRBM Coverage.** This map depicts notional coverage based on the range of land and sea based missile systems, including advanced SAMs that China would likely employ in a Taiwan conflict. A single PLA Navy Destroyer is used to illustrate the range of sea-based SAM coverage. Actual air defense coverage would be non-contiguous and dependent upon precise deployment sites. If deployed near the Taiwan Strait, the PMU2's extended range provides the PLA's SAM force with an offensive capability against Taiwan aircraft.

**Limited Force or Coercive Options.** Beijing might use a variety of disruptive, punitive, or lethal military actions in a limited campaign against Taiwan, likely in conjunction with overt and clandestine economic and political activities. Such a campaign could include computer network or limited kinetic attacks against Taiwan's political, military, and economic infrastructure to induce fear in Taiwan and degrade the populace's confidence in the Taiwan leadership. Similarly, PLA special operations forces could infiltrate Taiwan and conduct attacks against infrastructure or leadership targets.

**Air and Missile Campaign.** Limited SRBM attacks and precision strikes against air defense systems, including air bases, radar sites, missiles, space assets, and communications facilities, could be conducted in an attempt to degrade Taiwan's defenses, neutralize Taiwan's leadership, or break the public's will to fight.

**Amphibious Invasion.** Publicly available PRC writings describe different operational concepts for amphibious invasion. The most prominent of these, the Joint Island Landing Campaign, envisions a complex operation relying on coordinated, interlocking campaigns for logistics, air and naval support, and electronic warfare. The objective would

be to break through or circumvent shore defenses, establish and build a beachhead, transport personnel and materiel to designated landing sites in the north or south of Taiwan's western coastline, and launch attacks to seize and occupy key targets and/or the entire island.

The PLA is capable of accomplishing various amphibious operations short of a full-scale invasion of Taiwan. With few overt military preparations beyond routine training, China could launch an invasion of small, Taiwan-held islands such as Pratas Reef or Itu Aba. A PLA invasion of a medium-sized, defended, offshore island such as Mazu or Jinmen is within China's capabilities. Such an invasion would demonstrate military capability and political resolve while achieving tangible territorial gain and simultaneously showing some measure of restraint. However, this type of operation involves significant

operational and political risk. It could galvanize the Taiwan populace and catalyze a strong international reaction. Operationally, large-scale amphibious invasion is one of the most complicated military maneuvers. Success depends upon air and sea superiority, rapid buildup and sustainment of supplies on shore, and uninterrupted support. An attempt to invade Taiwan would strain China's untested armed forces and invite international intervention. These stresses, combined with China's combat force attrition and the complexity of urban warfare and counterinsurgency (assuming a successful landing and breakout), make amphibious invasion of Taiwan a significant political and military risk. Taiwan's investments to harden infrastructure and strengthen defensive capabilities could also decrease Beijing's ability to achieve its objectives.



## CHAPTER SIX: U.S.-CHINA MILITARY-TO-MILITARY CONTACTS

---

### OVERVIEW

Over the past two decades, the PRC has steadily transformed a poorly equipped, terrestrially focused military into a more capable force that is assuming diverse missions well beyond China's shores. Given this trajectory, the need for a robust U.S.-China military-to-military relationship that builds trust and helps manage friction continues to grow. During their January 2011 summit, U.S. President Barack Obama and PRC President Hu Jintao jointly affirmed that a "healthy, stable, and reliable military-to-military relationship is an essential part of [their] shared vision for a positive, cooperative, and comprehensive U.S. China relationship." Both sides have repeatedly endorsed this objective. However, placing the military relationship on a firm foundation has proven challenging.

In 2010, the PLA suspended military relations with the United States for a second time since 2008. The suspension on January 30, 2010 came just one day after the U.S. Government approved the sale of an arms package to Taiwan. In response, MG Qian Lihua, Director of the Ministry of Defense Foreign Affairs Office (MND/FAO), noted the PLA "expresses grave indignation and strongly condemns such a move to grossly interfere in China's internal affairs and harm China's national security interests." Although the United States and China maintained working level contact during the nine-month suspension that followed, routine military-to-military exchanges did not resume until the final quarter of 2010.

The fundamental purpose for two countries to conduct military-to-military relations is to gain a better understanding of how each side thinks about the role and use of military power in achieving political and strategic objectives. It is precisely during periods of

tension when a working relationship is most important. Over the long term, a fully functioning relationship should help both parties develop a more acute awareness of the potential for cooperation and competition. Speaking at the Shangri-la Dialogue in June 2010, then-Secretary of Defense Robert Gates asserted that the Defense Department "wants what both Presidents Obama and Hu want: sustained and reliable military-to-military contacts at all levels that can help reduce miscommunication, misunderstanding, and the risks of miscalculation."

The United States bases its contacts and exchanges with China's military on the principles of mutual respect, mutual trust, reciprocity, mutual interest, continuous dialogue, and mutual risk reduction. The Department of Defense conducts them in a manner consistent with the provisions of Section 1201 of the National Defense Authorization Act for Fiscal Year 2000 [Public Law 106-65 (1999)], which provide the Secretary of Defense sufficient latitude to develop a program of exchanges with China that supports U.S. national interests.

### MILITARY RELATIONS IN 2010

In September 2010, after Beijing expressed a desire to resume military-to-military relations, Deputy Assistant Secretary of Defense (DASD) Michael Schiffer met with MG Qian Lihua to lay the groundwork for a series of bilateral military engagements for late 2010 and early 2011.

As a starting point, in mid-October 2010, the U.S. Pacific Command hosted a plenary session of the Military Maritime Consultative Agreement (MMCA) with China's Ministry of National Defense in Honolulu, HI. During the MMCA session, the two sides discussed



issues of maritime safety, including a series of increasingly close PLA intercepts of U.S. aircraft operating in international airspace. On October 17, 2010, Secretary Gates and PRC Minister of National Defense, General Liang Guanglie, met on the sidelines of the ASEAN Defense Ministerial Meeting in Hanoi. General Liang invited Secretary Gates to visit China in early 2011 and agreed to a Chairman of the Joint Chiefs of Staff counterpart visit with PLA Chief of the General Staff, General Chen Bingde.

On December 10, 2010, Under Secretary of Defense for Policy Michèle Flournoy hosted the 11th Defense Consultative Talks (DCT) in Washington, D.C. with Deputy Chief of the PLA General Staff, General Ma Xiaotian. During these talks, the two sides addressed the importance of moving beyond the on-again-off-again cycle that has characterized the relationship. They also discussed potential opportunities to build trust and expand cooperation, including a shared interest in stability on the Korean Peninsula.

Under Secretary Flournoy and General Ma agreed to develop a framework for military-to-military relations based on the seven-point consensus established between then-Secretary Gates and Vice Chairman of the Central Military Commission Xu Caihou in 2009. This meeting also set the stage for Secretary Gates' visit to China and President Hu Jintao's subsequent visit to the United States in January 2011.

The resumption of dialogue in late 2010 enabled the U.S. and PRC militaries to candidly discuss a range of important topics, including North Korea's provocations; concerns related to Iran, Afghanistan, and Pakistan; and transnational and strategic security issues. Continuous dialogue, particularly at high levels, is an important platform for developing common approaches to challenges in the international security environment.

## **U.S. STRATEGY FOR MILITARY ENGAGEMENT**

The complexity of the security environment both in the Asia-Pacific region and globally, calls for a continuous dialogue between the armed forces of the United States and China. The U.S. position is that our engagement with China should expand cooperation in areas of mutual interest, provide a forum to candidly address areas of disagreement and improve mutual understanding. The United States sees value in sustained and reliable military ties and regards the military relationship as an integral component of a comprehensive U.S.-China relationship.

The U.S. Defense Department's plan for military-to-military engagement with the PRC supports the vision of a "positive, cooperative, and comprehensive U.S.-China relationship for the 21<sup>st</sup> century," that the U.S. and PRC presidents jointly endorsed. Sustained military engagement underpins U.S. policy objectives of promoting China's development in a manner consistent with international rules and norms and that contributes to regional and global problem-solving. The U.S. National Defense Strategy emphasizes that U.S. defense interaction with China will be long-term and multi-dimensional. The objective of this effort is to mitigate near term challenges while pursuing and enhancing U.S. national advantage over time.

Our military-to-military engagement with China serves three general purposes in support of the broader relationship. First, it allows the U.S. and PRC militaries to build cooperative capacity. This is achieved through activities that enhance or facilitate our ability to interact at a tactical or operational level. Second, our engagement fosters understanding of each others' military institutions in ways that dispel misconceptions and encourage common ground for dialogue. Third, military engagement allows our senior-most leaders to address the global security environment and

relevant challenges. This interaction can facilitate common approaches to challenges and serves as a bridge to build more productive working relationships.

## **OPPORTUNITIES AND CHALLENGES IN U.S.-CHINA MILITARY-TO- MILITARY RELATIONS**

President Obama reiterated in January 2011 that the United States welcomes a “strong, prosperous, and successful China that plays a greater role in world affairs.” China’s military modernization has created new opportunities for cooperation with the United States, including peacekeeping efforts, humanitarian and disaster relief, and counter-piracy operations. At the same time, the PLA’s development remains a potential source of friction.

The Asia-Pacific region is contending with an array of challenges including rising powers, failing states, proliferation of nuclear and ballistic missiles, extremist violence, and new technologies capable of disrupting critical arteries of global commerce. Secretary Gates has noted that “confronting these tasks is not the task of any one nation acting alone.” China’s growing economic and military capability makes it a natural partner in efforts to promote regional stability. It is the U.S. position that inevitable differences on certain issues should not prevent our cooperation in those areas where we share common interests.

In early January 2011, Secretary Gates traveled to China at the invitation of PRC Minister of National Defense, General Liang Guanglie. Speaking at a joint press event with General Liang, Secretary Gates noted that even though we face obstacles to genuine “strategic understanding,” our two nations have many opportunities to build and improve on areas of bilateral cooperation.

China’s growing capacity in areas of counter-piracy, UN peace missions, and humanitarian aid and disaster relief opens new doors for cooperation with the United States and the international community. As the Chinese

military develops the capability to deliver medical and humanitarian assistance beyond its immediate region, there will be opportunities for the United States and China to collaborate and share “lessons learned” from these endeavors.

The Department of Defense and China’s Ministry of National Defense signed an archival arrangement in 2008 that, for the first time, gave the United States access to PLA archives containing information regarding U.S. servicemen missing in China from World War II, the Korean War and the Cold War. As a result of this agreement, the Defense POW/Missing Personnel Office has made slow but steady progress in accounting for Americans missing in China. Archival research led to the discovery of a U.S. Navy crash site from the Korean War, and consequently, in February 2011, a U.S. recovery operation supported by representatives from the PLA Archives.

The United States and China have opportunities to enhance tactical cooperation, communication, and trust through bilateral and multilateral exercises. Additionally, reciprocal exchanges between mid-grade and junior officers and institutions of professional military education cultivate a generation of rising leaders on both sides who are adept at handling this increasingly complex and vital relationship. ADM Mullen noted in the U.S. Maritime Strategy, “A Cooperative Strategy for 21<sup>st</sup> Century Seapower,” that “trust and cooperation cannot be surged.” The skills acquired through our peacetime interactions foster habits of cooperation and safe communication practices that mitigate risk and diffuse tensions.

The pace and scope of China’s military development, combined with a relative lack of transparency, remains a point of concern in the United States and among our regional allies and partners. In recent years China has demonstrated occasional signs of assertiveness in Asia, particularly in the maritime domain. This trend has contributed to friction between China and some of its

neighbors over disputed maritime territory in the East and South China Seas.

Additionally, the United States and China continue to hold differing views over the rights of coastal states in the waters and airspace beyond their territorial seas. In 2010 several PLA fighter aircraft conducted unusually close intercepts of U.S. military aircraft operating in international airspace. In recent years Chinese ships have also harassed U.S. military survey vessels operating beyond China's territorial seas.

A sustained and reliable military relationship is vital to managing these challenges and ensuring that they do not come to define the relationship or escalate into a crisis. Our military-to-military contacts should support deterrence of conflict and lower the risk of miscalculation by encouraging continuous dialogue based on open and substantive discussion of strategic issues. Although PRC leaders have repeatedly affirmed a commitment to a sustained and reliable military-to-military relationship, they have also linked continuation of engagement to ~~“respect”~~ for China's ~~“core”~~ interests.”

## SPECIAL TOPIC: CHINA'S EVOLVING MARITIME STRATEGY

### THE RISE OF CHINA'S MARITIME SECURITY INTERESTS

Historically a continental power, China increasingly looks to the maritime domain as a source of economic prosperity and national security. China's evolving "maritime consciousness," as reflected in senior-level rhetoric and resource allocation, has potentially far reaching consequences in the Asia Pacific region and beyond. Many PRC officials and citizens view maritime power as a prerequisite to becoming a "great power." This chapter addresses China's attention to the maritime domain, with a particular focus on the security dimension. It identifies the catalysts influencing PRC thinking on maritime interests and the steps China has taken to address these challenges, including naval development, legislation, improving civilian maritime enforcement, and diplomatic initiatives. Finally, it addresses China's specific maritime interests and addresses how China's posture could evolve in the future.

In its 2010 "China Ocean's Development Report," China's State Oceanic Administration (SOA) proclaimed, "building maritime power is China's historic task for the 21<sup>st</sup> century, and the decade from 2010-2020 is the key historic stage for realizing this task." Although China appears to lack an official maritime strategy, PRC officials, military strategists, and academics are focused on the growing relevance of maritime power to China's interests.

### THE EVOLUTION IN "MARITIME CONSCIOUSNESS"

Since the early 1980s, two important factors catalyzed a transformation in Beijing's maritime outlook. First, China's geostrategic environment fundamentally shifted after the Cold War ended. As PRC concerns over a major continental conflict, including the possibility of nuclear war with Russia,

subsided, Beijing turned its attention towards a range of other challenges, particularly Taiwan, which it feared was drifting steadily toward a state of *de jure* independence.

The U.S. response in the 1995-96 Taiwan Strait crisis underscored to Beijing the potential challenge of U.S. military intervention and highlighted the importance of developing a modern navy, capable of conducting A2AD operations, or "counter-intervention operations" in the PLA's lexicon.

Second, China's expanding economic interests, including both maritime commerce and the exploitation of marine resources, have affected Beijing's perception of maritime power as it relates to national interests. Speaking in 2007, President Hu asserted that, "to develop maritime issues is one of the strategic tasks to boost our national economic development." China looks to the oceans as a critical resource, providing fish and potentially large oil and gas reserves.

The oceans also serve as a vital artery for trade and support China's economic health, with approximately ninety percent of China's imports and exports transiting by sea. A net oil exporter until 1993, China now imports over half of the oil it consumes, over 80 percent of which transits the Malacca Strait and South China Sea. Additionally, China's economic engine is concentrated in dense population centers along the country's East coast. Conflicts affecting these coastal regions would have far reaching consequences for China.

### EVOLVING NAVAL STRATEGY

PLA General Liu Huaqing, who commanded a poorly equipped and trained PLA Navy through most of the 1980s, and later served on the CCP Politburo Standing Committee and

as CMC Vice Chairman, advanced the cause of naval modernization amid a strategic culture overwhelmingly dominated by the PLA ground force. Until Liu instituted the PLA Navy's "Offshore Defense" strategy in 1986, the PLA Navy was focused mainly on resisting invasions and defending the homeland."

Often referred to as the "father of the modern Chinese Navy," Liu, who died in January 2011, called for naval operations beyond the PRC littoral and appealed for the eventual development of aircraft carriers. Years would pass before many of Liu's proposals gained political support; however, his ideas fundamentally affected the way PRC strategists conceptualize maritime power and approach maritime strategy.

Although not defined by specific boundaries, Offshore Defense is generally characterized by the maritime space within China's Exclusive Economic Zone (EEZ) or sometimes by the "first island chain," including the Yellow Sea, East China Sea, and South China Sea. In recent years, the PLA Navy has begun emphasizing missions in the so-called "far seas," an area loosely defined by the "second island chain," which stretches from Northern Japan, through the Northern Mariana Islands, through Guam.

Consideration of more distant contingencies has been accompanied by limited peacetime operations outside of this region, including counter-piracy patrols, humanitarian and disaster relief and noncombatant evacuations. These peacetime operations have provided the PLA with valuable operational experience.

## NEW SECURITY INTERESTS DRIVING REQUIREMENTS

In the early 1990s, the PRC watched with concern as more modern militaries adopted high technology weapons and platforms that were changing the nature of modern warfare, including in the maritime domain. From the perspective of many PRC strategists and military officials, military developments in

developed nations made the PLA's coastal-oriented Navy appear antiquated, inadequate, and vulnerable. PRC leaders subsequently directed the PLA to prepare to fight and win "local wars under modern, high-tech conditions." The term "high-tech" was later replaced with "informatized" to reflect the importance of network-centric warfare and information technology.

In his 1992 address to the 14<sup>th</sup> Party Congress, former President Jiang Zemin articulated the need to protect China's evolving "maritime interests." During the nearly two decades that followed, the PRC has pursued its maritime objectives through naval development, legislation, civilian enforcement, and diplomacy. Ambitious naval acquisition closed many of the capability gaps that defined China's Navy prior to and through the 1990s. China today possesses a limited ability to respond to maritime threats beyond the range of land-based aviation. This includes limited power projection capability in the farther regions of the South China Sea and western Pacific. This progress has been slow, but has begun to accelerate as new systems come on line, and China's naval forces gain additional experience in operations beyond the littoral.

Civilian and military officials have underscored the economic impetus for advancing China's maritime interests, reflecting a perception that economic welfare and national security are increasingly linked. PLA Navy Commander Wu Shengli asserted in 2006 that China requires a "powerful navy to protect fishing, resource development and strategic passageways for energy." This dimension is particularly important to the CCP, which has built its legitimacy on the promise of sustained development.

China's maritime interests, including territorial and sovereignty disputes, resource interests, and critical SLOC dependencies remain heavily concentrated in Asia. Consequently, China's naval orientation retains a decidedly regional focus. However, the PLA is assuming more "global" missions.



This reflects the recognition that Chinese economic interests, including commercial shipping and investment projects, along with PRC citizens, are now located across the globe. It also reflects a desire to cast China as a “great power.” China’s leaders have offered unambiguous guidance that the PLA Navy will play a growing role in protecting China’s far-flung interests.

In 2004, not long after assuming Chairmanship of the CMC, Hu Jintao promulgated the “Historic Missions of the Armed Forces in the New Period of the New Century” (*Xin Shiji Xin Jieduan Wojun Lishi Shiming*), commonly referred to as the “New Historic Missions.” In addition to reiterating the Armed Forces’ role in sustaining CCP rule, and protecting China’s sovereignty and territorial integrity, the New Historic Missions highlight the PLA’s role in safeguarding China’s expanding “national interests” and in “ensuring world peace.”

In drawing a clear link between China’s economic interests and national security, the New Historic Missions established a justification for missions beyond China’s maritime periphery. Although the PLA remains focused on regional contingencies, the New Historic Missions imply that the pursuit of China’s interests would not be constrained by geographic boundaries and would evolve to meet a diverse array of challenges. China’s 2006 National Defense White Paper expanded upon the New Historic Missions, when it introduced the concept of “diversified military tasks” (*duoyanghua junshi renwu*—多样化军事任务). This emphasized the need for the PLA to prepare not only for traditional military missions, but also military operations other than war (MOOTW). The PLA Navy has since focused greater attention on counter-piracy, HA/DR, and noncombatant evacuation operations (NEO).

## NEW “FIRSTS” FOR THE PLA NAVY

The PLA Navy’s counter-piracy deployment to the Gulf of Aden, which it has sustained since 2009, remains the most visible manifestation of this policy shift under Hu Jintao. Not including naval diplomacy, the Gulf of Aden mission marked China’s first operational deployment of naval forces outside of regional waters. In September 2010, the PLA Navy’s hospital ship, “PEACE ARK” conducted its first overseas humanitarian mission by visiting five countries in Asia and Africa.

Most recently, the PLA Navy participated in its first noncombatant evacuation operation (NEO). In February 2011, the PLA Navy deployed a JIANGKAI-II class frigate, which had been operating in the Gulf of Aden, to support its evacuation of PRC citizens from Libya. Although largely symbolic, this deployment enabled the PLA Navy to demonstrate a commitment to the protection of PRC citizens living and working overseas.

## CHINA’S MARITIME INTERESTS

These increasingly “diverse” missions have not supplanted regional priorities. The Taiwan challenge remains the “main strategic direction” (*zhuyao zhanlue fangxiang*—主要战略方向) for China’s armed forces, particularly the Navy. Aside from Taiwan, China faces several high priority maritime challenges. First is strengthening and gradually expanding China’s maritime buffer zone as a means to prevent foreign attack or “interference.” A second priority remains advancing China’s maritime territorial claims, particularly the East and South China Seas. Third, China is focused on the protection of regional sea lines of communication (SLOCs).

Fourth, the PRC hopes to advance China’s image as a “great power,” and finally, China intends to deploy a survivable, sea-based nuclear deterrent in the foreseeable future.

**Expanding the Maritime Periphery:** China has long regarded the Yellow Sea, East China Sea, and South China Sea as areas of unique strategic importance. From the perspective of Beijing, these so called “near seas” constitute a security buffer and hold potentially significant oil and gas resources. The PRC has attempted to use legal pronouncements, civilian enforcement, and naval assets to advance PRC interests within this buffer zone.

In 1992, China’s National People’s Congress passed the Law of Territorial Sea and Contiguous Zones, which proclaimed the South China Sea as PRC “historic waters.” Beijing has crafted a series of laws that codify PRC claims to regional territory and proscribe special restrictions on foreign activities in China’s EEZ.

As the name implies, the Exclusive Economic Zone affords states exclusive access to the economic resources within a defined maritime space, not exceeding 200 nautical miles from the coastal baseline. China has attempted to apply security restrictions to the EEZ, which are inconsistent with customary international law as reflected in UNCLOS. Attempts to impede or harass sovereign U.S. vessels and aircraft operating legally in China’s EEZ (beyond China’s 12nm territorial seas) have repeatedly created friction in the U.S.-China relationship.

**Regional Territorial Disputes:** During the 1930s and 1940s, the Republic of China (ROC) began delineating essentially all of the South China Sea, including the Spratly and Paracel Islands, within a nine-dashed line. Although preserving ambiguity on the nature of this claim, the PRC maintains that the territories within the dashed line and their adjacent waters belong to China. Different portions of China’s expansive claim are disputed in whole or in part by Taiwan,

Vietnam, the Philippines, Malaysia, and Brunei. China’s ability to employ coercion in these disputes has grown steadily in recent years. China’s naval modernization, in particular, is affecting security perceptions among rival South China Sea claimants.

China is leveraging both civilian enforcement and naval assets in pursuit of its territorial objectives. In recent years, PRC naval ships and civilian law enforcement agencies have shown signs of greater assertiveness in the region, occasionally triggering friction with rival claimants. In the East China Sea, China faces a contentious dispute with Japan over maritime boundaries. Where this line is drawn has implications for disputed territory and subsea energy resources. In 2010, tensions between Tokyo and Beijing rose after a PRC fishing boat rammed a Japanese Coast Guard vessel near the disputed Senkaku Islands.

The PRC has increasingly sought to enforce its broad maritime claims with civilian assets including the maritime police, the Border Control Department (BCD), Maritime Safety Administration (MSA), State Oceanographic Administration (SOA), Fisheries Law Enforcement Command (FLEC), and Coast Guard. Beijing wishes to present the issue of regional maritime territory as one of law enforcement rather than military rivalry. Beijing likely calculates that the employment of naval assets in these matters raises the risk of escalation, generates regional animosity, and unnecessarily burdens the PLA Navy with non-military tasks. Compared to developed countries, particularly Japan and the United States, China’s civilian maritime agencies are poorly equipped and operated. However, they are improving steadily and will play an increasingly critical function in China’s maritime enforcement efforts.

### Debating China's Role in "Distant Seas"

Around the time President Hu Jintao articulated the "New Historic Missions" in 2004, Chinese officials and scholars began openly discussing the extent to which China should expand its maritime power. The term "*yuanghai fangwei*" (远海防卫) which translates to "distant/far sea defense," began appearing with increasing frequency in Chinese publications. Authors associated with the Naval Research Institute (NRI) called the "shift from offshore to open ocean naval operations" an "inevitable historic choice" for China noting that naval power must "match the expansion of China's maritime interests."

Navy deployment trends in recent years underscore China's interests in a limited "far seas" capability. Some PRC commentators advocate a sustained shift from an "Offshore Defense" strategy to "Far Seas Defense." Many others characterize Far Seas Defense as simply an extension or adjustment of the existing strategy, rather than a fundamental change. China's 2010 Defense White Paper reiterated the PLA Navy's commitment to its Offshore Defense strategy while acknowledging efforts to improve operational capabilities in far seas.

Recently, several Navy officials and commentators have broached the once-taboo topic of overseas military basing. In late 2009, Rear Admiral Yin Zhuo (retired), attracted extensive international media attention when he suggested in an interview, that China requires a "stable and permanent supply and repair base" to support its overseas counter-piracy activities. With an aircraft carrier program being realized over the next decade, the Navy may face even greater incentive to improve its support options.

It is not clear if China will pursue traditional military "bases," suited for supporting distant combat operations, or a more limited set of logistical supply "places," that are better suited to peacetime deployments, such as counter-piracy and HA/DR.

### SEA LANE PROTECTION

Since China's emergence as a global economic actor, it has relied nearly exclusively on the United States as the guarantor of a safe and unrestricted maritime domain. Approximately 90 percent of China's trade volume is conducted via maritime transport and approximately 50 percent of global merchant traffic passes through regional waters.

This dependency has prompted greater attention to SLOC protection missions. PRC officials have expressed particular concern over the Strait of Malacca. Even with its recent advances in naval power, would face great difficulty responding to threats to shipping in the far reaches of the South China Sea, including the Strait of Malacca.

The PLA Navy's ongoing effort in the Gulf of Aden underscores China's strong interest in protecting maritime commerce, from both traditional and non-traditional threats. The United States welcomes China's contribution to maintaining the safety and security of the global maritime domain. This deployment underscores an area where mutual interest can foster cooperation.

### GREAT POWER STATUS

China's ambitious naval modernization remains a great source of pride for the PRC public and leadership. China has deployed its most modern ships to engage in naval diplomacy and counter-piracy in a coalition environment. Many in China see naval power as a prerequisite for great power status.

PRC officials and commentators occasionally lament the fact that China is the only permanent member of the U.S. Security Council without an aircraft carrier. The PLA Navy's anticipated deployment of aircraft carriers over the coming decade will likely serve as a great source of national pride, regardless of actual combat capability.

China's leaders have tapped into this nationalistic sentiment, contrasting China's current naval power with the late Qing Dynasty, which was easily overwhelmed by more modern Japanese and Western naval forces. On December 27, 2006, President Hu Jintao expressed confidence in China's naval development, asserting to a group of PLA Navy officers that China was now "a great maritime power" (*haiyang daguo*), adding that the PRC must continue strengthening and modernizing its Navy.

### SEA-BASED NUCLEAR FORCES

China continues efforts to deploy a sea-based nuclear deterrent. Although the PLA Navy has received the JIN-class SSBN, it has faced repeated challenges with the JL-2 weapons system. The system did not reach an initial operational capability (IOC) by 2010 as DoD had anticipated. Once China overcomes remaining technical hurdles, the PLA Navy will be charged with protection of a nuclear asset.

### OVERCOMING KEY CHALLENGES

Although areas of PLA progress frequently attract attention, lesser understood capability gaps remain. For example, the Gulf of Aden deployment has underscored the complexity of distant operations to China's military and civilian leadership. According to Rear Admiral Yin Zhuo, the Gulf of Aden mission has "shown the Navy's equipment is not particularly suited to blue water operations... [and] our equipment, our technology, especially our level of information infrastructure and communication means, as well as our blue water deployment

capabilities... still have a relatively long way to go to catch up with that of the Western countries."

China's regional capabilities have improved significantly over the past two decades. However, in the near term, China would face great difficulty projecting military power beyond regional waters during a sustained conflict. China lacks overseas bases and supply infrastructure, and despite some recent progress, remains reliant on shore-based defenses. Over time, China's growing involvement in international peacekeeping efforts, military diplomacy, counter-piracy operations, humanitarian assistance and disaster relief, evacuation of Chinese citizens from overseas trouble spots, and exercise activity, will improve the PLA's capability to operate at greater distances from the mainland. This operational experience could eventually facilitate a "global" military presence, should China's leadership pursue that course.

### ASSESSING THE FUTURE

The evolution of China's economic and geostrategic interests has fundamentally altered Beijing's view of maritime power. Today, the PLA Navy and China's civilian maritime agencies are addressing gaps in regional capabilities while engaging in a small number of peacetime operations beyond the region, where their capabilities remain more limited. The expansion of missions reflects the availability of resources and the PRC's increasingly diverse interests.

Beyond immediate regional interests, China's expanding capabilities might facilitate greater attention to maritime challenges further into the Pacific and Indian Oceans. In contrast to a decade ago, many of China's new naval platforms can utilize space-based communications, advanced sensors, and area air-defense, enabling combat capability at great distances from land. Current peacetime deployments are providing PLA Navy

operators with valuable experience outside of the region.

The establishment of overseas bases and the development of more than a few aircraft carriers might signal a trend towards more “global” missions. Greater openness from

China regarding the nature and scope of its maritime ambitions could help mitigate suspicions and ensure that China’s maritime development becomes a source of global stability rather than a source of friction.



*(This page left intentionally blank)*

## **SPECIAL TOPIC: CHINA'S MILITARY ENGAGEMENT**

---

The PLA has increasingly engaged with foreign militaries over the past decade. At the operational level, military engagement provides opportunities to share doctrine, tactics, techniques, and procedures with other militaries, both modern and developing. At the strategic level, military engagement allows Beijing to demonstrate its capabilities and emerging role in the international system.

China's military modernization has facilitated cooperation in two key respects. First, PLA modernization has removed capability-based constraints, allowing the PLA to operate with more advanced forces and at greater distances from the PRC mainland. Just a decade ago, for example, China's sustained deployment to the Gulf of Aden and the many associated foreign engagements would have proven exceedingly difficult, if not impossible for China.

Second, Beijing takes pride in "showing the flag" with an increasingly modern array of platforms, both imported and indigenously designed. The international fanfare surrounding the PLA Navy's 60<sup>th</sup> Anniversary celebration in 2009 underscored the growing confidence in China's military development and desire to showcase these achievements.

### **TRADITIONAL MILITARY DIPLOMACY**

Senior level visits and exchanges provide the PRC with opportunities to increase military officers' international exposure, communicate China's positions to foreign audiences, better understand alternative world views, and advance foreign relations through interpersonal contacts and military assistance programs.

PLA engagement with foreign partners has grown in tandem with China's global profile, enabling China's military officers to observe and study foreign military command structures, unit formations, and operational

training. PLA Navy port calls within Asia and beyond the region have steadily increased since 2002. In 2010, the PLA maintained a regular presence in over 100 countries with at least 300 attachés posted abroad, up from 201 in 2002 and 220 in 2005. The number of countries with defense attachés in Beijing is also increasing. As of 2010, 102 countries had established military attaché offices in China, up from 79 countries in 1996.

The PLA Navy's counter-piracy role in the Gulf of Aden has provided opportunities to advance China's image as a modern military that can act alongside other major world navies. PLA Navy port calls made both in the region and in transit to and from the Gulf of Aden reinforce China's political, military, and economic ties with those countries.

China hosts foreign military officers as students in its military academies. In October 2009, foreign military students from over 70 countries observed the PLA exercise VANGUARD 2009, which included a live fire demonstration. The first PLA exercise opened to observation by foreign military students was QIANFENG 2008, which reportedly involved an armored brigade conducting an offensive maneuver in a mountainous area.

The PLA's first instance of a mixed training class with both Chinese and foreign officers culminated with a June 2009 graduation ceremony at the Air Force Command College (AFCC), which included 56 officers from the air forces of 29 foreign countries and 12 officers from the PLA Air Force.

### **COMBINED EXERCISES**

The PLA participates in a growing number of bilateral and multilateral military exercises in areas such as counter-terrorism, mobility operations, and logistics. The PLA gains operational insight by observing tactics,

command decision making, and equipment used by more advanced militaries.

China is eager to present these activities as constructive, peaceful, and not directed against any other country. Many of the PLA's exercises with foreign militaries are conducted under the rubric of counter-terrorism. Beijing has held exercises bilaterally with Russia, India, Pakistan, Thailand, Singapore, Australia, and multilaterally with the Shanghai Cooperation Organization and the various countries that participated in the Pakistan-hosted exercise AMAN-09. In 2010, the PLA conducted five training exercises with foreign militaries, three of which were held in China.

Additionally, China has invited foreign military observers and resident military attachés to observe PLA exercises on at least six occasions since 2003, enabling China to project an overall national image of “peaceful development” and increased military transparency.

The PLA Navy routinely conducts search and rescue exercises with foreign militaries, including exercises with Australia, the United Kingdom, India, Pakistan, Japan, New Zealand, Russia, Vietnam, and others. These exercises serve training purposes and build rapport with foreign countries.

## PEACEKEEPING OPERATIONS

Prior to 2002, Beijing generally avoided participation in UN peacekeeping operations (PKO), due to lingering skepticism of the international system and a long-stated policy of “non-interference” in other countries' internal affairs. China's participation from 1991-1993 in the UN Transitional Authority in Cambodia marked a notable exception to this policy. China's attitude towards UN PKOs has changed dramatically over the past decade, particularly since Hu Jintao promulgated the New Historic Missions in 2004.

In January 2004, China had just 359 peacekeepers deployed to eight UN peacekeeping missions, with no single contingent containing more than 70 troops. Six years later, in January 2010, China had 2,131 peacekeepers (all non-combat) supporting 10 UN missions, with five separate contingents containing more than 200 troops. China is now the leading contributor of peacekeeping personnel among the five permanent members of the UN Security Council. PRC contributions have consisted of civilian police; military observers; and engineering, logistics, and medical troops. China provided several rotations of over 100 police officers to the United Nations Stabilization Mission in Haiti (MINUSTAH). In 2010, China will shoulder approximately \$300 million of the UN peacekeeping budget.

China regards participation in UN peacekeeping operations as serving multiple objectives, including improving China's international standing and image, demonstrating support for international stability in troubled regions, providing opportunities to initiate and expand intelligence collection, and enhancing relationships in the affected areas. Beijing has also demonstrated a growing willingness to deploy personnel on missions where conditions are more hazardous. After the 2006 death of a PRC peacekeeper in Lebanon, for example, the PLA increased its troop contributions to the UN Interim Force in Lebanon (UNIFIL). As of July 2010, Beijing will be deploying over 400 members of the 7<sup>th</sup> Chinese Peacekeeping Troops to support the African Union-UN Mission in Sudan.

Highlighting PRC interest in PKO's, China opened the Ministry of National Defense (MND) Peacekeeping Center in July 2009, the first PLA peacekeeping facility dedicated to professional training and international exchange. Later in September 2010, the MND co-hosted with the UN the first senior commanders' training course on peacekeeping. Although China has yet to deploy combat troops for peacekeeping duty,

Beijing has openly discussed this as a future possibility.

## **HUMANITARIAN ASSISTANCE/DISASTER RELIEF**

Over the past decade the PLA steadily increased its participation in international HA/DR missions. Investment in large amphibious ships, a new hospital ship, long-range transport aircraft, and improved logistics has made this mission a practical reality. Since 2002, the PLA has contributed to at least thirteen emergency relief operations in fourteen countries in China's immediate region as well as in Haiti during the aftermath of the earthquake in January 2010. Like PKOs, involvement in international HA/DR enables China to present a positive face to its military development while simultaneously advancing China's image as a responsible global power.

In late 2010, PLA Navy's new hospital ship PEACE ARK conducted the 88-day "MISSION HARMONY-2010" deployment to the Gulf of Aden to provide medical care to the PLA Navy counter-piracy flotilla and to treat needy residents in Djibouti, Kenya, Tanzania, Seychelles, and Bangladesh. This mission marked the PLA Navy's first foreign deployment of a hospital ship.

The PLA's humanitarian relief capability and capacity remains limited, but China is seeking to collaborate with regional partners to improve these capabilities. China and Indonesia drafted the "Association of Southeast Asian Nations (ASEAN) Regional Forum General Guidelines on Disaster Relief Cooperation" to steer the development of Standard Operating Procedures for future

HA/DR operations, which were adopted in July 2007.

China has also learned that growing capability and capacity can heighten foreign expectations for support. For example, in August 2010, critics suggested that many nations, including China, had reacted too slowly and inadequately to Pakistan's massive flooding. Despite the close political relationship between Beijing and Islamabad, China's early contributions to the 2010 disaster response were small compared to those of other nations.

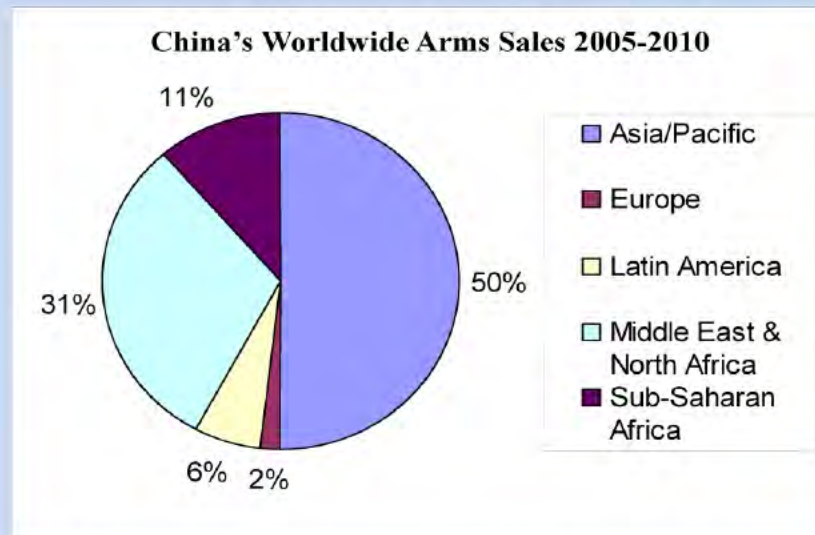
## **ARMS SALES**

Beijing conducts arms sales to enhance foreign relationships and generate revenue. Although weighted more towards small arms and ammunition, PRC arms sales also include the joint development or transfer of advanced weapons systems. Chinese companies sell primarily to developing countries where China's lower-cost weapons and fewer political constraints provide a competitive advantage. Arms sales also play a role in advancing trade relationships, particularly where energy or valuable raw materials are concerned. For example, arms sales and other forms of security assistance to Iran and Sudan have deepened ties and helped to offset the cost of PRC energy imports. Arms sales play an important role in China's efforts to influence cash-strapped countries, many of which do not have access to other sources of arms for either political or economic reasons. As the quality and range of PRC-produced arms improves, Beijing will be increasingly able to wield arms sales as an instrument of influence.



### PRC Arms Sales

From 2005 to 2010, China sold approximately \$11 billion worth of conventional weapons systems worldwide, ranging from general purpose materiel to major end items. PRC arms exports will likely increase in the coming years as China's domestic defense industry improves. Although China's defense industry is primarily oriented toward supplying the PLA, foreign arms sales are also important. Arms sales provide a means to cultivate relationships with important strategic partners, such as Pakistan, while generating revenue for its defense industry. PRC defense firms are marketing and selling arms throughout the world, with the bulk of their sales to Asia and the Middle East/North Africa. China is able to make gains in these markets because of modest improvements in quality of its equipment coupled with relatively low costs and favorable conditions for payment.



*PRC Worldwide Arms Sales. Arms sales for 2005-2010, by region.*

From 2005-2010, China sold approximately \$11 billion worth of conventional weapons systems worldwide. Pakistan remains China's primary customer for conventional weapons. Beijing engages in both arms sales and defense industrial cooperation with Islamabad. Sales to Islamabad have included the JF-17 fighter aircraft and associated production facilities; F-22P frigates with helicopters; K-8 jet trainers; F-7 fighter aircraft; early warning and control aircraft; tanks; air-to-air missiles; anti-ship cruise missiles; missile technologies; and small arms and ammunition. Sales to other countries include fighter, transport, and jet trainer aircraft; helicopters; tanks; air defense equipment, including radar, rockets, military vehicles, patrol boats, missiles and missile technology; and small arms and ammunition.

China is targeting niche markets, introducing weapons systems not offered by Russian or Western suppliers. These systems include GPS and GLOSNASS-equipped multiple rocket launcher systems and short-range ballistic missiles that have been marketed and sold to Middle East and African partners.

The volume of PRC defense sales is still modest compared to the world's leading arms sellers. However, interest in PRC arms will likely increase in the future as China's defense firms market and sell increasingly sophisticated yet affordable arms. China offers generous repayment options and technology transfer to persuade other countries to purchase from PRC firms.



### *Sales to Areas of Instability*

Several PRC entities continue to provide arms to customers in unstable regions.

- **Iran:** China supported UN Security Council Resolutions 1737, 1747, 1803, 1835, and 1929. China has stated that it is committed to implementing resolution 1929 and the other resolutions on Iran fully and faithfully, but China has also stated that it does not support sanctions beyond those contained in the UN resolutions. China has stated that it agrees with the United States that a nuclear-armed Iran would pose a grave regional and international threat. The United States is continuing to work closely with China on this issue. A number of PRC transfers to Iran resulted in U.S. trade penalties and sanctions against entities in China. Some weapons that PRC entities supplied to Iran were found to have been transferred to terrorist organizations in Iraq and Afghanistan. This is a serious issue that the United States continues to monitor.
- **Sudan:** The PRC has at times used its influence with the Sudanese government to address in a positive way international concerns over Darfur and to support the implementation of the Comprehensive Peace Agreement between North and South Sudan. However, China has sided with Khartoum at the UN Security Council, including blocking targeted

sanctions against Sudanese officials accused of atrocities. China continues to sell arms to Sudan despite the passage of UN Security Council Resolutions 1556 (2004) and 1591 (2005), both of which ban the transfer of arms to Darfur. Between 2004 and 2006, when the violence in Darfur was at its peak, 90 percent of small arms sales to Sudan were of PRC origin. The PRC argues that arms sales constitute part of normal commercial relations, and that the arms supplied by Chinese companies were not meant for use in Darfur. However, UN Group of Experts and NGO reports have demonstrated that Chinese arms have been used by the Sudanese government in combat operations in Darfur.

### CONCLUSION

Beijing's approach to international engagement has evolved with its perception of its own interests in a dynamic security environment. As China's regional and international interests expand, so too will China's impetus for additional engagement, especially in the areas of peacekeeping operations, HA/DR, and joint exercises. In addition to furthering PLA modernization, these engagements will likely be geared toward building China's political ties, assuaging fears about China's rise, and expanding China's international influence, particularly in Asia.

*(This page left intentionally blank)*

**APPENDIX I:**  
**CHINA AND TAIWAN FORCES DATA**

<b>Taiwan Strait Military Balance, Ground Forces</b>			
	<b>China</b>		<b>Taiwan</b>
	<i>Total</i>	<i>Taiwan Strait Area</i>	<i>Total</i>
<b><i>Personnel (Active)</i></b>	1.25 million	400,000	130,000
<b><i>Group Armies</i></b>	18	8	3
<b><i>Infantry Divisions</i></b>	17	5	0
<b><i>Infantry Brigades</i></b>	22	9	8
<b><i>Mechanized Infantry Divisions</i></b>	6	2	0
<b><i>Mechanized Infantry Brigades</i></b>	6	1	3
<b><i>Armor Divisions</i></b>	9	4	0
<b><i>Armor Brigades</i></b>	8	3	4
<b><i>Artillery Divisions</i></b>	2	2	0
<b><i>Artillery Brigades</i></b>	17	6	5
<b><i>Airborne Divisions</i></b>	3	3	0
<b><i>Amphibious Divisions</i></b>	2	2	0
<b><i>Amphibious Brigades</i></b>	3	3	3
<b><i>Tanks</i></b>	7,000	3,100	1,100
<b><i>Artillery Pieces</i></b>	8,000	3,400	1,600
<p><b>Note:</b> PLA active ground forces are organized into Group Armies. Infantry, armor, and artillery units are organized into a combination of divisions and brigades deployed throughout the PLA's seven MRs. A significant portion of these assets are deployed in the Taiwan Strait area, specifically the Nanjing, Guangzhou, and Jinan MRs. Taiwan has seven Defense Commands, three of which have Field Armies. Each Army contains an Artillery Command roughly equivalent to a brigade plus.</p>			



#### CHINA: Group Armies (GA) Primary Missions

<b>Shenyang MR</b>	<b>Nanjing MR</b>	<b>Lanzhou MR</b>
16 GA – Defensive, Offensive CT	1 GA – Amphibious, Offensive CT	47 GA – Defensive, Offensive CT
39 GA – RRU, Offensive MF	12 GA – Amphibious, Offensive CT	21 GA – Offensive MF, Defensive
40 GA – Defensive, Offensive CT	31 GA – Amphibious, Offensive CT	
<b>Beijing MR</b>	<b>Guangzhou MR</b>	
65 GA – Defensive	15 Airborne – RRU, Offensive MF	
38 GA – RRU, Offensive MF	41 GA – Offensive CT, Amphibious	
27 GA – Defensive	42 GA – Amphibious	
<b>Jinan MR</b>	<b>Chengdu MR</b>	
26 GA – Offensive CT, Defensive	13 GA – Defensive, Offensive CT	
20 GA – Offensive CT, Defensive	14 GA – Defensive, Offensive CT	
54 GA – Offensive MF, Amphibious		

MR – Military Region  
MF – Mobile Force  
RRU – Rapid Reaction Unit  
CT – Complex Terrain (mountain, urban, jungle, etc.)

#### Major Ground Units



<b>Taiwan Strait Military Balance, Naval Forces</b>			
	<b>China</b>		<b>Taiwan</b>
	<i><b>Total</b></i>	<i><b>East and South Sea Fleets</b></i>	<i><b>Total</b></i>
<i><b>Destroyers</b></i>	26	16	4
<i><b>Frigates</b></i>	53	44	22
<i><b>Tank Landing Ships/ Amphibious Transport Dock</b></i>	27	25	12
<i><b>Medium Landing Ships</b></i>	28	21	4
<i><b>Diesel Attack Submarines</b></i>	49	33	4
<i><b>Nuclear Attack Submarines</b></i>	5	2	0
<i><b>Coastal Patrol (Missile)</b></i>	86	68	61
<p><b>Note:</b> The PLA Navy has the largest force of principal combatants, submarines, and amphibious warfare ships in Asia. After years of neglect, the force of missile-armed patrol craft is also growing. In the event of a major Taiwan conflict, the East and South Sea Fleets would be expected to participate in direct action against the Taiwan Navy. The North Sea Fleet would be responsible primarily for protecting Beijing and the northern coast, but could provide mission-critical assets to support other fleets.</p>			



### Major Naval Units

Taiwan Strait Military Balance, Air Forces			
China			Taiwan
<i>Aircraft</i>	<i>Total</i>	<i>Within range of Taiwan</i>	<i>Total</i>
<i>Fighters</i>	1,680	330	388
<i>Bombers/Attack</i>	620	160	22
<i>Transport</i>	450	40	21
<p><b>Note:</b> The PLAAF and the PLA Navy have approximately 2,300 operational combat aircraft. These consist of air defense and multi-role fighters, ground attack aircraft, fighter-bombers, and bombers. An additional 1,450 older fighters, bombers and trainers are employed for training and R&amp;D. The two air arms also possess approximately 450 transports and over 100 surveillance and reconnaissance aircraft with intelligence, surface search, and airborne early warning capabilities. The majority of PLAAF and PLA Navy aircraft are based in the eastern half of the country. Currently, 490 aircraft could conduct combat operations against Taiwan without refueling. However, this number could be significantly increased through any combination of aircraft forward deployment, decreased ordnance loads, or altered mission profiles.</p>			



### Major Air Units

<i>China's Missile Force</i>			
<i>System</i>	<i>Missiles</i>	<i>Launchers</i>	<i>Estimated Range</i>
ICBM	50-75	50-75	5,400-13,000+ km
IRBM	5-20	5-20	3,000+ km
MRBM	75-100	75-100	1,750+ km
SRBM	1,000-1,200	200-250	300-600 km
GLCM	200-500	40-55	1,500+ km



**APPENDIX II:**  
**MILITARY-TO-MILITARY EXCHANGES**

**Bilateral and Multilateral Exercises Since 2005**

<b>Year</b>	<b>Exercise Name</b>	<b>Type of Exercise</b>	<b>Participants</b>
2005	China-India Friendship 2005	Search and Rescue	India
	China-Pakistan Friendship 2005	Search and Rescue	Pakistan
	China-Thailand Friendship 2005	Search and Rescue	Thailand
	Peace Mission 2005	Counter-terrorism	Russia
2006	Cooperation 2006	Counter-terrorism	Tajikistan
	Friendship 2006	Counter-terrorism	Pakistan
	<i>Unnamed</i>	Search and Rescue	United States
2007	Aman (Peace) 2007	Search and Rescue	Pakistan
	China-France Friendship 2007	Maritime	France
	China-Spain Friendship 2007	Maritime	Spain
	Cooperation 2007	Counter-terrorism	Russia
	Hand-in-Hand 2007	Counter-terrorism	India
	Peace Mission 2007	Counter-terrorism	Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan
	Strike 2007	Counter-terrorism	Thailand
	Western Pacific Naval Symposium	Search and Rescue	United States, France, Japan, Australia, New Zealand, India, Pakistan, ROK, Singapore
	<i>Unnamed</i>	Maritime	India
	<i>Unnamed</i>	Search and Rescue	Australia, New Zealand
2008	Hand-in-Hand 2008	Counter-terrorism	India
	Strike 2008	Counter-terrorism	Thailand
2009	Aman (Peace) 2009	Maritime	Hosted by Pakistan (38 countries participated)
	Cooperation 2009	Counter-terrorism	Singapore

2009	Country-Gate Sharp Sword 2009	Counter-terrorism	Russia
	Peace Angel 2009	Medical	Gabon
	Peace Keeping Mission 2009	Peacekeeping Operations	Mongolia
	Peace Mission 2009	Counter-terrorism	Russia
	Peace Shield 2009	Counter-piracy	Russia
	<i>Unnamed</i>	Maritime	Singapore
2010	Blue Strike/Blue Assault 2010	Counter-terrorism	Thailand
	Cooperation 2010	Counter-terrorism	Singapore
	Friendship 2010	Counter-terrorism	Pakistan
	Friendship Action 2010	Ground (Mountain Warfare)	Romania
	Peace Angel 2010	Medical	Peru
	Peace Mission 2010	Counter-terrorism	Russia, Kazakhstan, Kyrgyzstan, Tajikistan
	Strike 2010	Counter-terrorism	Thailand
	<i>Unnamed</i>	Search and Rescue	Australia
	<i>Unnamed</i>	Maritime	New Zealand
	<i>Unnamed</i>	Counter-Piracy	South Korea
	<i>Unnamed</i>	Search and Rescue	Taiwan
	<i>Unnamed</i>	Air	Turkey
	<i>Unnamed</i>	Ground	Turkey
	<i>Unnamed</i>	Search and Rescue	Vietnam

***Chinese Involvement in bilateral and multilateral military exercises since 2005.***

**Countries Visited by Senior Chinese Military Leaders, 2005-2010**

2005	2006	2007	2008	2009	2010
Argentina	Australia	Argentina	Bahrain	Australia	Angola
Bangladesh	Belarus	Chile	Belarus	Bulgaria	Australia
Cuba	Burma	Cuba	Brazil	Burma	Brazil
Denmark	Cambodia	Greece	Brunei	Finland	Colombia
Egypt	Denmark	Japan	Chile	Germany	Congo
Germany	France	Kuwait	Germany	Japan	Egypt
India	Hungary	Kyrgyzstan	Hungary	New Zealand	Germany
Kazakhstan	India	Mongolia	India	North Korea	Indonesia
Netherlands	Laos	Philippines	Indonesia	Pakistan	Kazakhstan
Philippines	Malaysia	Russia	Italy	Papua New Guinea	Kenya
Russia	New Zealand	South Korea	Japan	Russia	Macedonia
Sudan	North Korea	Thailand	Nepal	Serbia-Montenegro	Mexico
Tajikistan	Norway	United States	Norway	Singapore	Mongolia
Tanzania	Pakistan	Uzbekistan	Oman	Slovakia	Namibia
Turkey	Romania	Vietnam	Qatar	South Korea	New Zealand
Uruguay	Russia		Saudi Arabia	Thailand	North Korea
	Singapore		Serbia-Montenegro	Turkey	Pakistan
	South Korea		Singapore	United States	Romania
	Tajikistan		South Korea	Vietnam	Russia
	Thailand		Tajikistan		Serbia
	United States		Thailand		Singapore
	Vietnam		United Arab Emirates		Tanzania
			Venezuela		Turkmenistan
					United Kingdom
					Vietnam

**Senior Foreign Military Officials Visiting China in 2010**

Afghanistan	Guyana	Qatar
Algeria	India	Rwanda
Angola	Italy	Serbia
Australia	Japan	Singapore
Austria	Laos	Switzerland
Azerbaijan	Lebanon	Thailand
Belarus	Macedonia	Tonga
Bolivia	Montenegro	Turkey
Burma	Nepal	Uganda
Cambodia	New Zealand	United Arab Emirates
Congo	North Korea	United Kingdom
Cuba	Norway	Vietnam
Ethiopia	Oman	Zambia
Ghana	Pakistan	Zimbabwe
Greece	Poland	

*This list includes visits by senior defense officials and chiefs of the armed services. It excludes visits associated with multilateral military exercises.*



*(This page left intentionally blank)*

# EXHIBIT 6



STATEMENT FOR THE RECORD

# **WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY**

---

**Daniel R. Coats**  
Director of National Intelligence

13 February 2018

STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT  
of the  
US INTELLIGENCE COMMUNITY

February 13, 2018

**INTRODUCTION**

Chairman Burr, Vice Chairman Warner, Members of the Committee, thank you for the invitation to offer the United States Intelligence Community's 2018 assessment of threats to US national security. My statement reflects the collective insights of the Intelligence Community's extraordinary women and men, whom I am privileged and honored to lead. We in the Intelligence Community are committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

The order of the topics presented in this statement does not necessarily indicate the relative importance or magnitude of the threat in the view of the Intelligence Community.

Information available as of 8 February 2018 was used in the preparation of this assessment.

## CONTENTS

INTRODUCTION .....	2
CONTENTS .....	3
FOREWORD .....	4
GLOBAL THREATS .....	5
CYBER THREATS .....	5
WEAPONS OF MASS DESTRUCTION AND PROLIFERATION .....	7
TERRORISM .....	9
COUNTERINTELLIGENCE AND FOREIGN DENIAL AND DECEPTION .....	11
EMERGING AND DISRUPTIVE TECHNOLOGY .....	12
TECHNOLOGY ACQUISITIONS AND STRATEGIC ECONOMIC COMPETITION .....	12
SPACE AND COUNTERSPACE .....	13
TRANSNATIONAL ORGANIZED CRIME .....	13
ECONOMICS AND ENERGY .....	15
HUMAN SECURITY .....	16
REGIONAL THREATS .....	18
EAST ASIA .....	18
MIDDLE EAST AND NORTH AFRICA .....	19
SOUTH ASIA .....	22
RUSSIA AND EURASIA .....	23
EUROPE .....	25
AFRICA .....	26
THE WESTERN HEMISPHERE .....	27



## FOREWORD

*Competition among countries will increase in the coming year as major powers and regional aggressors exploit complex global trends while adjusting to new priorities in US foreign policy. The risk of interstate conflict, including among great powers, is higher than at any time since the end of the Cold War. The most immediate threats of regional interstate conflict in the next year come from North Korea and from Saudi-Iranian use of proxies in their rivalry. At the same time, the threat of state and nonstate use of weapons of mass destruction will continue to grow.*

- Adversaries and malign actors will use all instruments of national power—including information and cyber means—to shape societies and markets, international rules and institutions, and international hot spots to their advantage.
- China and Russia will seek spheres of influence and to check US appeal and influence in their regions. Meanwhile, US allies' and partners' uncertainty about the willingness and capability of the United States to maintain its international commitments may drive them to consider reorienting their policies, particularly regarding trade, away from Washington.
- Forces for geopolitical order and stability will continue to fray, as will the rules-based international order. New alignments and informal networks—outside traditional power blocs and national governments—will increasingly strain international cooperation.

*Tension within many countries will rise, and the threat from Sunni violent extremist groups will evolve as they recoup after battlefield losses in the Middle East.*

- Slow economic growth and technology-induced disruptions in job markets are fueling populism within advanced industrial countries and the very nationalism that contributes to tension among countries.
- Developing countries in Latin America and Sub-Saharan Africa face economic challenges, and many states struggle with reforms to tamp down corruption. Terrorists and criminal groups will continue to exploit weak state capacity in Africa, the Middle East, and Asia.
- Challenges from urbanization and migration will persist, while the effects of air pollution, inadequate water, and climate change on human health and livelihood will become more noticeable. Domestic policy responses to such issues will become more difficult—especially for democracies—as publics become less trusting of authoritative information sources.

## GLOBAL THREATS

### CYBER THREATS

*The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits.* The risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war.

- In 2016 and 2017, state-sponsored cyber attacks against Ukraine and Saudi Arabia targeted multiple sectors across critical infrastructure, government, and commercial networks.
- Ransomware and malware attacks have spread globally, disrupting global shipping and production lines of US companies. The availability of criminal and commercial malware is creating opportunities for new actors to launch cyber operations.
- We assess that concerns about US retaliation and still developing adversary capabilities will mitigate the probability of attacks aimed at causing major disruptions of US critical infrastructure, but we remain concerned by the increasingly damaging effects of cyber operations and the apparent acceptance by adversaries of collateral damage.

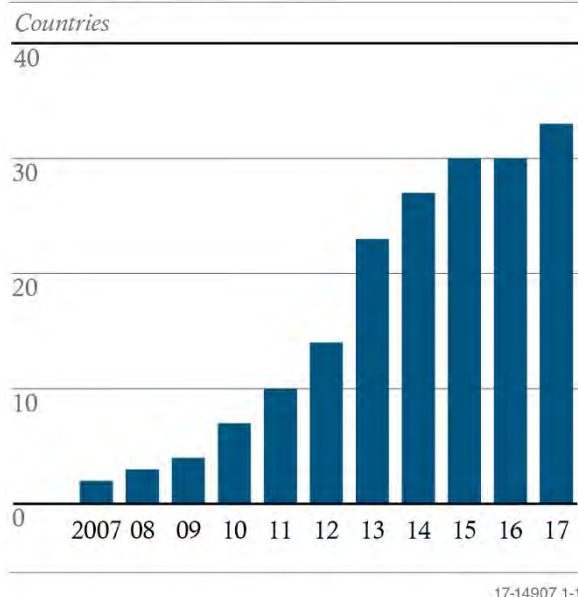
#### Adversaries and Malign Actors Poised for Aggression

*Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year.*

These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations. Nonstate actors will continue to use cyber operations for financial crime and to enable propaganda and messaging.

- The use of cyber attacks as a foreign policy tool outside of military conflict has been mostly limited to sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing more aggressive cyber attacks that pose growing threats to the United States and US partners.

**Countries With Cyber Attack Capabilities**



**Russia.** *We expect that Russia will conduct bolder and more disruptive cyber operations during the next year, most likely using new capabilities against Ukraine.* The Russian Government is likely to build on the wide range of operations it is already conducting, including disruption of Ukrainian energy-distribution networks, hack-and-leak influence operations, distributed denial-of-service attacks, and false flag operations. In the next year, Russian intelligence and security services will continue to probe US and allied critical infrastructures, as well as target the United States, NATO, and allies for insights into US policy.

**China.** *China will continue to use cyber espionage and bolster cyber attack capabilities to support national security priorities.* The IC and private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral US-China cyber commitments of September 2015. Most detected Chinese cyber operations against US private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide. China since 2015 has been advancing its cyber attack capabilities by integrating its military cyber attack and espionage resources in the Strategic Support Force, which it established in 2015.

**Iran.** *We assess that Iran will continue working to penetrate US and Allied networks for espionage and to position itself for potential future cyber attacks, although its intelligence services primarily focus on Middle Eastern adversaries—especially Saudi Arabia and Israel.* Tehran probably views cyberattacks as a versatile tool to respond to perceived provocations, despite Iran's recent restraint from conducting cyber attacks on the United States or Western allies. Iran's cyber attacks against Saudi Arabia in late 2016 and early 2017 involved data deletion on dozens of networks across government and the private sector.

**North Korea.** *We expect the heavily sanctioned North Korea to use cyber operations to raise funds and to gather intelligence or launch attacks on South Korea and the United States.* Pyongyang probably has a number of techniques and tools it can use to achieve a range of offensive effects with little or no warning, including distributed denial of service attacks, data deletion, and deployment of ransomware.

- North Korean actors developed and launched the WannaCry ransomware in May 2017, judging from technical links to previously identified North Korean cyber tools, tradecraft, and operational infrastructure. We also assess that these actors conducted the cyber theft of \$81 million from the Bank of Bangladesh in 2016.

**Terrorists and Criminals.** *Terrorist groups will continue to use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations.* Given their current capabilities, cyber operations by terrorist groups mostly likely would result in personally identifiable information (PII) disclosures, website defacements, and denial-of-service attacks against poorly protected networks. Transnational criminals will continue to conduct for-profit cyber-enabled crimes, such as theft and extortion against US networks. We expect the line between criminal and nation-state activity to become increasingly blurred as states view cyber criminal tools as a relatively inexpensive and deniable means to enable their operations.

## WEAPONS OF MASS DESTRUCTION AND PROLIFERATION

*State efforts to modernize, develop, or acquire weapons of mass destruction (WMD), their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and its allies.* Both state and nonstate actors have already demonstrated the use of chemical weapons in Iraq and Syria. Biological and chemical materials and technologies—almost always dual-use—move easily in the globalized economy, as do personnel with the scientific expertise to design and use them for legitimate and illegitimate purposes. Information about the latest discoveries in the life sciences also diffuses rapidly around the globe, widening the accessibility of knowledge and tools for beneficial purposes and for potentially nefarious applications.

### Russia

Russia has developed a ground-launched cruise missile (GLCM) that the United States has declared is in violation of the Intermediate-Range Nuclear Forces (INF) Treaty. Despite Russia's ongoing development of other Treaty-compliant missiles with intermediate ranges, Moscow probably believes that the new GLCM provides sufficient military advantages to make it worth risking the political repercussions of violating the INF Treaty. In 2013, a senior Russian administration official stated publicly that the world had changed since the INF Treaty was signed in 1987. Other Russian officials have made statements complaining that the Treaty prohibits Russia, but not some of its neighbors, from developing and possessing ground-launched missiles with ranges between 500 and 5,500 kilometers.

### China

The Chinese People's Liberation Army (PLA) continues to modernize its nuclear missile force by adding more survivable road-mobile systems and enhancing its silo-based systems. This new generation of missiles is intended to ensure the viability of China's strategic deterrent by providing a second-strike capability. China also has tested a hypersonic glide vehicle. In addition, the PLA Navy continues to develop the JL-2 submarine-launched ballistic missile (SLBM) and might produce additional JIN-class nuclear-powered ballistic missile submarines. The JIN-class submarines—armed with JL-2 SLBMs—give the PLA Navy its first long-range, sea-based nuclear capability. The Chinese have also publicized their intent to form a triad by developing a nuclear-capable next-generation bomber.

### Iran and the Joint Comprehensive Plan of Action

Tehran's public statements suggest that it wants to preserve the Joint Comprehensive Plan of Action because it views the JCPOA as a means to remove sanctions while preserving some nuclear capabilities. Iran recognizes that the US Administration has concerns about the deal but expects the other participants—China, the EU, France, Germany, Russia, and the United Kingdom—to honor their commitments. Iran's implementation of the JCPOA has extended the amount of time Iran would need to produce enough fissile material for a nuclear weapon from a few months to about one year, provided Iran continues to adhere to the deal's major provisions. The JCPOA has also enhanced the transparency of Iran's nuclear activities, mainly by fostering improved access to Iranian nuclear facilities for the IAEA and its investigative authorities under the Additional Protocol to its Comprehensive Safeguards Agreement.

Iran's ballistic missile programs give it the potential to hold targets at risk across the region, and Tehran already has the largest inventory of ballistic missiles in the Middle East. Tehran's desire to deter the United States might drive it to field an ICBM. Progress on Iran's space program, such as the launch of the Simorgh SLV in July 2017, could shorten a pathway to an ICBM because space launch vehicles use similar technologies.

#### North Korea

***North Korea will be among the most volatile and confrontational WMD threats to the United States over the next year.*** North Korea's history of exporting ballistic missile technology to several countries, including Iran and Syria, and its assistance during Syria's construction of a nuclear reactor—destroyed in 2007—illustrate its willingness to proliferate dangerous technologies.

In 2017 North Korea, for the second straight year, conducted a large number of ballistic missile tests, including its first ICBM tests. Pyongyang is committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States. It also conducted its sixth and highest yield nuclear test to date.

We assess that North Korea has a longstanding BW capability and biotechnology infrastructure that could support a BW program. We also assess that North Korea has a CW program and probably could employ these agents by modifying conventional munitions or with unconventional, targeted methods.

#### Pakistan

Pakistan continues to produce nuclear weapons and develop new types of nuclear weapons, including short-range tactical weapons, sea-based cruise missiles, air-launched cruise missiles, and longer-range ballistic missiles. These new types of nuclear weapons will introduce new risks for escalation dynamics and security in the region.

#### Syria

We assess that the Syrian regime used the nerve agent sarin in an attack against the opposition in Khan Shaykhun on 4 April 2017, in what is probably the largest chemical weapons attack since August 2013. We continue to assess that Syria has not declared all the elements of its chemical weapons program to the Chemical Weapons Convention (CWC) and that it has the capability to conduct further attacks. Despite the creation of a specialized team and years of work by the Organization for the Prohibition of Chemical Weapons (OPCW) to address gaps and inconsistencies in Syria's declaration, numerous issues remain unresolved. The OPCW-UN Joint Investigative Mechanism (JIM) has attributed the 4 April 2017 sarin attack and three chlorine attacks in 2014 and 2015 to the Syrian regime. Even after the attack on Khan Shaykhun, we have continued to observe allegations that the regime has used chemicals against the opposition.

#### ISIS

We assess that ISIS is also using chemicals as a means of warfare. The OPCW-UN JIM concluded that ISIS used sulfur mustard in two attacks in 2015 and 2016, and we assess that it has used chemical weapons in numerous other attacks in Iraq and Syria.



## TERRORISM

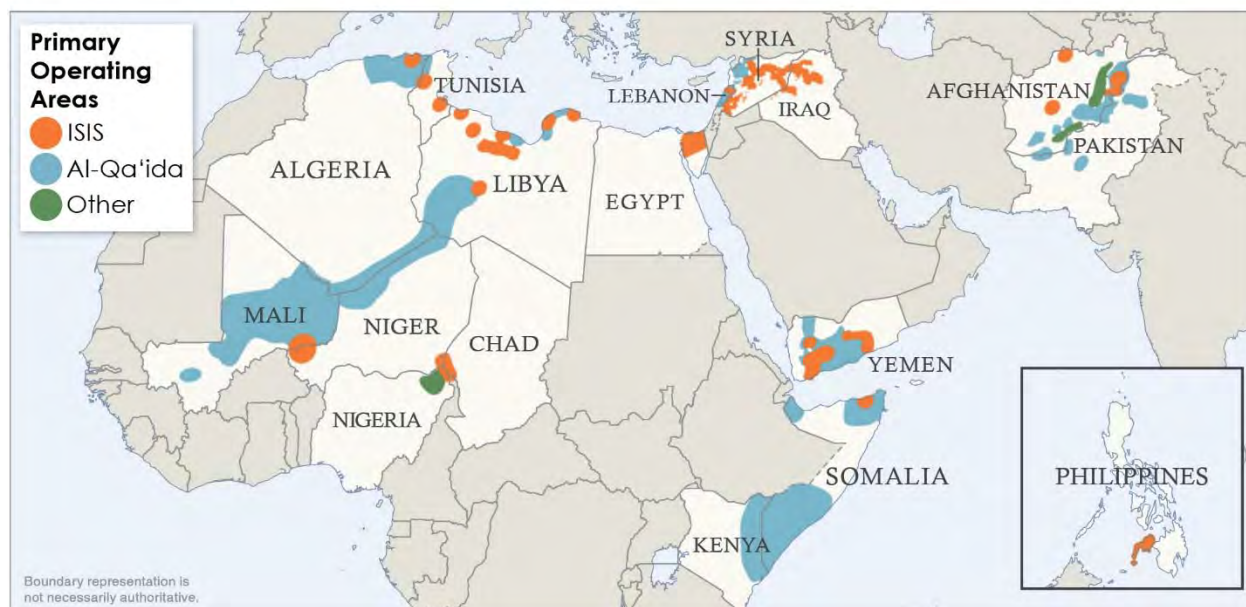
Sunni violent extremists—most notably ISIS and al-Qa‘ida—pose continuing terrorist threats to US interests and partners worldwide, while US-based homegrown violent extremists (HVEs) will remain the most prevalent Sunni violent extremist threat in the United States. Iran and its strategic partner Lebanese Hizballah also pose a persistent threat to the United States and its partners worldwide.

### Sunni Violent Extremism

*Sunni violent extremists are still intent on attacking the US homeland and US interests overseas, but their attacks will be most frequent in or near conflict zones or against enemies that are more easily accessible.*

- Sunni violent extremist groups are geographically diverse; they are likely to exploit conflict zones in the Middle East, Africa, and Asia, where they can co-mingle terrorism and insurgency.
- ISIS and al-Qa‘ida and their respective networks will be persistent threats, as will groups not subordinate to them, such as the Haqqani Taliban Network.

### Sunni Violent Extremists' Primary Operating Areas as of 2017



17-15890 12-17

### ISIS

*Over the next year, we expect that ISIS is likely to focus on regrouping in Iraq and Syria, enhancing its global presence, championing its cause, planning international attacks, and encouraging its members and sympathizers to attack in their home countries.* ISIS's claim of having a functioning caliphate that governs populations is all but thwarted.

- ISIS core has started—and probably will maintain—a robust insurgency in Iraq and Syria as part of a long-term strategy to ultimately enable the reemergence of its so-called caliphate. This activity will challenge local CT efforts against the group and threaten US interests in the region.

- ISIS almost certainly will continue to give priority to transnational terrorist attacks. Its leadership probably assesses that, if ISIS-linked attacks continue to dominate public discourse, the group's narrative will be buoyed, it will be difficult for the counter-ISIS coalition to portray the group as defeated, and the coalition's will to fight will ultimately weaken.
- Outside Iraq and Syria, ISIS's goal of fostering interconnectivity and resiliency among its global branches and networks probably will result in local and, in some cases, regional attack plans.

### Al-Qa'ida

***Al-Qa'ida almost certainly will remain a major actor in global terrorism because of the combined staying power of its five affiliates. The primary threat to US and Western interests from al-Qa'ida's global network through 2018 will be in or near affiliates' operating areas. Not all affiliates will have the intent and capability to pursue or inspire attacks in the US homeland or elsewhere in the West.***

- Al-Qa'ida's affiliates probably will continue to dedicate most of their resources to local activity, including participating in ongoing conflicts in Afghanistan, Somalia, Syria, and Yemen, as well as attacking regional actors and populations in other parts of Africa, Asia, and the Middle East.
- Al-Qa'ida leaders and affiliate media platforms almost certainly will call for followers to carry out attacks in the West, but their appeals probably will not create a spike in inspired attacks. The group's messaging since at least 2010 has produced few such attacks.

### Homegrown Violent Extremists

***Homegrown violent extremists (HVEs) will remain the most prevalent and difficult-to-detect Sunni terrorist threat at home, despite a drop in the number of attacks in 2017.*** HVE attacks are likely to continue to occur with little or no warning because the perpetrators often strike soft targets and use simple tactics that do not require advanced skills or outside training.

- HVEs almost certainly will continue to be inspired by a variety of sources, including terrorist propaganda as well as in response to perceived grievances related to US Government actions.

### Iran and Lebanese Hizballah

Iran remains the most prominent state sponsor of terrorism, providing financial aid, advanced weapons and tactics, and direction to militant and terrorist groups across the Middle East and cultivating a network of operatives across the globe as a contingency to enable potential terrorist attacks.

Lebanese Hizballah has demonstrated its intent to foment regional instability by deploying thousands of fighters to Syria and by providing weapons, tactics, and direction to militant and terrorist groups. Hizballah probably also emphasizes its capability to attack US, Israeli, and Saudi Arabian interests.

## COUNTERINTELLIGENCE AND FOREIGN DENIAL AND DECEPTION

***The United States will face a complex global foreign intelligence threat environment in 2018. We assess that the leading state intelligence threats to US interests will continue to be Russia and China, based on their services' capabilities, intent, and broad operational scope.*** Other states in the Near East, South Asia, East Asia, and Latin America will pose local and regional intelligence threats to US interests. For example, Iranian and Cuban intelligence and security services continue to view the United States as a primary threat.

Penetrating the US national decisionmaking apparatus and the Intelligence Community will remain primary objectives for numerous foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other areas will remain a persistent threat to US interests.

Nonstate entities, including international terrorists and transnational organized crime groups, are likely to continue to employ and improve their intelligence capabilities, including human, technical, and cyber means. As with state intelligence services, these nonstate entities recruit sources and perform physical and technical surveillance to facilitate their illicit activities and to avoid detection and capture.

Trusted insiders who disclose sensitive or classified US Government information without authorization will remain a significant threat in 2018 and beyond. The sophistication and availability of information technology that increases the scope and impact of unauthorized disclosures exacerbate this threat.

### Russia and Influence Campaigns

***Influence operations, especially through cyber means, will remain a significant threat to US interests as they are low-cost, relatively low-risk, and deniable ways to retaliate against adversaries, to shape foreign perceptions, and to influence populations.*** Russia probably will be the most capable and aggressive source of this threat in 2018, although many countries and some nonstate actors are exploring ways to use influence operations, both domestically and abroad.

***We assess that the Russian intelligence services will continue their efforts to disseminate false information via Russian state-controlled media and covert online personas about US activities to encourage anti-US political views.*** Moscow seeks to create wedges that reduce trust and confidence in democratic processes, degrade democratization efforts, weaken US partnerships with European allies, undermine Western sanctions, encourage anti-US political views, and counter efforts to bring Ukraine and other former Soviet states into European institutions.

- Foreign elections are critical inflection points that offer opportunities for Russia to advance its interests both overtly and covertly. The 2018 US mid-term elections are a potential target for Russian influence operations.
- At a minimum, we expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokespeople, and other means of influence to try to exacerbate social and political fissures in the United States.

## EMERGING AND DISRUPTIVE TECHNOLOGY

*New technologies and novel applications of existing technologies have the potential to disrupt labor markets and alter health, energy, and transportation systems.* We assess that technology developments—in the biotechnology and communications sectors, for example—are likely to outpace regulation, which could create international norms that are contrary to US interests and increase the likelihood of technology surprise. Emerging technology and new applications of existing technology will also allow our adversaries to more readily develop weapon systems that can strike farther, faster, and harder and challenge the United States in all warfare domains, including space.

- The widespread proliferation of artificial intelligence (AI)—the field of computer science encompassing systems that seek to imitate aspects of human cognition by learning and making decisions based on accumulated knowledge—is likely to prompt new national security concerns; existing machine learning technology, for example, could enable high degrees of automation in labor-intensive activities such as satellite imagery analysis and cyber defense. Increasingly capable AI tools, which are often enabled by large amounts of data, are also likely to present socioeconomic challenges, including impacts on employment and privacy.
- New biotechnologies are leading to improvements in agriculture, health care, and manufacturing. However, some applications of biotechnologies may lead to unintentional negative health effects, biological accidents, or deliberate misuse.
- The global shift to advanced information and communications technologies (ICT) will increasingly test US competitiveness because aspiring suppliers around the world will play a larger role in developing new technologies and products. These technologies include next-generation, or 5G, wireless technology; the internet of things; new financial technologies; and enabling AI and big data for predictive analysis. Differences in regulatory and policy approaches to ICT-related issues could impede growth and innovation globally and for US companies.
- Advanced materials could disrupt the economies of some commodities-dependent exporting countries while providing a competitive edge to developed and developing countries that create the capacity to produce and use the new materials. New materials, such as nanomaterials, are often developed faster than their health and environmental effects can be assessed. Advances in manufacturing, particularly the development of 3D printing, almost certainly will become even more accessible to a variety of state and nonstate actors and be used in ways contrary to our interests.

## TECHNOLOGY ACQUISITIONS AND STRATEGIC ECONOMIC COMPETITION

*Persistent trade imbalances, trade barriers, and a lack of market-friendly policies in some countries probably will continue to challenge US economic security. Some countries almost certainly will continue to acquire US intellectual property and proprietary information illicitly to advance their own economic and national security objectives.*

- China, for example, has acquired proprietary technology and early-stage ideas through cyber-enabled means. At the same time, some actors use largely legitimate, legal transfers and

relationships to gain access to research fields, experts, and key enabling industrial processes that could, over time, erode America's long-term competitive advantages.

## SPACE AND COUNTERSPACE

Continued global space industry expansion will further extend space-enabled capabilities and space situational awareness to nation-state, nonstate, and commercial space actors in the coming years, enabled by the increased availability of technology, private-sector investment, and growing international partnerships for shared production and operation. All actors will increasingly have access to space-derived information services, such as imagery, weather, communications, and positioning, navigation, and timing for intelligence, military, scientific, or business purposes. Foreign countries—particularly China and Russia—will continue to expand their space-based reconnaissance, communications, and navigation systems in terms of the numbers of satellites, the breadth of their capability, and the applications for use.

Both Russia and China continue to pursue antisatellite (ASAT) weapons as a means to reduce US and allied military effectiveness. Russia and China aim to have nondestructive and destructive counterspace weapons available for use during a potential future conflict. We assess that, if a future conflict were to occur involving Russia or China, either country would justify attacks against US and allied satellites as necessary to offset any perceived US military advantage derived from military, civil, or commercial space systems. Military reforms in both countries in the past few years indicate an increased focus on establishing operational forces designed to integrate attacks against space systems and services with military operations in other domains.

Russian and Chinese destructive ASAT weapons probably will reach initial operational capability in the next few years. China's PLA has formed military units and begun initial operational training with counterspace capabilities that it has been developing, such as ground-launched ASAT missiles. Russia probably has a similar class of system in development. Both countries are also advancing directed-energy weapons technologies for the purpose of fielding ASAT weapons that could blind or damage sensitive space-based optical sensors, such as those used for remote sensing or missile defense.

Of particular concern, Russia and China continue to launch "experimental" satellites that conduct sophisticated on-orbit activities, at least some of which are intended to advance counterspace capabilities. Some technologies with peaceful applications—such as satellite inspection, refueling, and repair—can also be used against adversary spacecraft.

Russia and China continue to publicly and diplomatically promote international agreements on the nonweaponization of space and "no first placement" of weapons in space. However, many classes of weapons would not be addressed by such proposals, allowing them to continue their pursuit of space warfare capabilities while publicly maintaining that space must be a peaceful domain.

## TRANSNATIONAL ORGANIZED CRIME

*Transnational organized criminal groups and networks will pose serious and growing threats to the security and health of US citizens, as well as to global human rights, ecological integrity, government revenues, and efforts to deal with adversaries and terrorists. In the most severe cases abroad, criminal enterprises will*



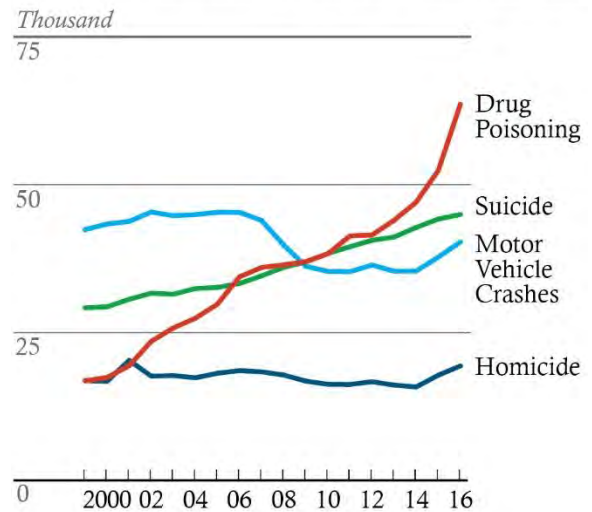
*contribute to increased social violence, erode governments' authorities, undermine the integrity of international financial systems, and harm critical infrastructure.*

### Drug Trafficking

***Transnational organized criminal groups supply the dominant share of illicit drugs consumed in the United States, fueling high mortality rates among US citizens.***

- Americans in 2016 died in record numbers from drug overdoses, 21 percent more than in 2015.
- Worldwide production of cocaine, heroin, and methamphetamine is at record levels. US mortality from potent synthetic opioids doubled in 2016, and synthetic opioids have become a key cause of US drug deaths.
- Mexican criminal groups will continue to supply much of the heroin, methamphetamine, cocaine, and marijuana that cross the US-Mexico border, while China-based suppliers ship fentanyl and fentanyl precursors to Mexico-, Canada-, and US-based distributors or sell directly to consumers via the Internet.

**Causes of US Premature Deaths, 1999-2016**



Source: US Centers for Disease Control and Prevention.

17-15892 12-17

### Broader Threats From Transnational Crime

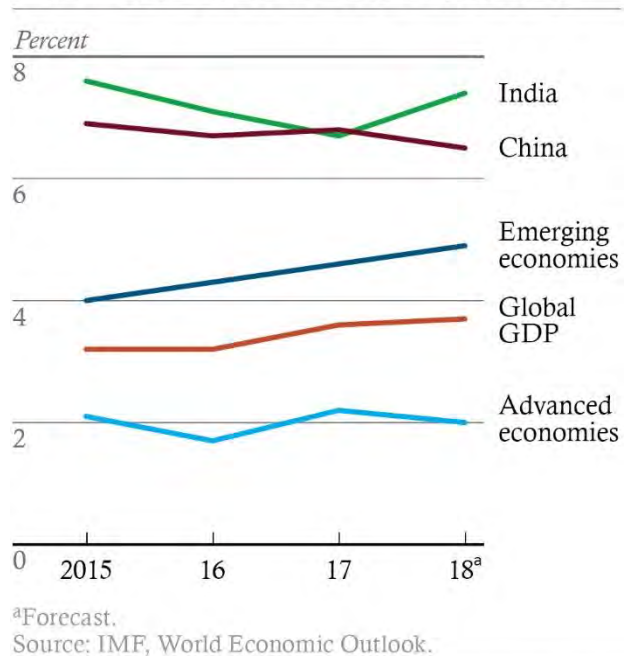
***Transnational organized criminal groups, in addition to engaging in violence, will continue to traffic in human beings, deplete natural resources, and siphon money from governments and the global economy.***

- Human trafficking will continue in virtually every country. International organizations estimate that about 25 million people are victims.
- The FBI assesses that US losses from cybercrime in 2016 exceeded \$1.3 billion, and some industry experts predict such losses could cost the global economy \$6 trillion by 2021.
- Criminal wildlife poaching, illegal fishing, illicit mining, and drug-crop production will continue to threaten economies, biodiversity, food supply security, and human health. For example, academic studies show that illicit mining alone adds some 650 to 1,000 tons of toxic mercury to the ecosystem each year.
- Transnational organized criminal groups probably will generate more revenue from illicit activity in the coming year, which the UN last estimated at \$1.6-\$2.2 trillion for 2014.

## ECONOMICS AND ENERGY

*Global growth in 2018—projected by the IMF to rise to 3.9 percent—is likely to become more broadly based, but growth remains weak in many countries, and inflation is below target in most advanced economies.* The relatively favorable outlook for real economic growth suggests little near-term risk of unfavorable deficit-debt dynamics among the advanced economies. Supportive financial conditions and improving business sentiment will help to drive economic activity in advanced countries. China's growth may decelerate as the property sector cools and if Beijing accelerates economic reforms. India's economy is expected to rebound after headwinds from taxation changes and demonetization, and the continuing upswing in emerging and developing economies could be tempered by capital outflows from a stronger dollar and monetary policy normalization in the United States and Europe.

Worldwide Economic Growth, 2015-18



17-15891 12-17

*Oil-exporting countries continue to suffer from the late-2014 oil price drop, and their economic woes are likely to continue, with broader negative implications.* Subdued economic growth, combined with sharp increases in North American oil and gas production, probably will continue putting downward pressure on global energy prices, harming oil-exporting economies. The US Energy Information Administration forecasts that 2018 West Texas Intermediate and Brent prices will average \$58 and \$62 per barrel, respectively, far below the average annual prices of \$98 and \$109 in 2013.

- Low oil prices and production declines—along with poor economic policies—have pushed Venezuela and the state-owned oil company, Petroleos de Venezuela, to miss debt payments, putting them in selective default.
- Saudi Arabia and other Persian Gulf oil exporters have experienced sharp increases in budget deficits, forcing governments to issue debt and enact politically unpopular fiscal reforms, such as cuts to subsidies, social programs, and government jobs.
- In Africa, declining oil revenue, mismanagement, and inadequate policy responses to oil price shocks have contributed to Angolan and Nigerian fiscal problems, currency strains, and deteriorating foreign exchange reserves.
- OPEC member countries and select non-OPEC producers, including Russia, in early 2017 committed to cut oil production in order to lift prices, with compliance likely to be offset somewhat as Libya or Nigeria—both are exempt from the deal—are able to resume production.

## HUMAN SECURITY

***Governance shortfalls, violent conflict, environmental stresses, and increased potential for a global health crisis will create significant risks to human security, including high levels of human displacement and migration flows.***

### Governance and Political Turbulence

***Domestic and foreign challenges to democracy and institutional capacity will test governance quality globally in 2018***, especially as competitors manipulate social media to shape opinion. Freedom House reported the 11th consecutive year of decline in “global freedom” in 2017, and nearly one-quarter of the countries registering declines were in Europe.

- While the number of democracies has remained steady for the past decade, some scholars suggest the quality of democracy has declined.
- We note that more governments are using propaganda and misinformation in social media to influence foreign and domestic audiences.
- The number and sophistication of government efforts to shape domestic views of politics have increased dramatically in the past 10 years. In 2016, Freedom House identified 30 countries, including the Philippines, Turkey, and Venezuela, whose governments used social media to spread government views, to drive agendas, and to counter criticism of the government online.

***Poor governance, weak national political institutions, economic inequality, and the rise of violent nonstate actors all undermine states’ abilities to project authority and elevate the risk of violent—even regime-threatening—instability and mass atrocities.***

### Environment and Climate Change

***The impacts of the long-term trends toward a warming climate, more air pollution, biodiversity loss, and water scarcity are likely to fuel economic and social discontent—and possibly upheaval—through 2018.***

- The past 115 years have been the warmest period in the history of modern civilization, and the past few years have been the warmest years on record. Extreme weather events in a warmer world have the potential for greater impacts and can compound with other drivers to raise the risk of humanitarian disasters, conflict, water and food shortages, population migration, labor shortfalls, price shocks, and power outages. Research has not identified indicators of tipping points in climate-linked earth systems, suggesting a possibility of abrupt climate change.
- Worsening air pollution from forest burning, agricultural waste incineration, urbanization, and rapid industrialization—with increasing public awareness—might drive protests against authorities, such as those recently in China, India, and Iran.
- Accelerating biodiversity and species loss—driven by pollution, warming, unsustainable fishing, and acidifying oceans—will jeopardize vital ecosystems that support critical human systems. Recent estimates suggest that the current extinction rate is 100 to 1,000 times the natural extinction rate.

- Water scarcity, compounded by gaps in cooperative management agreements for nearly half of the world's international river basins, and new unilateral dam development are likely to heighten tension between countries.

### Human Displacement

*Global displacement almost certainly will remain near record highs during the next year, raising the risk of disease outbreaks, recruitment by armed groups, political upheaval, and reduced economic productivity.* Conflicts will keep many of the world's refugees and internally displaced persons from returning home.

### Health

*The increase in frequency and diversity of reported disease outbreaks—such as dengue and Zika—probably will continue through 2018, including the potential for a severe global health emergency that could lead to major economic and societal disruptions, strain governmental and international resources, and increase calls on the United States for support. A novel strain of a virulent microbe that is easily transmissible between humans continues to be a major threat, with pathogens such as H5N1 and H7N9 influenza and Middle East Respiratory Syndrome Coronavirus having pandemic potential if they were to acquire efficient human-to-human transmissibility.*

- The frequency and diversity of disease outbreaks have increased at a steady rate since 1980, probably fueled by population growth, travel and trade patterns, and rapid urbanization. Ongoing global epidemics of HIV/AIDS, malaria, and tuberculosis continue to kill millions of people annually.
- Increasing antimicrobial resistance, the ability of pathogens—including viruses, fungi, and bacteria—to resist drug treatment, is likely to outpace the development of new antimicrobial drugs, leading to infections that are no longer treatable.
- The areas affected by vector-borne diseases, including dengue, are likely to expand, especially as changes in climatological patterns increase the reach of the mosquito.
- The World Bank has estimated that a severe global influenza pandemic could cost the equivalent of 4.8 percent of global GDP—more than \$3 trillion—and cause more than 100 million deaths.

## REGIONAL THREATS

### EAST ASIA

#### China

***China will continue to pursue an active foreign policy—especially in the Asia Pacific region—highlighted by a firm stance on its sovereignty claims in the East China Sea (ECS) and South China Sea (SCS), its relations with Taiwan, and its pursuit of economic engagement across the region.*** Regional tension will persist due to North Korea's nuclear and missile programs and simmering tension over territorial and maritime disputes in the ECS and SCS. China will also pursue efforts aimed at fulfilling its ambitious Belt and Road Initiative to expand China's economic reach and political influence across Eurasia, Africa, and the Pacific through infrastructure projects.

#### North Korea

North Korea's weapons of mass destruction program, public threats, defiance of the international community, confrontational military posturing, cyber activities, and potential for internal instability pose a complex and increasing threat to US national security and interests.

***In the wake of accelerated missile testing since 2016, North Korea is likely to press ahead with more tests in 2018, and its Foreign Minister said that Kim may be considering conducting an atmospheric nuclear test over the Pacific Ocean.*** Pyongyang's commitment to possessing nuclear weapons and fielding capable long-range missiles, all while repeatedly stating that nuclear weapons are the basis for its survival, suggests that the regime does not intend to negotiate them away.

Ongoing, modest improvements to North Korea's conventional capabilities continue to pose a serious and growing threat to South Korea and Japan. Despite the North Korean military's many internal challenges and shortcomings, Kim Jong Un continues to expand the regime's conventional strike options with more realistic training, artillery upgrades, and close-range ballistic missiles that improve North Korea's ability to strike regional US and allied targets with little warning.

#### Southeast Asia

***Democracy and human rights in many Southeast Asian countries will remain fragile in 2018 as autocratic tendencies deepen in some regimes and rampant corruption and cronyism undermine democratic values.*** Countries in the region will struggle to preserve foreign policy autonomy in the face of Chinese economic and diplomatic coercion.

- Cambodian leader Hun Sen will repress democratic institutions and civil society, manipulate government and judicial institutions, and use patronage and political violence to guarantee his rule beyond the 2018 national election. Having alienated Western partners, Hun Sen will rely on Beijing's political and financial support, drawing Cambodia closer to China as a result.
- The crisis resulting from the exodus of more than 600,000 Rohingyas from Burma to Bangladesh will threaten Burma's fledgling democracy, increase the risk of violent extremism, and provide openings for Beijing to expand its influence.



- ***In the Philippines, President Duterte will continue to wage his signature campaign against drugs, corruption, and crime.*** Duterte has suggested he could suspend the Constitution, declare a “revolutionary government,” and impose nationwide martial law. His declaration of martial law in Mindanao, responding to the ISIS-inspired siege of Marawi City, has been extended through the end of 2018.
- ***Thailand’s leaders have pledged to hold elections in late 2018, but the new Constitution will institutionalize the military’s influence.***

## MIDDLE EAST AND NORTH AFRICA

### Iran

***Iran will seek to expand its influence in Iraq, Syria, and Yemen, where it sees conflicts generally trending in Tehran’s favor,*** and it will exploit the fight against ISIS to solidify partnerships and translate its battlefield gains into political, security, and economic agreements.

- Iran’s support for the Popular Mobilization Committee (PMC) and Shia militants remains the primary threat to US personnel in Iraq. We assess that this threat will increase as the threat from ISIS recedes, especially given calls from some Iranian-backed groups for the United States to withdraw and growing tension between Iran and the United States.
- In Syria, Iran is working to consolidate its influence while trying to prevent US forces from gaining a foothold. Iranian-backed forces are seizing routes and border crossings to secure the Iraq-Syria border and deploying proregime elements and Iraqi allies to the area. Iran’s retaliatory missile strikes on ISIS targets in Syria following ISIS attacks in Tehran in June were probably intended in part to send a message to the United States and its allies about Iran’s improving military capabilities. Iran is pursuing permanent military bases in Syria and probably wants to maintain a network of Shia foreign fighters in Syria to counter future threats to Iran. Iran also seeks economic deals with Damascus, including deals on telecommunications, mining, and electric power repairs.
- In Yemen, Iran’s support to the Huthis further escalates the conflict and poses a serious threat to US partners and interests in the region. Iran continues to provide support that enables Huthi attacks against shipping near the Bab al Mandeb Strait and land-based targets deep inside Saudi Arabia and the UAE, such as the 4 November and 19 December ballistic missile attacks on Riyadh and an attempted 3 December cruise missile attack on an unfinished nuclear reactor in Abu Dhabi.

***Iran will develop military capabilities that threaten US forces and US allies in the region, and its unsafe and unprofessional interactions will pose a risk to US Navy operations in the Persian Gulf.***

Iran continues to develop and improve a range of new military capabilities to target US and allied military assets in the region, including armed UAVs, ballistic missiles, advanced naval mines, unmanned explosive boats, submarines and advanced torpedoes, and antiship and land-attack cruise missiles. Iran has the largest ballistic missile force in the Middle East and can strike targets up to 2,000 kilometers from Iran’s borders. Russia’s delivery of the SA-20c SAM system in 2016 has provided Iran with its most advanced long-range air defense system.

- Islamic Revolutionary Guard Corps (IRGC) Navy forces operating aggressively in the Persian Gulf and Strait of Hormuz pose a risk to the US Navy. Most IRGC interactions with US ships are professional, but as of mid-October, the Navy had recorded 14 instances of what it describes as “unsafe and/or unprofessional” interactions with Iranian forces during 2017, the most recent interaction occurring last August, when an unarmed Iranian drone flew close to the aircraft carrier USS Nimitz as fighter jets landed at night. The Navy recorded 36 such incidents in 2016 and 22 in 2015. Most involved the IRGC Navy. We assess that these interactions, although less frequent, will continue and that they are probably intended to project an image of strength and, possibly, to gauge US responses.

***Iranian centrist and hardline politicians increasingly will clash as they attempt to implement competing visions for Iran’s future.*** This contest will be a key driver in determining whether Iran changes its behavior in ways favorable to US interests.

- Centrists led by President Hasan Ruhani will continue to advocate greater social progress, privatization, and more global integration, while hardliners will view this agenda as a threat to their political and economic interests and to Iran’s revolutionary and Islamic character.
- Supreme Leader Ali Khamenei’s views are closer to those of the hardliners, but he has supported some of Ruhani’s efforts to engage Western countries and to promote economic growth. The Iranian economy’s prospects—still driven heavily by petroleum revenue—will depend on reforms to attract investment, strengthen privatization, and grow nonoil industries, which Ruhani will continue pursuing, much to the dismay of hardliners. National protests over economic grievances in Iran earlier this year have drawn more attention to the need for major reforms, but Ruhani and his critics are likely to use the protests to advance their political agendas.
- Khamenei has experienced health problems in the past few years, and, in an effort to preserve his legacy, he probably opposes moving Iran toward greater political and economic openness. As their relationship has deteriorated since the presidential election last June, Ruhani has tried to mend relations with Khamenei as well as his allies, but, in doing so, he risks failing to make progress on reforms in the near-term.

## Syria

***The conflict has decisively shifted in the Syrian regime’s favor, enabling Russia and Iran to further entrench themselves inside the country. Syria is likely to experience episodic conflict through 2018, even as Damascus recaptures most of the urban terrain and the overall level of violence decreases.***

- ***The Syrian opposition’s seven-year insurgency is probably no longer capable of overthrowing President Bashar al-Asad or overcoming a growing military disadvantage.*** Rebels probably retain the resources to sustain the conflict for at least the next year.
- ISIS is likely on a downward trajectory in Syria; yet, despite territorial losses, it probably possesses sufficient resources, and a clandestine network in Syria, to sustain insurgency operations through 2018.

- Moscow probably cannot force President Asad to agree to a political settlement that he believes significantly weakens him, unless Moscow is willing to remove Asad by force. While Asad may engage in peace talks, he is unlikely to negotiate himself from power or offer meaningful concessions to the opposition.
- Russia and Iran are planning for a long-term presence, securing military basing rights and contracts for reconstruction and oil and gas exploitation. Iran is also seeking to establish a land corridor from Iran through Syria to Lebanon. The Kurdish People's Protection Unit—the Syrian militia of the Kurdistan Workers' Party (PKK)—probably will seek some form of autonomy but will face resistance from Russia, Iran, and Turkey.
- As of October 2017, there were more than 5 million Syrian refugees in neighboring countries, and an estimated 6.3 million internally displaced. Reconstruction could cost at least \$100 billion and take at least 10 years to complete. Asad's battered economy will likely continue to require significant subsidies from Iran and Russia to meet basic expenses.

#### Iraq

***Iraq is likely to face a lengthy period of political turmoil and conflict as it struggles to rebuild, reconstitute the Iraqi state, maintain pressure on ISIS, and rein in the Iranian-backed Shia militias that pose an enduring threat to US personnel.***

- The Iraqi Government, which has accrued \$120 billion in debt, requires substantial external assistance to cover hundreds of millions of dollars in humanitarian-aid shortfalls and a World Bank estimated \$88.2 billion to restore heavily damaged infrastructure, industry, and service sectors in areas retaken from ISIS.
- Prime Minister Haydar al-Abadi's forceful reassertion of Baghdad's authority after the Kurdistan Regional Government's (KRG) independence referendum in September illustrates the divisions among Iraqi leaders over the future of the state. The move to curb Kurdish autonomy was popular among many Arab Shia and Sunnis and may prompt Iraqi leaders to be uncompromising in political reconciliation discussions in order to consolidate votes in the run-up to elections planned for next spring.
- ISIS will remain a terrorist and insurgent threat, and the group will seek to exploit Sunni discontent to conduct attacks and try to regain Iraqi territory. Baghdad will struggle to reorient the Iraqi Security Forces (ISF) from conventional warfare to counterinsurgency and counterterrorism against ISIS while consolidating state control of territory and integrating the Iranian-backed and Shia-dominated Popular Mobilization Committee (PMC).
- There is an increasing risk that some Shia militants will seek to attack US targets in Iraq because they believe that the US security presence is no longer needed, want to reassert Iraqi sovereignty, and support Iran's goal of reducing US influence in Iraq.

Baghdad will have to contend with longstanding and war-hardened ethnosectarian divisions between Shia, Sunnis, and Kurds that were kept in check by the threat from ISIS. Despite ISIS's loss of territory, the social and political challenges that gave rise to the group remain and threaten the cohesion of the Iraqi state.

## Yemen

The war in Yemen is likely to continue for the foreseeable future because the Iranian-backed Huthis and the Saudi-led coalition remain far apart on terms for ending the conflict. The death of former Yemeni President Ali Abdallah Salih is only likely to further complicate the conflict as the Huthis and others scramble to win over those who previously backed Salih. We assess that the Huthis will continue to pursue their goals militarily and that, as a result, US allies and interests on the Arabian Peninsula will remain at risk of Huthi missile attacks until the conflict is resolved.

- Continued fighting almost certainly will worsen the vast humanitarian crisis, which has left more than 70 percent of the population—or about 20 million people—in need of assistance and aggravated a cholera outbreak that has reached nearly 1 million confirmed cases. Relief operations are hindered by security and bureaucratic constraints established by both the Huthi-Salih alliance and the Saudi-led coalition and by international funding shortages.

## SOUTH ASIA

### Afghanistan

*The overall situation in Afghanistan probably will deteriorate modestly this year in the face of persistent political instability, sustained attacks by the Taliban-led insurgency, unsteady Afghan National Security Forces (ANSF) performance, and chronic financial shortfalls.* The National Unity Government probably will struggle to hold long-delayed parliamentary elections, currently scheduled for July 2018, and to prepare for a presidential election in 2019. The ANSF probably will maintain control of most major population centers with coalition force support, but the intensity and geographic scope of Taliban activities will put those centers under continued strain. Afghanistan's economic growth will stagnate at around 2.5 percent per year, and Kabul will remain reliant on international donors for the great majority of its funding well beyond 2018.

South Asian Threats Challenge  
US Security Interests in 2018



Boundary representation is  
not necessarily authoritative.

17-15888 1-18

### Pakistan

*Pakistan will continue to threaten US interests by deploying new nuclear weapons capabilities, maintaining its ties to militants, restricting counterterrorism cooperation, and drawing closer to*

*China.* Militant groups supported by Islamabad will continue to take advantage of their safe haven in Pakistan to plan and conduct attacks in India and Afghanistan, including against US interests. Pakistan's perception of its eroding position relative to India, reinforced by endemic economic weakness and domestic security issues, almost certainly will exacerbate long-held fears of isolation and drive Islamabad's pursuit of actions that run counter to US goals for the region.

### India-Pakistan Tension

*Relations between India and Pakistan are likely to remain tense, with continued violence on the Line of Control and the risk of escalation if there is another high-profile terrorist attack in India or an uptick in violence on the Line of Control.*

### India-China Tension

*We expect relations between India and China to remain tense and possibly to deteriorate further, despite the negotiated settlement to their three-month border standoff in August, elevating the risk of unintentional escalation.*

### Bangladesh-Burma Rohingya Crisis

*The turmoil resulting from more than 600,000 Rohingyas fleeing from Burma to Bangladesh increases regional tension and may expand opportunities for terrorist recruitment in South and Southeast Asia. Further operations by Burmese security forces against Rohingya insurgents or sustained violence by ethnic Rakhine militias probably would make it difficult to repatriate Burmese from Bangladesh.*

## RUSSIA AND EURASIA

### Russia

*In his probable next term in office, President Vladimir Putin will rely on assertive and opportunistic foreign policies to shape outcomes beyond Russia's borders. He will also resort to more authoritarian tactics to maintain control amid challenges to his rule.*

Moscow will seek cooperation with the United States in areas that advance its interests. Simultaneously, Moscow will employ a variety of aggressive tactics to bolster its standing as a great power, secure a "sphere of influence" in the post-Soviet space, weaken the United States, and undermine Euro-Atlantic unity. The highly personalized nature of the Russian political system will enable Putin to act decisively to defend Russian interests or to pursue opportunities he views as enhancing Russian prestige and power abroad.

Russia will compete with the United States most aggressively in Europe and Eurasia, while applying less intense pressure in "outer areas" and cultivating partnerships with US rivals and adversaries—as well as with traditional US partners—to constrain US power and accelerate a shift toward a "multipolar" world. Moscow will use a range of relatively low-cost tools to advance its foreign policy objectives, including influence campaigns, economic coercion, cyber operations, multilateral forums, and measured military force. Russia's slow

### Economic and Military Affiliations in Russia's Neighborhood



17-15889 12-17



economic growth is unlikely to constrain Russian foreign policy or by itself trigger concessions from Moscow in Ukraine, Syria, or elsewhere in the next year.

President Putin is likely to increase his use of repression and intimidation to contend with domestic discontent over corruption, poor social services, and a sluggish economy with structural deficiencies. He will continue to manipulate the media, distribute perks to maintain elite support, and elevate younger officials to convey an image of renewal. He is also likely to expand the government's legal basis for repression and to enhance his capacity to intimidate and monitor political threats, perhaps using the threat of "extremism" or the 2018 World Cup to justify his actions.

In 2018, Russia will continue to modernize, develop, and field a wide range of advanced nuclear, conventional, and asymmetric capabilities to balance its perception of a strategic military inferiority vis-a-vis the United States.

## Ukraine

***Ukraine remains at risk of domestic turmoil, which Russia could exploit to undermine Kyiv's pro-West orientation.*** These factors will threaten Ukraine's nascent economic recovery and potentially lead to changes in its foreign policy that further inflame tension between Russia and the West.

- Popular frustrations with the pace of reforms, depressed standards of living, perceptions of worsening corruption, and political polarization ahead of scheduled presidential and legislative elections in 2019 could prompt early elections.
- Opposition leaders will seek to capitalize on popular discontent to weaken President Petro Poroshenko and the ruling coalition ahead of elections in 2019.

***The conflict in eastern Ukraine is likely to remain stalemated and marked by fluctuating levels of violence. A major offensive by either side is unlikely in 2018, although each side's calculus could change if it sees the other as seriously challenging the status quo.*** Russia will continue its military, political, and economic destabilization campaign against Ukraine to stymie and, where possible, reverse Kyiv's efforts to integrate with the EU and strengthen ties to NATO. Kyiv will strongly resist concessions to Moscow but almost certainly will not regain control of Russian-controlled areas of eastern Ukraine in 2018. Russia will modulate levels of violence to pressure Kyiv and shape negotiations in Moscow's favor.

- Russia will work to erode Western unity on sanctions and support for Kyiv, but the Kremlin is coping with sanctions at existing levels.

## Belarus, the Caucasus, Central Asia, Moldova

***The Kremlin will seek to maintain and, where possible, expand its influence throughout the former Soviet countries that it asserts are in its self-described sphere of influence.***

Russia views Belarus as a critical buffer between itself and NATO and will seek to spoil any potential warming between Minsk and the West. Belarus President Aleksandr Lukashenko will continue close security cooperation with Moscow but will continue to aim for normalized relations with the West as a check on Russia's influence.

Russia's continued occupation of 20 percent of Georgia's territory and efforts to undermine its Western integration will remain the primary sources of Tbilisi's insecurity. The ruling Georgian Dream party is likely to seek to stymie the opposition and reduce institutional constraints on its power.

Tension over the disputed region of Nagorno-Karabakh could devolve into a large-scale military conflict between Armenia and Azerbaijan, which could draw in Russia to support its regional ally. Both sides' reluctance to compromise, mounting domestic pressures, Azerbaijan's steady military modernization, and Armenia's acquisition of new Russian equipment sustain the risk of large-scale hostilities in 2018.

Russia will pressure Central Asia's leaders to reduce engagement with Washington and support Russian-led economic and security initiatives, while concerns about ISIS in Afghanistan will push Moscow to strengthen its security posture in the region. Poor governance and weak economies raise the risk of radicalization—especially among the many Central Asians who travel to Russia or other countries for work—presenting a threat to Central Asia, Russia, and Western societies. China will probably continue to expand outreach to Central Asia—while deferring to Russia on security and political matters—because of concern that regional instability could undermine China's economic interests and create a permissive environment for extremists, which, in Beijing's view, could enable Uighur militant attacks in China.

Moldova's ostensibly pro-European ruling coalition—unless it is defeated in elections planned for November—probably will seek to curb Russian influence and maintain a veneer of European reform while avoiding changes that would damage the coalition's grip on power. The current Moldovan Government probably will move forward on implementing Moldova's EU Association Agreement against the will of openly pro-Russian and Russian-backed President Igor Dodon. Settlement talks over the breakaway region of Transnistria will continue, but progress likely will be limited to small issues.

## EUROPE

*The European Union and European national governments will struggle to develop common approaches to counter a variety of security challenges, including instability on their periphery, irregular migration to their region, heightened terrorist threats, and Russian influence campaigns, undercutting Western cohesion.*

- These concerns are spurring many countries to increase defense spending and enhance capabilities.
- European governments will need to strengthen their counterterrorism regimes to deal with a diverse threat, including ISIS aspirants and returning foreign fighters.

Turkey's counterterrorism cooperation with the United States against ISIS is likely to continue, but thwarting Kurdish regional ambitions will be a foreign policy priority. President Recep Tayyip Erdogan is likely to employ polarizing rhetoric, straining bilateral relations and cooperation on shared regional goals.

## AFRICA

***Nigeria—the continent's largest economy—will face a security threat from Boko Haram and ISIS West Africa (ISIS-WA) while battling internal challenges from criminal, militant, and secessionist groups.***

ISIS-WA and Boko Haram are regional menaces, conducting cross-border attacks in Nigeria, Cameroon, Chad, and Niger and posing a threat to Western interests. Meanwhile, militant and secessionist groups in the southern and central areas of Nigeria are capitalizing on longstanding social and economic grievances as the country nears the 2019 presidential election.

***Politically fragile governments in Africa's Sahel region will remain vulnerable to terror attacks in 2018, despite efforts to coordinate their counterterror operations.*** ISIS and al-Qa'ida-allied groups, along with other violent extremists, will attempt to target Western and local government interests in the region, and a stalled peace process is likely to undercut the presidential election in Mali.

***The Ethiopian and Kenyan Governments are likely to face opposition from publics agitating for redress of political grievances. Somalia's recently elected government probably will struggle to project its authority and implement security reforms amid the drawdown of African Union forces in 2018, while al-Shabaab—the most potent terrorist threat to US interests in East Africa—probably will increase attacks.***

***Clashes between the South Sudanese Government and armed opposition groups will continue, raising the risk of additional mass atrocities as both sides use ethnic militias and hate speech and the government continues its crackdown on ethnic minorities.*** The South Sudanese are the world's fastest growing refugee population, and the significant humanitarian challenges stemming from the conflict, including severe food insecurity, will strain the resources of neighboring countries hosting refugees.

***Sudan is likely to continue some aspects of its constructive engagement with the United States following the suspension of sanctions because it has given priority to shedding its international pariah status and reviving its economy.*** Khartoum probably will acquiesce to some US requests, such as increasing counterterrorism cooperation and improving humanitarian access, but will be reluctant to take any steps that it perceives jeopardize its national security interests.

***Political unrest and security threats across the region are likely to intensify as the Presidents of Burundi and the Democratic Republic of the Congo (DRC) face public and armed opposition to their rule and the Central African Republic (CAR) struggles to cope with a nationwide surge in conflict.*** Over-stretched UN missions in CAR and DRC are unlikely to stem the rising challenges from their concurrent humanitarian and security crises.

## THE WESTERN HEMISPHERE

*A key feature of the 2018 political environment in Latin America almost certainly will be popular frustration with low economic growth, corruption scandals, and the specter of endemic criminal activity in some countries.* Larger and increasingly sophisticated middle classes—with greater access to social media—are demanding more accountability from their governments. Presidential elections, including those in Mexico and Colombia, will occur at a time when support for political parties and governing institutions is at record lows and could bolster the appeal of outsider candidates.

### Mexico

Mexicans are focused on presidential and legislative elections scheduled for July 2018, in which corruption, high violence, and a tepid economy will be key issues. The Mexican Government has made slow progress implementing rule-of-law reforms and will continue to rely on the military to lead counternarcotics efforts. Mexico's \$1.1 trillion economy benefits from strong economic fundamentals, but uncertainty over trade relationships and higher-than-expected inflation could further slow economic growth. President Enrique Peña Nieto is focusing on domestic priorities, including recovery from the September 2017 earthquakes and managing impacts from potential US policy shifts ahead of the elections. In recent years, Mexican US-bound migration has been net negative but might increase if economic opportunity at home declined.

### Central America

Insecurity and lack of economic opportunities likely will remain the principal drivers of irregular migration from the Northern Triangle countries of El Salvador, Guatemala, and Honduras. Homicide rates in these countries remain high, and gang-related violence is still prompting Central Americans to flee.

### Venezuela

Economic woes and international diplomatic pressure probably will put political pressure on the Venezuelan Government in 2018. Living standards have declined and shortages of basic goods are driving the increase in Venezuelans seeking asylum in the United States and the region. Venezuela's negotiations with creditors probably will lead to messy legal battles. Venezuela almost certainly will seek to minimize further disruptions to oil production and exports to maintain its critical oil export earnings. Oil prices have increased slightly this year, but crude oil production continues to decline.

### Colombia

President Juan Manuel Santos will seek to cement implementation of the Revolutionary Armed Forces of Colombia (FARC) peace accord, as campaigning intensifies for the May 2018 presidential election. The FARC's new political-party status and the uncertainty around the transitional justice reforms will be a factor in the political environment ahead of elections. Substantial budget constraints will slow major programs or policy changes. The influx of FARC dissidents, drug traffickers, and other illegal actors into remote areas will challenge security forces during the next 12 months. Cocaine production in Colombia is at an all-time high, and crop substitution and eradication programs are facing stiff local resistance.

## Cuba

Havana will seek to manage President Raul Castro's planned retirement in April 2018. Castro's successor will inherit a stagnant economy and a stalled economic reform process.

## Haiti

As President Jovenel Moise begins his second year in office, he will confront competing interests within his government, a vocal opposition, and a fragile economy. Crime and protest activity will test the Haitian National Police following the departure of the UN Stabilization Mission in October 2017 and the transition to a police-only UN mission.



# EXHIBIT 7

## **Statement for the Record**

# **Worldwide Threat Assessment of the US Intelligence Community**

**Senate Select Committee on Intelligence**



**Daniel R. Coats**

**Director of National Intelligence**

**May 11, 2017**

**STATEMENT FOR THE RECORD**  
**WORLDWIDE THREAT ASSESSMENT**  
**of the**  
**US INTELLIGENCE COMMUNITY**

May 11, 2017

---

**INTRODUCTION**

---

Chairman Burr, Vice Chairman Warner, Members of the Committee, thank you for the invitation to offer the United States Intelligence Community's 2017 assessment of threats to US national security. My statement reflects the collective insights of the Intelligence Community's extraordinary men and women, whom I am privileged and honored to lead. We in the Intelligence Community are committed every day to provide the nuanced, multidisciplinary intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

The order of the topics presented in this statement does not necessarily indicate the relative importance or magnitude of the threat in the view of the Intelligence Community.

Information available as of April 24, 2017 was used in the preparation of this assessment.

# TABLE OF CONTENTS

*Page*

<b>GLOBAL THREATS</b>	
<b>Cyber Threat</b>	1
<b>Emerging and Disruptive Technologies</b>	3
<b>Terrorism</b>	4
<b>Weapons of Mass Destruction and Proliferation</b>	6
<b>Space and Counterspace</b>	8
<b>Counterintelligence</b>	9
<b>Transnational Organized Crime</b>	10
<b>Economics and Natural Resources</b>	12
<b>Human Security</b>	13
<b>REGIONAL THREATS</b>	
<b>East Asia</b>	16
China	16
North Korea	16
Southeast Asia	17
<b>Russia and Eurasia</b>	18
Russia	18
Ukraine, Moldova, and Belarus	19
The Caucasus and Central Asia	19
<b>Europe</b>	20
Key Partners	20
Turkey	20
<b>Middle East and North Africa</b>	21
Syria	21
Iraq	22
Iran	23
Yemen	24

---

<b>South Asia</b>	24
Afghanistan	24
Pakistan	24
India-Pakistan	25
<b>Sub-Saharan Africa</b>	25
South Sudan	25
Sudan	25
Nigeria	26
Sahel	26
Somalia	26
Ethiopia	26
Democratic Republic of the Congo	26
<b>Western Hemisphere</b>	27
Mexico	27
Central America	27
Colombia	27
Cuba	27
Venezuela	28

---



---

## GLOBAL THREATS

---

### CYBER THREAT

Our adversaries are becoming more adept at using cyberspace to threaten our interests and advance their own, and despite improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years.

Cyber threats are already challenging public trust and confidence in global institutions, governance, and norms, while imposing costs on the US and global economies. Cyber threats also pose an increasing risk to public health, safety, and prosperity as cyber technologies are integrated with critical infrastructure in key sectors. These threats are amplified by our ongoing delegation of decisionmaking, sensing, and authentication roles to potentially vulnerable automated systems. This delegation increases the likely physical, economic, and psychological consequences of cyber attack and exploitation events when they do occur. Many countries view cyber capabilities as a viable tool for projecting their influence and will continue developing cyber capabilities. Some adversaries also remain undeterred from conducting reconnaissance, espionage, influence, and even attacks in cyberspace.

#### Cyber Threat Actors

**Russia.** Russia is a full-scope cyber actor that will remain a major threat to US Government, military, diplomatic, commercial, and critical infrastructure. Moscow has a highly advanced offensive cyber program, and in recent years, the Kremlin has assumed a more aggressive cyber posture. This aggressiveness was evident in Russia's efforts to influence the 2016 US election, and we assess that only Russia's senior-most officials could have authorized the 2016 US election-focused data thefts and disclosures, based on the scope and sensitivity of the targets. Outside the United States, Russian actors have conducted damaging and disruptive cyber attacks, including on critical infrastructure networks. In some cases, Russian intelligence actors have masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. Russia has also leveraged cyberspace to seek to influence public opinion across Europe and Eurasia. We assess that Russian cyber operations will continue to target the United States and its allies to gather intelligence, support Russian decisionmaking, conduct influence operations to support Russian military and political objectives, and prepare the cyber environment for future contingencies.

**China.** We assess that Beijing will continue actively targeting the US Government, its allies, and US companies for cyber espionage. Private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral Chinese-US cyber commitments of September 2015. Beijing has also selectively used offensive cyber operations against foreign targets that it probably believes threaten Chinese domestic stability or regime legitimacy.

**Iran.** Tehran continues to leverage cyber espionage, propaganda, and attacks to support its security priorities, influence events and foreign perceptions, and counter threats—including against US allies in the region. Iran has also used its cyber capabilities directly against the United States. For example, in

2013, an Iranian hacker conducted an intrusion into the industrial control system of a US dam, and in 2014, Iranian actors conducted a data deletion attack against the network of a US-based casino.

**North Korea.** Pyongyang has previously conducted cyber-attacks against US commercial entities—specifically, Sony Pictures Entertainment in 2014—and remains capable of launching disruptive or destructive cyber attacks to support its political objectives. Pyongyang also poses a cyber threat to US allies. South Korean officials have suggested that North Korea was probably responsible for the compromise and disclosure of data in 2014 from a South Korean nuclear plant.

**Terrorists.** Terrorists—to include the Islamic State of Iraq and ash-Sham (ISIS)—will also continue to use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations. Hizballah and HAMAS will continue to build on their cyber accomplishments inside and outside the Middle East. ISIS will continue to seek opportunities to target and release sensitive information about US citizens, similar to their operations in 2015 disclosing information about US military personnel, in an effort to inspire attacks.

**Criminals.** Criminals are also developing and using sophisticated cyber tools for a variety of purposes including theft, extortion, and facilitation of other criminal activities. “Ransomware,” malware that employs deception and encryption to block users from accessing their own data, has become a particularly popular tool of extortion. In 2016, criminals employing ransomware turned their focus to the medical sector, disrupting patient care and undermining public confidence in some medical institutions.

### **Physical Consequences**

Our adversaries are likely to seek capabilities to hold at risk US critical infrastructure as well as the broader ecosystem of connected consumer and industrial devices known as the “Internet of Things” (IoT). Security researchers continue to discover vulnerabilities in consumer products including automobiles and medical devices. If adversaries gain the ability to create significant physical effects in the United States via cyber means, they will have gained new avenues for coercion and deterrence. For example, a cyber attack on a Ukrainian power network in 2015 caused power outages for several hours.

### **Economic and Security Consequences**

Adversaries will continue to use cyber operations to undermine US military and commercial advantage by hacking into US defense industry and commercial enterprises in pursuit of scientific, technical, and business information. Examples include theft of data on the F-35 Joint Strike Fighter, the F-22 Raptor fighter jet, and the MV-22 Osprey. In addition, adversaries often target personal accounts of government officials and their private-sector counterparts. This espionage reduces cost and accelerates the development of foreign weapon systems, enables foreign reverse-engineering and countermeasures development, and undermines US military, technological, and commercial advantage.

### **Psychological Consequences**

The impact of cyber threats extends beyond the physical and commercial realms. Online threats—from both states and non-state actors—distort the perceptions and decisionmaking processes of the target, whether they are countries or individuals, in ways that are both obvious and insidious. Information from

cyber espionage can be leaked indiscriminately or selectively to shape perceptions. Furthermore, even a technically secure Internet can serve as a platform for the delivery of manipulative content crafted by foes seeking to gain influence or foment distrust.

### **Global Security, Diplomacy, and Norms**

We assess that as foreign countries seek to balance security, economic growth, and interoperability objectives, many will implement new laws and technical changes to monitor and control access to information within and across their borders. Some states will continue to seek to control user access through means such as restrictions on encryption and steps to reduce anonymity online. However, these states will probably not significantly erode the overall global connectivity of the Internet. Furthermore, some state information control efforts will almost certainly be challenged by a broad coalition of states and non-state cyber stakeholders, including innovative technologists, industry leaders, privacy advocates, “hackers,” and others with an interest in opposing censorship or government control of cyberspace.

Although recognition is widespread that existing international law applies to states’ conduct in cyberspace, how that law applies to states’ use of information and communication technologies (ICT) remains a subject of significant international discussion. In addition, although efforts are ongoing to gain adherence to certain voluntary, non-binding norms of responsible state behavior in cyberspace, they have not gained universal acceptance, and efforts to promote them are increasingly polarized. Despite the existence and widespread ratification of the Budapest Convention—the treaty on cybercrime of the Council of Europe—some states have called for the drafting of new international treaties to regulate cybercrime and other cyber-related issues. Moreover, although some countries might be willing to explore limits on cyber operations against certain targets, few would likely support a ban on offensive capabilities.

## **EMERGING AND DISRUPTIVE TECHNOLOGIES**

### **Strategic Outlook**

Continued rapid technological progress remains central to economic prosperity and social well-being, but it is also introducing potential new threats. Artificial intelligence (AI) is advancing computational capabilities that benefit the economy, yet those advances also enable new military capabilities for our adversaries. Genome editing has the potential to cure diseases and modify human performance, which presents new ethical and security issues. The Internet of Things (IoT) is connecting billions of new devices to the Internet, but it also broadens the attack potential of cyber actors against networks and information. Semiconductors remain core to the economy and the military, yet new national security risks might arise from next-generation chips because of technology plateaus and investments by other states.

### **Artificial Intelligence**

A surge of commercial and government research is improving AI capabilities while raising national security issues. Semi-autonomous cars, the victory of an AI-based system over the world champion in the game Go, and devices with AI-enabled personal assistants have drawn global attention to the field.

Corporations around the globe are investing in a range of AI applications including marketing, crime detection, health, and autonomous vehicles. Although the United States leads AI research globally, foreign state research in AI is growing. Foreign governments cite AI in their science and technology strategies or have planned specific efforts to enhance their AI capabilities. The implications of our adversaries' abilities to use AI are potentially profound and broad. They include an increased vulnerability to cyber attack, difficulty in ascertaining attribution, facilitation of advances in foreign weapon and intelligence systems, the risk of accidents and related liability issues, and unemployment.

### **Genome Editing**

The development of genome-editing technologies is accelerating the rate at which we can develop new approaches to address medical, health, industrial, environmental, and agricultural challenges and revolutionize biological research. However, the fast pace of development and broad range of applications are likely to challenge governments and scientific communities alike to develop regulatory and ethical frameworks or norms to govern the responsible application of the technology.

### **Internet of Things**

The widespread incorporation of “smart” devices into everyday objects is changing how people and machines interact with each other and the world around them, often improving efficiency, convenience, and quality of life. Their deployment has also introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Cyber actors have already used IoT devices for distributed denial-of-service (DDoS) attacks, and we assess they will continue. In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks.

### **Next-Generation Semiconductors**

Continual advancement of semiconductor technologies during the past 50 years in accordance with Moore's Law—which posits that the overall processing power of computers will double every two years—has been a key driver of the information technology revolution that underpins many US economic and security advantages. Industry experts, however, are concerned that Moore's Law might no longer apply by the mid-2020s as the fundamental limits of physics to further miniaturize transistors are reached, potentially eroding US national security advantages. Meanwhile, China is increasing its efforts to improve its domestic technological and production capabilities through mergers and acquisitions to reduce its dependence on foreign semiconductor technology, according to Western experts and business analysts.

## **TERRORISM**

The worldwide threat from terrorism will remain geographically diverse and multifaceted—a continuing challenge for the United States, our allies, and partners who seek to counter it. Sunni violent extremists will remain the primary terrorist threat. These extremists will continue to embroil conflict zones in the Middle East, Africa, and South Asia. Some will also seek to attempt attacks outside their operating areas.

- Iran continues to be the foremost state sponsor of terrorism and, with its primary terrorism partner, Lebanese Hizballah, will pose a continuing threat to US interests and partners worldwide. The Syrian, Iraqi, and Yemeni conflicts will continue to aggravate the rising Sunni-Shia sectarian conflict, threatening regional stability.

### **Terrorist Threat to the United States**

US-based homegrown violent extremists (HVEs) will remain the most frequent and unpredictable Sunni violent extremist threat to the US homeland. They will be spurred on by terrorist groups' public calls to carry out attacks in the West. The threat of HVE attacks will persist, and some attacks will probably occur with little or no warning. In 2016, 16 HVEs were arrested, and three died in attacks against civilian soft targets. Those detained were arrested for a variety of reasons, including attempting travel overseas for jihad and plotting attacks in the United States. In addition to the HVE threat, a small number of foreign-based Sunni violent extremist groups will also pose a threat to the US homeland and continue publishing multilingual propaganda that calls for attacks against US and Western interests in the US homeland and abroad.

### **Dynamic Overseas Threat Environment**

The **Islamic State of Iraq and ash-Sham (ISIS)** continues to pose an active terrorist threat to the United States and its allies because of its ideological appeal, media presence, control of territory in Iraq and Syria, its branches and networks in other countries, and its proven ability to direct and inspire attacks against a wide range of targets around the world. However, territorial losses in Iraq and Syria and persistent counterterrorism operations against parts of its global network are degrading its strength and ability to exploit instability and societal discontent. ISIS is unlikely to announce that it is ending its self-declared caliphate even if it loses overt control of its de facto capitals in Mosul, Iraq and Ar Raqqa, Syria and the majority of the populated areas it once controlled in Iraq and Syria.

Outside Iraq and Syria, ISIS is seeking to foster interconnectedness among its global branches and networks, align their efforts to ISIS's strategy, and withstand counter-ISIS efforts. We assess that ISIS maintains the intent and capability to direct, enable, assist, and inspire transnational attacks. The number of foreign fighters traveling to join ISIS in Iraq and Syria will probably continue to decline as potential recruits face increasing difficulties attempting to travel there. The number of ISIS foreign fighters leaving Iraq and Syria might increase. Increasing departures would very likely prompt additional would-be fighters to look for new battlefields or return to their home countries to conduct or support external operations.

During the past 16 years, US and global counterterrorism (CT) partners have significantly reduced **al-Qa'ida's** ability to carry out large-scale, mass casualty attacks, particularly against the US homeland. However, al-Qa'ida and its affiliates remain a significant CT threat overseas as they remain focused on exploiting local and regional conflicts. In 2016, **al-Nusrah Front and al-Qa'ida in the Arabian Peninsula (AQAP)** faced CT pressure in Syria and Yemen, respectively, but have preserved the resources, manpower, safe haven, local influence, and operational capabilities to continue to pose a threat. In Somalia, **al-Shabaab** sustained a high pace of attacks in Somalia and continued to threaten the northeast and coastal areas of Kenya. Its operations elsewhere in East Africa have diminished after the deaths of many external plotters since 2015, but al-Shabaab retains the resources, manpower,



influence, and operational capabilities to pose a real threat to the region, especially Kenya. In North and West Africa, **al-Qa'ida in the Lands of the Islamic Maghreb (AQIM)** escalated its attacks on Westerners in 2016 with two high-profile attacks in Burkina Faso and Cote d'Ivoire. It merged with allies in 2017 to form a new group intended to promote unity among Mali-based jihadists, extend the jihad beyond the Sahara and Sahel region, increase military action, and speed up recruitment of fighters. In Afghanistan and Pakistan, remaining members of al-Qa'ida and its regional affiliate, **al-Qa'ida in the Indian Subcontinent (AQIS)**, continued to suffer personnel losses and disruptions to safe havens in 2016 due to CT operations. However, both groups maintain the intent to conduct attacks against the United States and the West.

## WEAPONS OF MASS DESTRUCTION AND PROLIFERATION

State efforts to modernize, develop, or acquire weapons of mass destruction (WMD), their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and allies. Both state and non-state actors have already demonstrated the use of chemical weapons in the Levant. Biological and chemical materials and technologies—almost always dual use—move easily in the globalized economy, as do personnel with the scientific expertise to design and use them for legitimate and illegitimate purposes. Information about the latest discoveries in the life sciences also diffuses rapidly around the globe, widening the accessibility of knowledge and tools for beneficial purposes and for potentially nefarious applications.

### Russia Pressing Forward With Cruise Missile That Violates the INF Treaty

Russia has developed a ground-launched cruise missile (GLCM) that the United States has declared is in violation of the Intermediate-Range Nuclear Forces (INF) Treaty. Despite Russia's ongoing development of other Treaty-compliant missiles with intermediate ranges, Moscow probably believes that the new GLCM provides sufficient military advantages that make it worth risking the political repercussions of violating the INF Treaty. In 2013, a senior Russian administration official stated publicly that the world had changed since the INF Treaty was signed in 1987. Other Russian officials have made statements in the past complaining that the Treaty prohibits Russia, but not some of its neighbors, from developing and possessing ground-launched missiles with ranges between 500 to 5,500 kilometers.

### China Modernizing its Nuclear Forces

The Chinese People's Liberation Army (PLA) has established a Rocket Force—replacing the longstanding Second Artillery Corps—and continues to modernize its nuclear missile force by adding more survivable road-mobile systems and enhancing its silo-based systems. This new generation of missiles is intended to ensure the viability of China's strategic deterrent by providing a second-strike capability. In addition, the PLA Navy continues to develop the JL-2 submarine-launched ballistic missile (SLBM) and might produce additional JIN-class nuclear-powered ballistic missile submarines. The JIN-class submarines—armed with JL-2 SLBMs—will give the PLA Navy its first long-range, sea-based nuclear capability.

## **Iran and JCPOA**

Tehran's public statements suggest that it wants to preserve the Joint Comprehensive Plan of Action (JCPOA)—because it views the JCPOA as a means to remove sanctions while preserving some nuclear capabilities. It expects the P5+1 members to adhere to their obligations, although Iran clearly recognizes the new US Administration is concerned with the deal. Iran's implementation of the JCPOA has extended the amount of time Iran would need to produce enough fissile material for a nuclear weapon from a few months to about a year. The JCPOA has also enhanced the transparency of Iran's nuclear activities, mainly through improved access by the International Atomic Energy Agency (IAEA) and its investigative authorities under the Additional Protocol to its Comprehensive Safeguards Agreement.

Iran is pursuing capabilities to meet its nuclear energy and technology goals and to give it the capability to build missile-deliverable nuclear weapons, if it chooses to do so. Its pursuit of these goals will influence its level of adherence to the JCPOA. We do not know whether Iran will eventually decide to build nuclear weapons.

We judge that Tehran would choose ballistic missiles as its preferred method of delivering nuclear weapons, if it builds them. Iran's ballistic missiles are inherently capable of delivering WMD, and Tehran already has the largest inventory of ballistic missiles in the Middle East. Tehran's desire to deter the United States might drive it to field an intercontinental ballistic missile (ICBM). Progress on Iran's space program could shorten a pathway to an ICBM because space launch vehicles use similar technologies.

## **North Korea Continues To Expand WMD-Applicable Capabilities**

North Korea's nuclear weapons and missile programs will continue to pose a serious threat to US interests and to the security environment in East Asia in 2017. North Korea's export of ballistic missiles and associated materials to several countries, including Iran and Syria, and its assistance to Syria's construction of a nuclear reactor, destroyed in 2007, illustrate its willingness to proliferate dangerous technologies.

North Korea has also expanded the size and sophistication of its ballistic missile forces—from close-range ballistic missiles (CRBMs) to ICBMs—and continues to conduct test launches. In 2016, North Korea conducted an unprecedented number of ballistic missile tests. Pyongyang is committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States; it has publicly displayed its road-mobile ICBMs on multiple occasions. We assess that North Korea has taken steps toward fielding an ICBM but has not flight-tested it.

We have long assessed that Pyongyang's nuclear capabilities are intended for deterrence, international prestige, and coercive diplomacy.

## **Chemical Weapons in Iraq and Syria**

We assess the Syrian regime used the nerve agent sarin in an attack against the opposition in Khan Shaykhun on 4 April 2017 in what is probably the largest chemical weapons attack since August 2013. We continue to assess that Syria has not declared all the elements of its chemical weapons program to the Chemical Weapons Convention (CWC) and has the capability to conduct further attacks. Despite the

creation of a specialized team and years of work by the Organization for the Prohibition of Chemical Weapons (OPCW) to address gaps and inconsistencies in Syria's declaration, numerous issues remain unresolved. The OPCW-UN Joint Investigative Mechanism (JIM) attributed three chlorine attacks in 2014 and 2015 to the Syrian regime.

We assess that non-state actors in the region are also using chemicals as a means of warfare. The OPCW-UN JIM concluded that ISIS used sulfur mustard in an attack in 2015. ISIS has allegedly used chemicals in attacks in Iraq and Syria, suggesting that attacks might be widespread.

## SPACE AND COUNTERSPACE

### Space

**Global Trends.** Continued global space industry expansion will further extend space-enabled capabilities and space situational awareness to nation-state, non-state, and commercial space actors in the coming years, enabled by increased availability of technology, private-sector investment, falling launch service costs, and growing international partnerships for shared production and operation. Government and commercial organizations will increasingly have access to space-derived information services such as imagery, weather, Internet, communications, and positioning, navigation, and timing (PNT) for intelligence, military, scientific, or business purposes. For instance, China aims to become a world leader in PNT as it completes its dual-use global satellite navigation system by 2020.

**Military and Intelligence.** Russia aims to improve intelligence collection, missile warning, and military communications systems to better support situational awareness and tactical weapons targeting. Russian plans to expand its imagery constellation and double or possibly triple the number of satellites by 2025. China intends to continue increasing its space-based military and intelligence capabilities to improve global situational awareness and support complex military operations. Many countries in the Middle East, Southeast Asia, and South America are purchasing dual-use imaging satellites to support strategic military activities, some as joint development projects.

### Counterspace

**Space Warfare.** We assess that Russia and China perceive a need to offset any US military advantage derived from military, civil, or commercial space systems and are increasingly considering attacks against satellite systems as part of their future warfare doctrine. Both will continue to pursue a full range of anti-satellite (ASAT) weapons as a means to reduce US military effectiveness. In late 2015, China established a new service—the PLA Strategic Support Force—probably to improve oversight and command of Beijing's growing military interests in space and cyberspace. Russia and China remain committed to developing capabilities to challenge perceived adversaries in space, especially the United States, while publicly and diplomatically promoting nonweaponization of space and “no first placement” of weapons in space. Such commitment continues despite ongoing US and allied diplomatic efforts to dissuade expansion of threats to the peaceful use of space, including international engagements through the UN.

**Counterspace Weapons.** The global threat of electronic warfare (EW) attacks against space systems will expand in the coming years in both number and types of weapons. Development will very likely focus on jamming capabilities against dedicated military satellite communications (SATCOM), Synthetic Aperture Radar (SAR) imaging satellites, and enhanced capabilities against Global Navigation Satellite Systems (GNSS), such as the US Global Positioning System (GPS). Blending of EW and cyber-attack capabilities will likely expand in pursuit of sophisticated means to deny and degrade information networks. Chinese researchers have discussed methods to enhance robust jamming capabilities with new systems to jam commonly used frequencies. Russia intends to modernize its EW forces and field a new generation of EW weapons by 2020. Iran and North Korea are also enhancing their abilities to disrupt military communications and navigation.

Some new Russian and Chinese ASAT weapons, including destructive systems, will probably complete development in the next several years. Russian military strategists likely view counterspace weapons as an integral part of broader aerospace defense rearmament and are very likely pursuing a diverse suite of capabilities to affect satellites in all orbital regimes. Russian lawmakers have promoted military pursuit of ASAT missiles to strike low-Earth orbiting satellites, and Russia is testing such a weapon for eventual deployment. A Russian official also acknowledged development of an aircraft-launched missile capable of destroying satellites in low-Earth orbit. Ten years after China intercepted one of its own satellites in low-Earth orbit, its ground-launched ASAT missiles might be nearing operational service within the PLA. Both countries are advancing directed energy weapons technologies for the purpose of fielding ASAT systems that could blind or damage sensitive space-based optical sensors. Russia is developing an airborne laser weapon for use against US satellites. Russia and China continue to conduct sophisticated on-orbit satellite activities, such as rendezvous and proximity operations, at least some of which are likely intended to test dual-use technologies with inherent counterspace functionality. For instance, space robotic technology research for satellite servicing and debris-removal might be used to damage satellites. Such missions will pose a particular challenge in the future, complicating the US ability to characterize the space environment, decipher intent of space activity, and provide advance threat warning.

## COUNTERINTELLIGENCE

The United States will face a complex global foreign intelligence threat environment in 2017. We assess that the leading state intelligence threats to US interests will continue to be Russia and China, based on their services' capabilities, intent, and broad operational scope. Other states in South Asia, the Near East, East Asia, and Latin America will pose local and regional intelligence threats to US interests. For example, Iranian and Cuban intelligence and security services continue to view the United States as a primary threat.

Penetrating the US national decisionmaking apparatus and the Intelligence Community will remain primary objectives for numerous foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other areas will remain a persistent threat to US interests.

Non-state entities, including international terrorists and transnational organized crime groups, are likely to continue to employ and improve their intelligence capabilities including by human, technical, and cyber means. As with state intelligence services, these non-state entities recruit sources and perform physical and technical surveillance to facilitate their illicit activities and avoid detection and capture.

Trusted insiders who disclose sensitive or classified US Government information without authorization will remain a significant threat in 2017 and beyond. The sophistication and availability of information technology that increases the scope and impact of unauthorized disclosures exacerbate this threat.

## **TRANSNATIONAL ORGANIZED CRIME**

### **Rising US Drug Threat**

The illicit drug threat the United States is intensifying, as indicated by soaring US drug deaths, foreign drug production, and drug seizures.

- Deaths from synthetic opioids—including fentanyl and its analogues—increased 73 percent in 2015 compared to 2014, and mortality from all other illicit drugs increased 36 percent for the same period, according to the US Centers for Disease Control and Prevention (CDC). Preliminary data for 2016 from some states suggest that deaths have continued to increase.
- Seizures of cocaine and methamphetamine increased along the US southwest border in 2016 over 2015.

Rising foreign drug production, the staying power of Mexican trafficking networks, and strong demand are driving the US drug threat.

- In Mexico, the dominant source of US heroin, potential heroin production doubled from 2014 to 2016, according to the US Government estimates.
- Production of cocaine reached the highest levels on record for Colombia in 2016 and for Peru and Bolivia in 2015—the last years for which estimates are available—driven in part by a decline in coca eradication efforts.

Synthetic drugs from Asia—including synthetic opioids, cannabinoids, and cathinones—pose a strong and probably growing threat and have the potential to displace some traditional drugs produced from plants. Such drugs are often traded via the Internet or—in the case of cannabinoids and cathinones—sold over the counter in products marked “not intended for human consumption.” Counterfeit and substandard pharmaceutical trafficking is also on the rise, with the Internet being the primary means by which transnational criminal organizations target US citizens.

- Approximately 18-20 new illegal online pharmacy domain names are registered every day, according to estimates of the Food and Drug Administration, adding to the tens of thousands of existing illegal online pharmacies in operation.



### **Crime Enables Other Nefarious Actors**

Transnational Organized Crime (TOC) will pose a continuing threat to the United States and its allies through close relationships with foreign states and non-state actors. Some states use TOC networks as proxies to engage in activities from which the states wish to distance themselves. TOC networks also have the ability to capture territory in states or portions of states and control it with violence and corruption of public officials. They often receive sanctuary as a result of providing social services, incorporating corruptive methods, and creating dependencies. TOC networks facilitate terrorism by providing money and services, such as selling weapons. They also engage in cyber-based theft and extortion and offer their capabilities to other cyber actors.

- Hong Kong police arrested six individuals with suspected Chinese organized crime links in connection with death threats to a lawmaker elected in September 2016 who advocated for greater autonomy from China.
- In 2015, MS-13 gang members in San Pedro Sula, Honduras provided meals to children and the elderly, shielded residents from rival criminals, meted out justice for unauthorized crimes, and halted criminals from unofficially taxing residents and small businesses. Such support to local communities undermines government legitimacy and engenders public support for the criminal groups.

### **Global Human Trafficking Risks Rising**

The number of individuals at risk of human trafficking will almost certainly rise in 2017 because internal conflict, societal violence, and environmental crises are increasing the populations of refugees and Internally Displaced Persons (IDP). Risks of human trafficking vulnerability intensify during crisis situations when individuals often lose their support networks and sources of livelihood. In addition to crisis-induced displacement, entrenched structural factors—including political instability, government corruption, weak rule of law, soft economies, low levels of democracy, and discrimination toward women, children, and minorities—will very likely continue to increase potential victims' vulnerability to human trafficking worldwide.

### **Wildlife Trafficking and Illegal Fishing**

Wildlife trafficking and poaching are widespread in many countries, especially those grappling with corruption, weak judiciaries, and scarce state resources. Some wildlife traffickers also move other contraband, such as drugs and weapons, at times relying on the same corrupt protectors. Awareness of wildlife crime and its impact is growing among source and demand countries, and regional leaders in Africa increasingly acknowledge the links among poaching, wildlife trafficking, instability, corruption, crime, and challenges to the rule of law.

Global fisheries face an existential threat in the decades ahead from surging worldwide demand, declining ocean health, and continued illegal, unreported, and unregulated (IUU) fishing. IUU fishing also harms legitimate fishing activities and livelihoods, jeopardizes food and economic security, benefits transnational crime, distorts markets, contributes to human trafficking, and undermines ongoing efforts to implement sustainable fisheries policies. It can also heighten tensions within and between countries and encourage piracy and frequently involves forced labor, a form of human trafficking.

## **ECONOMICS AND NATURAL RESOURCES**

Global growth is likely to remain subdued in 2017 amid growing headwinds in China's economy and tepid growth in advanced economies. Worldwide gross domestic product (GDP) growth was virtually unchanged in 2016 from the previous year at 3.1 percent and is forecast to grow 3.5 percent in 2017, according the International Monetary Fund (IMF). Improving growth in commodity-dependent economies is likely to boost global economic activity beyond 2017. Adverse shocks, however, such as a greater slowdown in China than the IMF projects or capital outflows from emerging markets stemming from rising US interest rates, would put the modest global economic recovery at risk.

### **Macroeconomic Stability**

The outlook for emerging markets and developing countries is improving, primarily because of stabilizing commodity prices and increased capital inflows. The IMF forecasts that growth in emerging economies will accelerate to 4.5 percent in 2017 as recoveries start to take hold in several countries. However, rising non-performing loans in China could reinforce the deceleration in Chinese economic growth, weighing on global economic and financial conditions and dampening global demand, particularly for commodities. Moreover, the prospect of higher interest rates in the United States and a strengthening dollar might lead to sustained capital outflows again from emerging markets.

Continued solid performance by the United States and increasingly stable conditions in many European states will probably help to support growth in developed economies. Many European countries and Japan, however, continue to rely on low interest rates and accommodative monetary policies to counter weak demand. Policy uncertainty also poses risks to the global economy.

### **Energy and Commodities**

Subdued growth, particularly in the industrialized economies, had a negative impact on commodity prices in recent years, which have been particularly harmful for emerging market economies, with the exception of net commodity importers, such as China and India. A collapsing economy in Venezuela—the result of the oil-price decline and years of flawed economic policy and profligate government spending—will leave Caracas struggling to avoid default in 2017. Saudi Arabia and other Persian Gulf oil exporters, who generally have more substantial financial reserves, have nonetheless seen a sharp increase in budget deficits that have forced politically unpopular fiscal reforms such as cuts to subsidies, government spending, and government jobs. In Africa, declining oil revenues, past mismanagement, and inadequate policy responses to oil price shock have contributed to Angolan and Nigerian fiscal problems, currency strains, and deteriorating foreign exchange reserves. The World Bank forecasts that prices for most commodities, however, will increase slightly in 2017 as markets continue to rebalance, albeit at lower levels than earlier in the decade.

Sluggish growth of global demand for oil and low prices continue to discourage plans to develop new resources and expand existing projects—particularly in high-cost areas such as the Arctic, Brazilian pre-salt region, or West Africa's deepwater. Projects already under development will probably be completed during the next five years, but longer-term prospects have been slashed, potentially setting the stage for shortfalls and higher prices when demand recovers.

## **The Arctic**

Arctic countries face an array of challenges and opportunities as diminishing sea ice increases commercial shipping prospects and possible competition over undersea resources in coming decades. In August 2016, the first large-capacity cruise ship traversed the Northwest Passage, and more such trips are planned. In September 2016, NASA measured the Arctic sea ice minimum extent at roughly 900,000 square miles less than the 1981-2010 average. Relatively low economic stakes in the past and fairly well established exclusive economic zones (EEZs) among the Arctic states have facilitated cooperation in pursuit of shared interests in the region, even as polar ice has receded and Arctic-capable technology has improved. However, as the Arctic becomes more open to shipping and commercial exploitation, we assess that risk of competition over access to sea routes and resources, including fish, will include countries traditionally active in the Arctic as well as other countries that do not border on the region but increasingly look to advance their economic interests there.

# **HUMAN SECURITY**

## **Environmental Risks and Climate Change**

The trend toward a warming climate is forecast to continue in 2017. The UN World Meteorological Organization (WMO) is warning that 2017 is likely to be among the hottest years on record—although slightly less warm than 2016 as the strong El Nino conditions that influenced that year have abated. The US National Oceanic and Atmospheric Administration (NOAA) and the National Aeronautics and Space Administration (NASA) reported that 2016 was the hottest year since modern measurements began in 1880. This warming is projected to fuel more intense and frequent extreme weather events that will be distributed unequally in time and geography. Countries with large populations in coastal areas are particularly vulnerable to tropical weather events and storm surges, especially in Asia and Africa.

Global air pollution is worsening as more countries experience rapid industrialization, urbanization, forest burning, and agricultural waste incineration, according to the World Health Organization (WHO). An estimated 92 percent of the world's population live in areas where WHO air quality standards are not met, according to 2014 information compiled by the WHO. People in low-income cities are most affected, with the most polluted cities located in the Middle East, Asia, and Africa. Public dissatisfaction with air quality might drive protests against authorities, such as those seen in recent years in China, India, and Iran.

Heightened tensions over shared water resources are likely in some regions. The dispute between Egypt and Ethiopia over the construction of the massive Grand Ethiopian Renaissance Dam (GERD) on the Nile is likely to intensify because Ethiopia plans to begin filling the reservoir in 2017.

Global biodiversity will likely continue to decline due to habitat loss, overexploitation, pollution, and invasive species, according to a study by a nongovernmental conservation organization, disrupting ecosystems that support life, including humans. Since 1970, vertebrate populations have declined an estimated 60 percent, according to the same study, whereas populations in freshwater systems declined

more than 80 percent. The rate of species loss worldwide is estimated at 100 to 1,000 times higher than the natural background extinction rate, according to peer-reviewed scientific literature.

We assess national security implications of climate change but do not adjudicate the science of climate change. In assessing these implications, we rely on US government-coordinated scientific reports, peer-reviewed literature, and reports produced by the Intergovernmental Panel on Climate Change (IPCC), which is the leading international body responsible for assessing the science related to climate change.

## **Health**

The Zika virus is likely to continue to affect the Western Hemisphere through 2017. Although it is causing minor or no illness for most infected people, it is producing severe birth defects in about 10 percent of babies born to mothers who were infected while pregnant and is likely causing neurological symptoms for a small number of infected adults. A separate strain of the virus will likely continue to affect Southeast Asia, where scientists believe it has circulated since the 1960s. However, scientists do not know whether the virus will cause a spike in birth defects there. Previous outbreaks in Asia and Africa might provide at least partial immunity and hinder the virus's spread in those regions.

The continued rise of antimicrobial resistance—the ability of pathogens, including viruses, fungi, and bacteria, to resist drug treatment—is likely to outpace development of new antimicrobial drugs. This resistance will result in increasingly difficult or impossible-to-cure infections of previously curable diseases. Drug-resistant forms of malaria and tuberculosis are on the rise, threatening progress in controlling these diseases. Meanwhile, some strains of gonorrhea are showing resistance to nearly all classes of antibiotics, leaving only treatments of last resort, greatly increasing the risk of incurable strains.

HIV/AIDS, malaria, and tuberculosis continue to kill millions of people annually and hinder development in many resource-constrained countries despite significant progress to alleviate the global burden of infectious diseases. Stagnating or declining funding for global health initiatives and lack of domestic resources threaten the continued progress against health threats despite the availability of more cost-effective treatments. Rapidly expanding populations, particularly in Sub-Saharan Africa, put additional stress on scarce resources. Malnutrition, weak healthcare systems, conflict, migration, poor governance, and urbanization will worsen the emergence, spread, and severity of disease outbreaks.

The emergence of a severe global public health emergency is possible in any given year and can have negative impacts on the security and stability of a nation or region. A novel or reemerging microbe that is easily transmissible between humans and is highly pathogenic remains a major threat because such an organism has the potential to spread rapidly and kill millions. Threats such as avian influenza and Middle East Respiratory Syndrome Coronavirus (MERS-CoV) have pandemic potential. The World Bank has estimated that a severe global influenza pandemic could cost the equivalent of 4.8 percent of global GDP, or more than \$3 trillion, during the course of an outbreak.

## **Atrocities and Instability**

Risk of large-scale, violent or regime-threatening instability and atrocities will remain elevated in 2017. Poor governance, weak national political institutions, economic inequality, and the rise of violent non-state actors all undermine states' abilities to project authority.

- Weak state capacity can heighten the risk for atrocities, including arbitrary arrests, extrajudicial killings, rape, and torture.

Groups that promote civil society and democratization are likely to continue to face restrictions in 2017. Freedom House reported the eleventh consecutive year of decline in “global freedom” in 2017. Middle East and North Africa had ratings as one of the worst regions in the world in 2015.

### **Global Displacement**

In 2015, the number of people forcibly displaced reached the highest levels ever recorded by the UN. In many cases, US partners and allies were either the source of refugees and other migrants—such as Afghanistan and South Sudan—or hosted them—such as Ethiopia, Europe, Jordan, Kenya, Lebanon, Turkey, and Uganda. These countries and others will look to the United States, the UN, and other international donors to help meet unprecedented assistance demands in 2017. Ongoing conflicts will continue to displace people, keeping displacement at record highs because few people can safely return home and family members seek to join those who left. Europe and other host countries will face accommodation and integration challenges in 2017, and refugees and economic migrants will probably continue to seek to transit to Europe.

- Primary drivers of global displacement include: conflicts, such as those in Afghanistan, Somalia, South Sudan, and Syria; weak border controls, such as in Libya, which broadened a route from Africa to Europe; relatively easy and affordable access to routes and information; endemic violence, such as in parts of Burundi, Central America, Nigeria, and Pakistan; and persecution, such as in Burma and Eritrea.
- The UN estimated that 65.3 million persons had been forcibly displaced worldwide at the end of 2015, including approximately 21.3 million refugees, 40.8 million IDPs, and 3.2 million asylum seekers. Refugees displaced for five or more years are more likely to remain in their host communities than to return home, according to academic research.
- In 2016, thousands of Syrian, Somali, Sudanese, and Afghan refugees who had fled their countries in preceding years were returned to their countries of origin, which are still undergoing intense conflict. These returnees are now internally displaced in areas still in conflict.

The scale of human displacement in 2017 will continue to strain the response capacity of the international community and drive record requests for humanitarian funding. Host and transit countries will struggle to develop effective policies and manage domestic concerns of terrorists exploiting migrant flows, particularly after attacks in 2016 by foreigners in Belgium, France, Germany, and Turkey.

---

## REGIONAL THREATS

---

### EAST ASIA

#### China

China will continue to pursue an active foreign policy—especially within the Asia Pacific region—highlighted by a firm stance on competing territorial claims in the East China Sea (ECS) and South China Sea (SCS), relations with Taiwan, and its pursuit of economic engagement across East Asia. Regional tension will persist as China completes construction at its expanded outposts in the SCS despite an overwhelmingly strong ruling against it by a UN Convention on the Law of the Sea (UNCLOS) arbitral tribunal in July 2016. China will also pursue efforts aimed at fulfilling its ambitious “One Belt, One Road” initiative to expand China’s economic role and outreach across Asia through infrastructure projects.

China will seek to build on its hosting of the G20 Summit in Hangzhou in September 2016, its “One-Belt, One-Road” initiative, and progress on launching the Asia Infrastructure Investment Bank to increase its global presence on international economic issues. China will increasingly be a factor in global responses to emerging problems, as illustrated by China’s participation in UN peacekeeping operations, its expanding counterterrorism cooperation, and infrastructure construction in Africa and Pakistan as part of the China-Pakistan Economic Corridor.

Domestically, Chinese leaders will move cautiously on their ambitious reform agenda, maintain their anti-corruption campaign, and try to manage China’s slowing economy. China’s economic growth continues to be driven by unsustainable debt accumulation, but Beijing has made limited progress on reforms needed to boost economic efficiencies. Debates among Chinese leaders over policy and personnel choices will intensify before the leadership transition at the 19<sup>th</sup> Party Congress in fall 2017 when Chinese President Xi Jinping will begin his second term as the head of the Chinese Communist Party.

#### North Korea

North Korea’s weapons of mass destruction program, public threats, defiance of the international community, confrontational military posturing, cyber activities, and potential for internal instability pose a complex and increasingly grave national security threat to the United States and its interests.

North Korea’s unprecedented level of testing and displays of strategic weapons in 2016 indicate that Kim is intent on proving he has the capability to strike the US mainland with nuclear weapons. In 2016, the regime conducted two nuclear tests—including one that was claimed to be of a standardized warhead design—and an unprecedented number of missile launches, including a space launch that put a satellite into orbit. These ballistic missile tests probably shortened North Korea’s pathway toward a reliable ICBM, which largely uses the same technology. Kim was also photographed beside a nuclear warhead design and missile airframes to show that North Korea has warheads small enough to fit on a missile, examining a reentry-vehicle nosecone after a simulated reentry, and overseeing launches from a submarine and from mobile launchers in the field, purportedly simulating nuclear use in warfighting scenarios. North



Korea is poised to conduct its first ICBM flight test in 2017 based on public comments that preparations to do so are almost complete and would serve as a milestone toward a more reliable threat to the US mainland. Pyongyang's enshrinement of the possession of nuclear weapons in its constitution, while repeatedly stating that nuclear weapons are the basis for its survival, suggests that Kim does not intend to negotiate them away at any price.

North Korea has long posed a credible and evolving military threat to South Korea and, to a lesser extent, Japan. North Korea possesses a substantial number of proven mobile ballistic missiles, capable of striking a variety of targets in both countries, as demonstrated in successful launches in 2016. Kim has further expanded the regime's conventional strike options in recent years, with more realistic training, artillery upgrades, and new close-range ballistic missiles that enable precision fire at ranges that can reach more US and allied targets in South Korea.

After five years in power, North Korean leader Kim Jong Un continues to defy international sanctions for his country's behavior and reinforce his authority through purges, executions, and leadership shuffles, restricting fundamental freedoms, and enforcing controls on information. He notably unveiled new ruling structures in conjunction with the first Korean Workers Party Congress in a generation, held in May 2016.

### **Southeast Asia**

Democracy in many Southeast Asian countries will remain fragile in 2017. Elites—rather than the populace—retain a significant level of control and often shape governance reforms to benefit their individual interests rather than to promote democratic values. Corruption and cronyism continue to be rampant in the region, and the threat of ISIS and domestic terrorist groups might provide some governments with a new rationale to address not only the terrorist threat but also to curb political opposition movements, as some regional leaders did in the post-9/11 environment.

In the **Philippines**, aggressive campaigns against corruption, crime, and drugs will probably continue despite charges by Filipino critics and international organizations that it is fostering a permissive environment for extrajudicial killings. Philippine efforts to diversify Manila's foreign relations away from the United States have increased uncertainty about the future of Philippine-US security ties. **Thailand** is undergoing its most significant transition in 70 years following the death of the king. In **Burma**, the government led by the National League for Democracy (NLD) seeks to continue the country's democratic transition process, but the military, which has retained significant political and economic power and exclusive control over the security forces, sometimes undermines the civilian government's objectives. In addition, the NLD will be challenged by its lack of governing experience and provisions of the 2008 Constitution that do not align with democratic norms. Burma's Government will continued to be challenged in dealing with the status of the Muslim minority Rohingya in western Burma.

Cohesion of the Association of Southeast Asian Nations (ASEAN) on economic and security issues will continue to be challenged by differing development levels among ASEAN members, their varying economic dependencies on China, and their views of the threat of Beijing's regional ambitions and assertiveness in the SCS. Southeast Asian SCS claimants will continue to seek various ways to strengthen cooperation in the region and, in some cases, with the United States on maritime security issues.

## **RUSSIA AND EURASIA**

### **Russia**

In 2017, Russia is likely to be more assertive in global affairs, more unpredictable in its approach to the United States, and more authoritarian in its approach to domestic politics. Emboldened by Moscow's ability to affect battlefield dynamics in Syria and by the emergence of populist and more pro-Russian governments in Europe, President Vladimir Putin is likely to take proactive actions that advance Russia's great power status.

Putin will seek to prevent any challenges to his rule in the runup to presidential elections scheduled for 2018. Putin remains popular at home, but low turnout in the Duma elections in 2016 and sustained economic hardship will probably enhance Putin's concerns about his ability to maintain control. Putin is likely to continue to rely on repression, state control over media outlets, and harsh tactics to control the political elite and stifle public dissent.

Russia is likely to emerge from its two-year recession in 2017, but the prospects for a strong recovery are slim. Russia is likely to achieve 1.3 percent GDP growth in 2017 and 1.7 percent in 2018, according to commercial forecasts. Putin has long sought to avoid structural reforms that would weaken his control of the country and is unlikely to implement substantial reforms before the presidential elections.

We assess that Russia will continue to look to leverage its military support to the Asad regime to drive a political settlement process in Syria on its terms. Moscow has demonstrated that it can sustain a modest force at a high-operations tempo in a permissive, expeditionary setting while minimizing Russian casualties and economic costs. Moscow is also likely to use Russia's military intervention in Syria, in conjunction with efforts to capitalize on fears of a growing ISIS and extremist threat, to expand its role in the Middle East.

We assess that Moscow's strategic objectives in Ukraine—maintaining long-term influence over Kyiv and frustrating Ukraine's attempts to integrate into Western institutions—will remain unchanged in 2017. Putin is likely to maintain pressure on Kyiv through multiple channels, including through Russia's actions in eastern Ukraine, where Russia arms so-called "separatists. Moscow also seeks to undermine Ukraine's fragile economic system and divided political situation to create opportunities to rebuild and consolidate Russian influence in Ukrainian decisionmaking.

Moscow will also seek to exploit Europe's fissures and growing populist sentiment in an effort to thwart EU sanctions renewal, justify or at least obfuscate Russian actions in Ukraine and Syria, and weaken the attraction of Western integration for countries on Russia's periphery. In particular, Russia is likely to sustain or increase its propaganda campaigns. Russia is likely to continue to financially and politically support populist and extremist parties to sow discord within European states and reduce popular support for the European Union.

The Kremlin is also likely to continue to see defense modernization as a top national priority even as the cumulative effect on the economy of low oil prices, sanctions, and systemic problems serves as a drag on key military goals. Moscow is pursuing a wide range of nuclear, conventional, and asymmetric

capabilities designed to achieve qualitative parity with the United States. These capabilities will give Moscow more options to counter US forces and weapons systems.

### **Ukraine, Belarus, and Moldova**

Russia's military intervention in eastern **Ukraine** continues more than two years after the "Minsk II" agreement concluded in February 2015. Russia continues to exert military and diplomatic pressure to coerce Ukraine into implementing Moscow's interpretation of the political provisions of the agreement—among them, constitutional amendments that would effectively give Moscow a veto over Kyiv's strategic decisions. Domestic Ukrainian opposition to making political concessions to Russia—especially while fighting continues in eastern Ukraine—will limit Kyiv's willingness and ability to compromise, complicating prospects for implementing the Minsk agreement. Russia largely controls the level of violence, which it uses to exert pressure on Kyiv and the negotiating process, and fluctuating levels of violence will probably continue along the front line. The struggle of Ukraine to reform its corrupt institutions will determine whether it can remain on a European path or fall victim again to elite infighting and Russian influence.

Rising popular discontent in **Belarus** will probably complicate the government's efforts to maintain its improved relations with the United States and the EU, which are aimed at bolstering its flagging economy and preserving some diplomatic maneuvering room with Russia. Minsk will continue close security cooperation with Moscow but will probably continue to oppose the establishment of Russian military bases in Belarus.

**Moldova** will probably also seek to balance its relations with Russia and the West rather than pursue a major shift in either direction. The Moldovan Government will almost certainly seek to move forward on implementing Moldova's EU Association Agreement despite the election of a more pro-Russian president. Settlement talks over the breakaway region of Transnistria will continue, but any progress is likely to be limited to smaller issues.

### **The Caucasus and Central Asia**

In **Georgia**, the ruling Georgian Dream (GD) coalition's decisive electoral victory in 2016 is likely to facilitate GD's efforts to target the former ruling United National Movement and expand political control. GD will continue to pursue greater Euro-Atlantic integration by attempting to cement ties with NATO and the EU.

Tensions between **Armenia** and **Azerbaijan** over the separatist region of Nagorno-Karabakh flared in April 2016, and both sides' unwillingness to compromise and mounting domestic pressures suggest that the potential for large-scale hostilities will remain in 2017. In **Azerbaijan**, ongoing economic difficulties are likely to challenge the regime and increase its tendency to repress dissent to maintain power while it continues to try to balance relations with Russia, Iran, and the West.

**Central Asian** states will continue to balance their relations among Russia, China, and the West to pursue economic and security assistance and protect their regimes' hold on power. They remain concerned about the threat of extremism to their stability, particularly in light of a reduced Coalition presence in Afghanistan. Russia and China share these concerns and are likely to use the threat of instability in Afghanistan to try to increase their involvement in Central Asian security affairs. Economic

challenges stemming from official mismanagement, low commodity prices, declining trade and remittances associated with weakening economies of Russia and China, ethnic tensions, and political repression are likely to present the most significant threats to stability in these countries.

## **EUROPE**

### **Key Partners**

The severity of multiple crises facing Europe—irregular migration, security threats, slow economic growth, and protracted debt issues—will challenge European policy cohesion and common action. Additionally, the form and substance of the UK's exit (Brexit) from the European Union will distract European policymakers.

#### **Migration**

The EU-Turkey Statement addressing migration issues concluded in March 2016 and that tightened border controls in the Balkans will continue to limit migration to Europe. Preserving the EU-Turkey agreement, completing trade deals and making investments offered to five African countries, and ensuring the success of a repatriation deal with Afghanistan will likely remain a focus for Europe.

#### **Security**

Terrorists have taken advantage of the influx of migrants and a potential rise in returning foreign fighters from the conflicts in Iraq and Syria might compound the problem. Europe will remain vulnerable to terrorist attacks, and elements of both ISIS and al-Qa'ida are likely to continue to direct and enable plots against targets in Europe

Some European states see Russia as less of a threat to Europe than others do, even as the Baltic states and Poland begin to host multinational battalions as part of NATO's enhanced Forward Presence.

#### **Economic/Financial Issues**

The European Commission projects that euro-zone growth will be about 1.6 percent in 2017. Its projections are based on weak investment growth, uncertainty stemming from Brexit, potential disruptions to trade, and political and practical limits to expanding monetary and fiscal efforts to support growth.

## **Turkey**

President Recep Tayyip Erdogan's narrow win in the mid-April popular referendum on expanding his powers and the ruling Justice and Development Party's (AKP's) post-coup crackdowns are increasing societal and political tension in Turkey.

Turkey's relations with the United States are strained because Ankara calculates that the United States has empowered Turkey's primary security threat—the Kurdistan Workers' Party (PKK)—by partnering

with the Syrian Kurdish People's Protection Units (YPG), which Turkey alleges is aligned with the PKK. European admonition of Turkey's conduct during the referendum—including limitations European countries placed on Turkish campaigning on their soil—is further straining Turkish ties to the EU.

- Two major Turkish complaints are Washington's unwillingness to meet Turkish demands to extradite US-person Fethullah Gulen—accused by the Turkish Government of orchestrating the failed coup in July 2016—and US support to the YPG in Syria.
- In November 2016, the Turkish president indicated that he would be willing to consider joining the Russian-led Shanghai Cooperation Organization (SCO) as an alternative to the EU.

## MIDDLE EAST AND NORTH AFRICA

### Syria

We assess that the Syrian regime, backed by Russia and Iran, will maintain its momentum on the battlefield but that the regime and the opposition are not likely to agree on a political settlement in 2017. Damascus has committed to participate in peace talks but is unlikely to offer more than cosmetic concessions to the opposition. The opposition, although on the defensive, is able to counterattack, which will probably prevent the regime from asserting territorial control over western and southern Syria, and remains committed to President Bashar al-Asad's departure.

The Islamic State of Iraq and ash-Sham (ISIS) has lost about 45 percent of the territory it held in Syria in August 2014, but it still controls much of the eastern section of the country, including the city of Ar Raqqa. ISIS will likely have enough resources and fighters to sustain insurgency operations and plan terrorists attacks in the region and internationally.

Asad's foreign supporters—Russia, Iran, and Lebanese Hizballah—want to keep an allied regime in power and maintain their influence in Syria. Moscow's deployment of combat assets to Syria in late 2015 helped change the momentum of the conflict; Russia has provided combat aircraft, warships, artillery, arms, and ammunition. Iran provides military advice, fighters, weaponry, fuel, and Shia militants. Lebanese Hizballah provides fighters and helps control the Lebanon-Syria border.

Most opposition backers maintain their support, in part by linking Asad's regime to Iran's malign influence in the region, but their lack of unity will hamper their effectiveness.

Syrian Kurdish People's Protection Units (YPG) control much of northern Syria and have worked closely with coalition forces to seize terrain from ISIS. The YPG's goal to unite its "cantons" across northern Syria is opposed by most Syrian Arabs and by Turkey, which views these Kurdish aspirations as a threat to its security. To weaken ISIS and check the Kurds, Ankara has used Syrian opposition groups, backed by Turkish artillery, aircraft, and armored vehicles, to establish a border security zone in Syria.

The continuation of the Syrian conflict will worsen already-disastrous conditions for Syrians and regional states and maintain migration pressure on Europe. As of late March 2017, more than 4.9 million Syrians

have left the country from a pre-conflict population of approximately 23 million, and an additional 6.3 million were internally displaced. ISIS's presence in Syria and ability to stage cross-border attacks will continue to jeopardize Iraq's stability.

## Iraq

The Iraqi Government's primary focus through 2017 will be recapturing and stabilizing Mosul, the largest urban ISIS stronghold in Iraq, and other ISIS-held territory. The Iraqi Security Forces (ISF) and Kurdish Peshmerga with coalition support and forces of the Shia-dominated Popular Mobilization Committee (PMC) are all involved in the Mosul campaign. Faced with the eventual loss of Mosul, ISIS is preparing to regroup and continue an insurgency and terrorist campaign.

- As the Mosul campaign progresses, Baghdad faces potential tensions between the Kurds and the Iranian-backed PMC members over disputed territory while also managing the Turkish presence in northern Iraq. Baghdad has rebuked Ankara for its presence at Bashiqa and warned of potential conflict if Turkey intervenes any farther in northern Iraq. Tensions might persist well after major counter-ISIS combat operations cease as external actors continue to pursue their political and strategic goals in Iraq.

Meanwhile, the Iraqi prime minister is trying to fend off political challenges and cope with an economy weakened by the fight with ISIS and depressed oil prices. A loose "reform" coalition in the Council of Representatives (COR) exploited political divisions in fall 2016 to remove the defense and finance ministers. Political factionalism has prevented the passage of needed political reform, heightened distrust among sectarian groups, and undermined governance.

- Iraq will probably need international financial support throughout 2017, but Iraq's finances could stabilize if oil prices continue to slowly rise and Baghdad makes progress on its reform program. In 2016, Iraq's revenue from crude oil sales averaged \$3.3 billion per month, less than half the monthly revenue in 2014, despite a rise in the number of barrels of oil exported. Oil sales account for about 90 percent of government revenues and make up almost 50 percent of Iraq's GDP. The United States and Iraq concluded a sovereign loan agreement in late January 2017 that could help Baghdad access international funds that it sorely needs to reconstruct areas liberated from ISIS.

Iraq will face serious challenges to its stability, political viability, and territorial integrity after control of Mosul is wrested from ISIS. More than 200,000 individuals have been displaced from Mosul due to the fighting. However, about a third have since returned to their homes, and as many as 1 million civilians might be eventually displaced, adding to the 3 million displaced persons in Iraq as of February 2016.

- Reconstruction of infrastructure and tens of thousands of civilian structures destroyed by fighting in Sunni areas once occupied by ISIS will cost billions of dollars and take years.
- Ethnosectarian reconciliation will also be an enduring challenge. Iraqi Shia, Sunnis, and Kurds increasingly view themselves as having diverging futures. ISIS will seek to exploit any Sunni discontent with Baghdad and try to regain Iraqi territory, whereas the Kurds will probably continue efforts to establish an independent state.



## Iran

The Islamic Republic of Iran remains an enduring threat to US national interests because of Iranian support to anti-US terrorist groups and militants, the Asad regime, Huthi rebels in Yemen, and because of Iran's development of advanced military capabilities. Despite Supreme Leader Khamenei's conditional support for the JCPOA nuclear deal implemented in January 2016, he is highly distrustful of US intentions. Iran's leaders remain focused on thwarting US and Israeli influence and countering what they perceive as a Saudi-led effort to fuel Sunni extremism and terrorism against Iran and Shia communities throughout the region.

Iran is immersed in ongoing conflicts in Iraq, Syria, and Yemen. Iranian officials believe that engaging adversaries away from Iran's borders will help prevent instability from spilling into Iran and reduce ISIS's threat to Iran and its regional partners. Iran's involvement in these conflicts, including sending hundreds of its own forces plus arming, financing, and training thousands of Iraqi, Afghan, and Pakistani Shia fighters to support the Asad regime, has aggravated sectarianism and increased tensions with other regional states. Tehran's provision of aid to the Huthis, including unmanned aerial vehicles (UAVs), explosive boat technology, and missile support, risks expanding and intensifying the conflict in Yemen and the broader Iranian-Saudi dispute. We assess that Iran's leaders intend to leverage their ties to local actors in Iraq, Syria, and Yemen to build long-term Iranian influence in the region. Iran will also utilize its relationship with Moscow to try to expand Iranian influence and counter US pressure.

Hardliners, who believe that the West is attempting to infiltrate Iran to undermine the regime, have driven the increase of arrests of citizens since 2014 who are dual nationals. The Islamic Revolutionary Guard Corps (IRGC) will likely continue to scrutinize, arrest, and detain individuals with ties to the West, particularly dual US-Iranian and UK-Iranian citizens. This practice will weaken prospects of attracting foreign investment into Iran's economy.

Iran continues to develop a range of new military capabilities to monitor and target US and allied military assets in the region, including armed UAVs, ballistic missiles, advanced naval mines, unmanned explosive boats, submarines and advanced torpedoes, and anti-ship and land-attack cruise missiles. Iran has the largest ballistic missile force in the Middle East and can strike targets up to 2,000 kilometers from Iran's borders. Russia's delivery of the SA-20c surface-to-air missile system in 2016 provides Iran with its most advanced long-range air defense system.

IRGC Navy forces operating aggressively in the Persian Gulf and Strait of Hormuz pose a risk to the US Navy. Most IRGC interactions with US ships are professional, although US Navy operators consider approximately 10 percent to be unsafe, abnormal, or unprofessional. We assess that limited aggressive interactions will continue and are probably intended to project an image of strength and possibly to gauge US responses.

## **Yemen**

Fighting in Yemen will almost certainly persist in 2017 despite international attempts to forge cease-fires between Huthi-aligned forces, trained by Iran, and the Yemeni Government, backed by a Saudi-led coalition. Neither the alliance between the Huthis and former Yemeni President Ali Abdallah Salih nor the government of Yemeni President Abd Rabuh Mansur Hadi has been able to achieve decisive results through military force, despite their prominent international backers. Efforts at peace talks are nascent, and both sides remain wary of the other's intentions.

As of late 2016, the fighting had displaced more than 2 million people and left 82 percent of Yemen's population in need of humanitarian aid. Temporary cease-fires have allowed for some increased access for humanitarian organizations, but relief operations are hindered by lack of security, bureaucratic constraints, and funding shortages. More than half the population is experiencing crisis or emergency levels of food insecurity.

AQAP and ISIS's branch in Yemen have exploited the conflict and the collapse of government authority to gain new recruits and allies and expand their influence. Both groups threaten Western interests in Yemen and have conducted attacks on Huthi, Yemeni Government, and Saudi-led coalition targets.

## **SOUTH ASIA**

### **Afghanistan**

The overall situation in Afghanistan will very likely continue to deteriorate, even if international support is sustained. Endemic state weaknesses, the government's political fragility, deficiencies of the Afghan National Security Forces (ANSF), Taliban persistence, and regional interference will remain key impediments to improvement. Kabul's political dysfunction and ineffectiveness will almost certainly be the greatest vulnerability to stability in 2017. ANSF performance will probably worsen due to a combination of Taliban operations, ANSF combat casualties, desertions, poor logistics support, and weak leadership. The ANSF will almost certainly remain heavily dependent on foreign military and financial support to sustain themselves and preclude their collapse. Although the Taliban was unsuccessful in seizing a provincial capital in 2016, it effectively navigated its second leadership transition in two years following the death of its former chief, Mansur, and is likely to make gains in 2017. The fighting will also continue to threaten US personnel, allies, and partners, particularly in Kabul and urban population centers. ISIS's Khorasan branch (ISIS-K)—which constitutes ISIS's most significant presence in South Asia—will probably remain a low-level developing threat to Afghan stability as well as to US and Western interests in the region in 2017.

### **Pakistan**

Pakistani-based terrorist groups will present a sustained threat to US interests in the region and continue to plan and conduct attacks in India and Afghanistan. The threat to the United States and the West from Pakistani-based terrorist groups will be persistent but diffuse. Plotting against the US homeland will be conducted on a more opportunistic basis or driven by individual members within these groups.

Pakistan will probably be able to manage its internal security. Anti-Pakistan groups will probably focus more on soft targets. The groups we judge will pose the greatest threat to Pakistan's internal security include Tehrik-e Taliban Pakistan, Jamaat ul-Ahrar, al-Qa'ida in the Indian Subcontinent, ISIS-K, Lashkar-e Jhangvi, and Lashkar-e Jhangvi al-Alami. The emerging China Pakistan Economic Corridor will probably offer militants and terrorists additional targets.

Pakistan's pursuit of tactical nuclear weapons potentially lowers the threshold for their use. Early deployment during a crisis of smaller, more mobile nuclear weapons would increase the amount of time that systems would be outside the relative security of a storage site, increasing the risk that a coordinated attack by non-state actors might succeed in capturing a complete nuclear weapon.

### **India-Pakistan**

Relations between India and Pakistan remain tense following two major terrorist attacks in 2016 by militants crossing into India from Pakistan. They might deteriorate further in 2017, especially in the event of another high-profile terrorist attack in India that New Delhi attributes to originating in or receiving assistance from Pakistan. Islamabad's failure to curb support to anti-India militants and New Delhi's growing intolerance of this policy, coupled with a perceived lack of progress in Pakistan's investigations into the January 2016 Pathankot cross-border attack, set the stage for a deterioration of bilateral relations in 2016. Increasing numbers of firefights along the Line of Control, including the use of artillery and mortars, might exacerbate the risk of unintended escalation between these nuclear-armed neighbors. Easing of heightened Indo-Pakistani tension, including negotiations to renew official dialogue, will probably hinge in 2017 on a sharp and sustained reduction of cross-border attacks by terrorist groups based in Pakistan and progress in the Pathankot investigation.

## **SUB-SAHARAN AFRICA**

### **South Sudan**

Clashes between Juba and the armed opposition will continue, heightening ethnic tensions and exacerbating the humanitarian crisis and famine amid a declining economy. Both sides' use of ethnic militias, hate speech, and the government's crackdown against ethnic minorities raise the risk of additional mass atrocities. The government will probably continue to restrict political freedoms and civil liberties and obstruct humanitarian assistance.

### **Sudan**

Khartoum probably hopes to continue constructive engagement with the United States following Washington's decision in January 2017 to suspend some sanctions on Sudan. The regime will probably largely adhere to a cessation of hostilities in conflict areas—required to receive sanctions relief—but skirmishing between the Sudanese military and rebel forces is likely to result in low levels of violence and population displacement. The regime's military gains since March 2016 and divisions among armed opponents will almost certainly inhibit the insurgents' ability to make significant political or military gains.

Public dissatisfaction over a weakened economy and austerity measures, however, will test the government's ability to maintain order.

### **Nigeria**

The Nigerian Government will confront a wide range of challenges in 2017, many of which are deeply rooted and have no "quick fix." Despite Nigeria's progress in 2016 reclaiming territory from ISIS in West Africa (ISIS-WA) and Boko Haram, both terrorist groups will remain a threat to military and civilians in northeastern Nigeria, as well as in neighboring Cameroon, Chad, and Niger. Moreover, Nigeria, with Africa's largest economy, is suffering a recession brought on by low oil prices and militant attacks on its oil infrastructure. This recession is handicapping Abuja's efforts to combat the terrorists and respond to a growing humanitarian crisis in the northeast.

### **Sahel**

Governments in Africa's Sahel region—particularly Chad, Mali, Mauritania, and Niger—will remain at risk of internal conflict and terrorist attacks in 2017. The region's shared geography, ethnic and religious connections, and a pervasive lack of border security have facilitated a rise in extremist groups, traffickers, and antigovernment militias since the collapse of Libya in 2011 and the northern Mali uprising in 2012. Al-Qa'ida in the Lands of the Islamic Maghreb (AQIM), al-Murabitun, Ansar al-Din, and other violent extremist groups will continue attacking Western and local interests in the region.

### **Somalia**

The Somali Government will continue to rely on international assistance, including in the areas of civilian protection, service provision, dispute resolution, security, and humanitarian relief. Progress in these areas is critical to maintain support from troop-contributing countries of the African Union Mission in Somalia (AMISOM), which plans to begin withdrawing from Somalia in 2018.

### **Ethiopia**

Ethiopia has faced widespread public protests and ethnic tensions and will struggle to address the underlying grievances while preserving the power of the ruling party. The risk of instability is high. Addis Ababa declared a state of emergency in October 2016 and continues mass arrests, targeting opposition leaders.

### **Democratic Republic of the Congo**

A deal between the government of the Democratic Republic of the Congo (DRC) and Congolese opposition and civil society over President Joseph Kabila's term extension has bought the regime time. Kabila named an opposition member as prime minister in April, but elections are unlikely to be held by the end of 2017 as called for under the agreement. Meanwhile, armed conflict in the east perpetrated by militia groups will exacerbate serious humanitarian challenges.

## **WESTERN HEMISPHERE**

### **Mexico**

The Mexican Government will focus on domestic priorities to help position the country for the presidential election in 2018 while also seeking to limit fallout from potential shifts in the bilateral relationship with the United States. Mexico will be challenged to make gains against corruption and rising crime and will continue to rely on the military to stymie criminal violence. Its \$1.1 trillion economy has benefitted from strong economic fundamentals and robust exports, but changes in trade relationships might weaken the export sector and slow economic growth. Mexican migration to the United States, which has decreased in recent years, might increase if economic opportunity at home declines. Apprehensions of undocumented Mexicans fell from about 268,000 in FY 2013 to 193,000 in FY 2016, according to DHS statistics.

### **Central America**

Insecurity, lack of economic opportunities, desire for family reunification, and views of US immigration policy are likely to remain the principal drivers of migration from the Northern Triangle countries of El Salvador, Guatemala, and Honduras to the United States. Human smuggling networks will continue to help migrants navigate travel routes and security at the US and Mexican border. Homicide rates in these countries remain high despite a decline in 2016, and gang-related violence is still prompting Central Americans to flee. DHS apprehensions along the southwest border of migrants from the Northern Triangle reached nearly 200,000 in FY 2016 but have declined sharply since February 2017.

### **Colombia**

The Colombian Government's ability to implement its historic peace deal with the Revolutionary Armed Forces of Colombia (FARC) in 2017 will be key to the country's prospects for fully harnessing economic and investment opportunities. The peace deal ended the country's 52-year civil war with the FARC and demobilized the Western Hemisphere's largest and longest-running insurgency. Colombia was already politically stable and markedly less violent than 20 years ago. Even so, some immediate post-conflict challenges will include stemming rising drug production and addressing social and economic inequality in rural areas.

### **Cuba**

As Cuba heads into the final year of preparations for its planned historic leadership transition in early 2018, the government's focus will be on preserving the regime's hold on power and dealing with the falling economic growth rate. Cuba blames its slowing economy on lower global commodity prices, the US embargo, and the economic crisis in Venezuela, a top trade partner and important source of political support and petroleum at generous financing terms. Havana, however, has stalled implementation of its own reform program, including changes to investment laws needed to address longstanding investor concerns and plans to unify its dual currency and exchange rate system.

Some Cuban migration to the United States via land routes through Central America and Mexico—especially by Cubans already in transit—is likely to continue despite a significant decrease following the end of the US “Wet Foot, Dry Foot” policy in January 2017. That policy allowed most undocumented Cubans who reached US soil—as opposed to being intercepted at sea—to remain in the United States and then apply for lawful permanent residency status after one year under the Cuban Adjustment Act of 1966. In FY 2016, some 42,000 Cuban migrants arrived at the US southwest border and maritime flows exceeded 7,300 migrants because of poor economic prospects in Cuba and apprehension about potential US policy shifts.

### **Venezuela**

Venezuela’s regime and the political opposition will remain at odds in 2017 as Venezuela’s domestic political and economic tensions intensify. The regime is struggling to contain spiraling inflation and finance imports, creating shortages of foodstuffs and medicines in the oil-rich country. The unpopular government charges that the opposition is waging an economic war and trying to stage a political coup and will probably ratchet up repression to maintain power. Shortages of food, medicine, and basic supplies will probably continue to stoke tensions through 2017.



# EXHIBIT 8

UNCLASSIFIED//FOUO



FBI

# COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP INTELLIGENCE NOTE (SPIN)

SPIN: 15-002

FEBRUARY 2015

## (U) Huawei

(U) A Chinese Government-Subsidized Telecommunication Company

### (U) RISK OVERVIEW

(U) With the expanded use of Huawei Technologies Inc. equipment and services in US telecommunications service provider networks, the Chinese Government's potential access to US business communications is dramatically increasing. Chinese Government-supported telecommunication equipment on US networks may be exploited through Chinese cyber activity, with China's intelligence services operating as an advanced persistent threat to US networks. Huawei has been identified publicly for selling or attempting to sell US intellectual property to export restricted countries (Iran/Cuba), making it a clear threat through its targeting of US economic and proprietary information. China makes no secret that its cyber warfare strategy is predicated on controlling global communications network infrastructure.



(U//FOUO) Huawei is a threat to intellectual property and business communications due to its opaque relationship with the Chinese Government. Huawei has legal obligations to work on behalf of the Chinese state, probably through the Chinese Communist Party (CCP) committee residing within Huawei. This relationship likely influences the company's decision-making through threats of corruption investigations.

(U) Since Huawei's inception in 1987, the company continues to receive open support from senior Chinese Communist Party officials and People's Liberation Army (PLA) Commanders. With over \$100 billion in Chinese Government subsidization and direct financing, Huawei is able to offer unsuspecting US businesses low-cost offers difficult to refuse in exchange for access to US networks.

(U) The purpose of this SPIN is to provide summaries of recent US and British Government investigative findings, private industry reporting, and news articles on Huawei Technology Inc.



(U) Ministry of State Security



(U) People's Liberation Army

### (U) HUAWEI'S EXECUTIVE TIES TO CHINESE MILITARY AND INTELLIGENCE SERVICES

(U) Sun Yafang reportedly worked for the Ministry of State Security (MSS) for an unspecified period of time before joining Huawei in 1989. She quickly rose through the company's ranks to serve as the company's Chairwoman of the Board from 1998-2011.

(U) Ren Zhengfei, a retired PLA officer and director of the PLA's General Staff Department Information Engineering Academy, founded Huawei in 1987. In 1988, he became the president of Huawei and has held the position ever since, according to Open Source reporting.

### (U) HUAWEI IN OTHER COUNTRIES

(U) The US is not the only highly capitalized country targeted by Huawei. The United Kingdom (UK) engaged with Huawei, only to regret its decision.



(U) Secret Intelligence Service (MI6)

The UK's national security policy makers were highly concerned with how Huawei discreetly accessed its critical telecommunication infrastructure. The government had difficulties trusting a cyber-security evaluation process to help

secure Huawei's integration, according to a report by the Parliamentary Intelligence and Security Committee. Australia, on the other hand, proactively decided twice to keep Huawei out of its national broadband infrastructure.



(U) House of Commons

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

## [ COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP INTELLIGENCE NOTE (SPIN) ]

Page 2

**(U) NATIONAL SECURITY IMPLICATIONS OF INVESTMENTS AND PRODUCTS FROM THE PEOPLE'S REPUBLIC OF CHINA IN THE TELECOMMUNICATIONS SECTOR**

(U) The Chinese Government views the telecommunications sector as a "strategic" industry and has expended significant effort and resources to promote and enable new business opportunities in the telecommunications field. These efforts are supported by national-level policies, as the country's senior leadership perceives investment in high-technology sectors to be instrumental in closing the technological gap between China and western nations.

(U) The large and growing state-controlled telecommunications sector is also a major source of government revenue. National security concerns have accompanied the dramatic growth of China's telecom sector. Signals intelligence is a significant source of Chinese intelligence collection, and there is growing public concern over the impacts of cyber espionage incidents that appear to originate in China. Additionally, large Chinese companies are subject to direction by the CCP, to include support for Chinese state policies and goals. From this point of view, the clear economic benefits of foreign investment in the United States must be weighed against *potential* security concerns related to infrastructure.

(U) Internet exchange points (IXP) use a host of networking equipment, including sophisticated routers and switches, which enables traffic to be properly routed. This equipment is comprised of integrated circuits that can be severely impacted, thereby modifying functionality, including backdoors and/or kill switches. Although hostile actors manufacturing such products could conceivably target all integrated circuits to be used in routers, they might instead target integrated circuits used in the most sophisticated equipment. The Internet in the United States could theoretically be brought down or severely disrupted because the routers and switches serving the IXPs were disabled. Traffic would no longer be routed between networks, except where carriers had their own private peering arrangements.

**(U) FOREIGN INVOLVEMENT IN BRITISH CRITICAL NATIONAL INFRASTRUCTURE: IMPLICATIONS FOR NATIONAL SECURITY**

(U) **British Parliamentary Report:** Huawei was allowed to gain a large foothold in the UK's Critical National Infrastructure (CNI); the question now is whether or not that foothold has implications for the UK's national security. When British Parliament Ministers were finally informed about Huawei's involvement in 2006, it was because approval was sought to carry out checks on Huawei's equipment.

(U) **Outlined Threat:** The British Security Service told the British Parliament in early 2008 the Chinese State may be able to exploit any vulnerabilities in Huawei's equipment in order to gain access to the British Telecom network. The Joint Intelligence Committee (JIC) had previously warned if a hostile actor were to exploit such an opportunity, an attack "would be very difficult to detect or prevent and could enable the Chinese to intercept covertly or disrupt traffic passing through Huawei supplied networks."

(U) The assessments underlined what could be at stake through Huawei's involvement in the UK's CNI. The British Parliament questioned how the government would react in the event of an attack, if it was detected. The Cabinet Office explained they would "have the option of putting pressure on the



Communications Service Providers (CSPs) to terminate any contract with Huawei. But the British Government would have to have firm evidence of Chinese attribution." The Committee is concerned at the apparent absence of any strategy to monitor or react to potential breaches. Any vulnerability would call into question whether a product is sufficiently well engineered. An insecure product would risk a third party exploiting its weaknesses to access UK networks for hostile purposes. While we [Intelligence and Security Committee] are reassured by GCHQ's confidence in BT, we also note they acknowledge the risk of unauthorized access cannot be entirely eliminated.

(U) **Conclusion:** The British Parliament remains concerned there is no guarantee any weaknesses or vulnerability in equipment deployed on UK networks, through no fault of the operator, could have serious security implications.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

## [ COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP INTELLIGENCE NOTE (SPIN) ]

Page 3

**(U) INVESTIGATIVE REPORT ON THE US NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANY HUAWEI**

(U) *The United States should view with suspicion the continued penetration of the US telecommunications market by Chinese telecommunications companies* –United States House Permanent Select Committee on Intelligence (HPSCI), Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Huawei and ZTE, October 8, 2012

(U) **HPSCI Recommendation:** Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with Huawei for equipment or services. US network providers and systems developers are also strongly encouraged to seek other vendors for their projects. Based on available information, Huawei cannot be trusted to be free of foreign state influence and thus poses a security threat to the United States and to our systems.

(U) **Overview:** The threat posed to US national-security interests by vulnerabilities in the telecommunications supply chain is an increasing priority given the country's reliance on interdependent critical infrastructure systems, the range of threats these systems face, the rise in cyber espionage, and the growing dependence all consumers have on a small group of equipment providers. China has the means, opportunity, and motive to use telecommunications companies for malicious purposes. Suggested "mitigation measures" cannot fully address the threat posed by Chinese telecommunications companies providing equipment and services to US critical infrastructure.



(U) **Findings:** The Committee finds Huawei did not:

- **Fully cooperate with the investigation** and was unwilling to explain its relationship with the Chinese Government or CCP, while credible evidence exists Huawei fails to comply with US laws.
- **Explain its relationships with the Chinese Government**, and its assertions denying support by the Chinese Government are not credible.
- **Explain what the Party Committee does** on behalf of the Party or which individuals compose the Committee.
- **Provide information** about the Chinese Government's 1999 investigation of the company for tax fraud, which exemplifies a company that refuses to be transparent.
- **Reveal sufficient details or supporting documentation** on its operations, financing, and management in the United States, undermining its claims of being a completely independent subsidiary of Huawei's parent company in Shenzhen, China.
- **Provide details of its operations** in Iran, though it denied doing business with the Government of Iran, and did not provide evidence to support its claims that it complies with all international sanctions or US export laws.
- **Provide details on its Research and Development (R&D) programs**, and other documents, undermining its claim that Huawei provides no R&D for the Chinese military or intelligence services.



(U) **HPSCI Conclusion:** Huawei exhibits a pattern of disregard for the intellectual property rights of other entities and companies in the United States. Huawei employees provided evidence of ostensibly illicit behavior by Huawei

(U//FOUO) This product was prepared by the FBI Strategic Partnership Unit (CD-4F). Please provide any questions or comments to your local Strategic Partnership Coordinator (SPC) or CD-4F at [Strategic\\_Partnerships@ic.fbi.gov](mailto:Strategic_Partnerships@ic.fbi.gov).

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

## [ COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP INTELLIGENCE NOTE (SPIN) ]

Page 4

**(U) Key Intelligence Questions**

(U) If you have any information that would help answer the following Key Intelligence Questions or would like additional information, please contact your local FBI Strategic Partnership Coordinator or FBI field office.

(U//FOUO) **Joint Projects/Collaborations:** Which specific programs/offices within your company have liaison relationships/joint efforts with domestic and foreign entities? Who initiated the partnership effort? Which specific titles/positions within your company work with individuals from foreign companies? How is this access being exploited by your partners? What processes do you use with regard to your due diligence when vetting potential foreign partners?

(U//FOUO) **Foreign Government Activities:** Describe the nature of foreign government involvement in your industry overseas. Please be as broad as government-funded R&D programs or as specific as exact offices/positions within a foreign company that liaise with their government representatives.

(U//FOUO) **Major Foreign Competitors:** Who are your major foreign competitors, particularly those with whom you share some cooperative endeavors? Are you aware of any of your main US/domestic competitors working or negotiating with foreign competitors?

(U//FOUO) **Circumventing/Manipulating US Laws and Regulations:** When you deny entry to your facility or access to your classified, trade secret, and proprietary information by a group or individual, have you experienced any attempts by these individuals to circumvent your actions (e.g., gain access to your facility, information, or personnel by other means?). If so, please explain. Have foreign businesses or groups/employees suggested or attempted to circumvent US law, regulation, company security systems, or policies, and if so, how?

(U//FOUO) **Visitors or Others Collecting Information:** What are the positions or titles of foreign representatives who contact your company? Why are you typically contacted? Are there certain members of visiting delegations who tend to ask most of the questions when you are hosting groups to your facility? If so, please identify these individuals. Are questions submitted in advance or asked randomly? What are other ways you receive unsolicited requests for information? How are requests for visas and visits handled and documented?

(U//FOUO) **Targeted Technology:** What technologies do you want to protect from your competitors (e.g., R&D, supply chain, pricing and customer service information, contracts, production and maintenance records, etc.)? Do you believe you are adequately protecting them? Can you rank these items by level of importance? What information or technology (including expertise in manufacturing, production, or operations) are foreign competitors lacking that keeps them from being competitive? Identify the various applications (both military and commercial) of your product or service.

(U//FOUO) **Criminal and Suspicious Activities:** Describe the various ways you may have experienced loss, theft, or targeting of your trade secrets, proprietary, and critical or emerging technologies, and by whom?

(U//FOUO) **Visitors:** What are the most common type of questions you receive when you are hosting foreign and domestic visitors and groups to your facility? Is there a distinct difference between these two groups in the type of questions they ask? What questions stand out as suspicious?

(U//FOUO) **Targeting Trends:** Has your company observed any trends in the way a domestic or foreign competitor is targeting your proprietary or trade secret information?

(U//FOUO) **Research and Development Losses:** Which countries are your most valuable customers? How do they support your research and development efforts? What is the estimated value of losses of your trade secret or proprietary information (if applicable)?

(U//FOUO) **Collaboration Among Foreign Partners:** How is your company connected to international partners (e.g., through supply chains, joint R&D, acquisition processes, distribution, etc.)? How do you determine your supply chain is sound and you are getting the quality products you purchased/requested? Have international partners sought any quality assurance testing on your products, either before or after a sale?

(U//FOUO) **Financial Matters:** Identify any suspicious financial activities of your business partners, distributors, suppliers, and employees that may aid business competitors or foreign organizations.

(U//FOUO) **Mergers/Acquisitions:** Has your company been approached for a merger or acquisition opportunity by a foreign competitor? If so, please explain the circumstances.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

## [ COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP INTELLIGENCE NOTE (SPIN) ]

Page 5

(U) Sources

1. (U) HPSCI; 08 OCT 2012; (U) Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.
2. (U) Intelligence and Security Committee Presented to Parliament by the Prime Minister on behalf of Her Majesty; JUN 2013; (U) Foreign involvement in the Critical National Infrastructure: The implications for national security.
3. (U) USCC; JAN 2011; (U) The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector.
4. (U) Industry Report; Northrop Grumman Corporation; 07 MAR 2012 (U) Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage; Report prepared for the US-China Economic and Security Review Commission.
5. (U) Nathaniel Ahrens, "China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan," Center for Strategic and International Studies; [http://csis.org/files/publication/130215\\_competitiveness\\_Huawei\\_casestudy\\_Web.pdf](http://csis.org/files/publication/130215_competitiveness_Huawei_casestudy_Web.pdf).
6. (U) Sheridan Prasso, "What Makes China telecom Huawei so Scary," CNN Money; 28 JUL 2011; <http://tech.fortune.cnn.com/2011/07/28/what-makes-china-telecom-huawei-so-scary/>
7. (U) Counter-espionage Law of the People's Republic of China; 01 NOV 2014; Standing Committee of the National People's Congress; [http://news.xinhuanet.com/politics/2014-11/01/c\\_1113074346.htm](http://news.xinhuanet.com/politics/2014-11/01/c_1113074346.htm)
8. (U) Reuters, <http://www.reuters.com/article/2013/01/31/us-huawei-skycom-idUSBRE90U0CC20130131>
9. (U) The Washington Free Beacon; <http://freebeacon.com/national-security/chinese-military-linked-telecom-firm-shipped-u-s-equipment-to-cuba/>
10. (U) ABC News; 29 OCT 2013; Government maintains NBN ban on Chinese telco Huawei after security briefings; <http://www.abc.net.au/news/>
11. (U) MANDIANT; APT1-Exposing One of China's Cyber Espionage Units.

UNCLASSIFIED//FOUO



# EXHIBIT 9



**2017**

**REPORT TO CONGRESS**

*of the*

**U.S.-CHINA ECONOMIC AND  
SECURITY REVIEW COMMISSION**

ONE HUNDRED FIFTEENTH CONGRESS  
FIRST SESSION

---

NOVEMBER 2017

---

Printed for the use of the  
U.S.-China Economic and Security Review Commission  
Available via the World Wide Web: <http://www.uscc.gov>

---

U.S. GOVERNMENT PUBLISHING OFFICE  
WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001



**U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION**

CAROLYN BARTHOLOMEW, *Chairman*  
Hon. DENNIS C. SHEA, *Vice Chairman*

**COMMISSIONERS**

ROBIN CLEVELAND  
Hon. BYRON L. DORGAN  
Hon. CARTE P. GOODWIN  
GLENN HUBBARD  
DANIEL M. SLANE

Hon. JONATHAN N. STIVERS  
Hon. JAMES M. TALENT  
Hon. KATHERINE C. TOBIN  
MICHAEL R. WESSEL  
LARRY M. WORTZEL

MICHAEL R. DANIS, *Executive Director*

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act of 2001, Pub. L. No. 106-398 (codified at 22 U.S.C. §7002), as amended by: The Treasury and General Government Appropriations Act, 2002, Pub. L. No. 107-67 (Nov. 12, 2001) (regarding employment status of staff and changing annual report due date from March to June); The Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of the Commission); The Science, State, Justice, Commerce, and Related Agencies Appropriations Act, 2006, Pub. L. No. 109-108 (Nov. 22, 2005) (regarding responsibilities of the Commission and applicability of FACA); The Consolidated Appropriations Act, 2008, Pub. L. No. 110-161 (Dec. 26, 2007) (regarding submission of accounting reports; printing and binding; compensation for the executive director; changing annual report due date from June to December; and travel by members of the Commission and its staff); The Carl Levin and Howard P. “Buck” McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291 (Dec. 19, 2014) (regarding responsibilities of the Commission). The Commission’s full charter <http://www.uscc.gov/about/uscc-charter> and Statutory Mandate [http://www.uscc.gov/about/fact\\_sheet](http://www.uscc.gov/about/fact_sheet) are available via the World Wide Web.

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

NOVEMBER 15, 2017

The Honorable Orrin G. Hatch

President Pro Tempore of the U.S. Senate, Washington, DC 20510

The Honorable Paul D. Ryan

Speaker of the U.S. House of Representatives, Washington, DC 20510

DEAR SENATOR HATCH AND SPEAKER RYAN:

On behalf of the U.S.-China Economic and Security Review Commission, we are pleased to transmit the Commission's 2017 Annual Report to the Congress—the fifteenth major Report presented to Congress by the Commission—pursuant to Public Law No. 106–398 (October 30, 2000), as amended by Public Law No. 109–108 (November 22, 2005); as amended by Public Law No. 110–161 (December 26, 2007); as amended by Public Law No. 113–291 (December 19, 2014). This Report responds to the mandate for the Commission “to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People’s Republic of China.” The Commission reached a broad and bipartisan consensus on the contents of this Report, with all 12 members voting to approve and submit it to Congress.

In accordance with our mandate, this Report, which is current as of October 6, includes detailed treatment of our investigations of the areas identified by Congress for our examination and recommendation. These areas are:

- The role of the People’s Republic of China in the proliferation of weapons of mass destruction and other weapon systems (including systems and technologies of a dual use nature), including actions the United States might take to encourage the People’s Republic of China to cease such practices;
- The qualitative and quantitative nature of the transfer of United States production activities to the People’s Republic of China, including the relocation of manufacturing, advanced technology and intellectual property, and research and development facilities, the impact of such transfers on the national security of the United States (including the dependence of the national security industrial base of the United States on imports from China), the economic security of the United States, and employment in the United States, and the adequacy of United States export control laws in relation to the People’s Republic of China;
- The effects of the need for energy and natural resources in the People’s Republic of China on the foreign and military policies of the People’s Republic of China, the impact of the large and growing economy of the People’s Republic of China on world energy and natural resource supplies, prices, and the environment, and the role the United States can play (including through joint research and development efforts and technological assistance) in influencing the energy and natural resource policies of the People’s Republic of China;

- Foreign investment by the United States in the People's Republic of China and by the People's Republic of China in the United States, including an assessment of its economic and security implications, the challenges to market access confronting potential United States investment in the People's Republic of China, and foreign activities by financial institutions in the People's Republic of China;
- The military plans, strategy and doctrine of the People's Republic of China, the structure and organization of the People's Republic of China military, the decision-making process of the People's Republic of China military, the interaction between the civilian and military leadership in the People's Republic of China, the development and promotion process for leaders in the People's Republic of China military, deployments of the People's Republic of China military, resources available to the People's Republic of China military (including the development and execution of budgets and the allocation of funds), force modernization objectives and trends for the People's Republic of China military, and the implications of such objectives and trends for the national security of the United States;
- The strategic economic and security implications of the cyber capabilities and operations of the People's Republic of China;
- The national budget, fiscal policy, monetary policy, capital controls, and currency management practices of the People's Republic of China, their impact on internal stability in the People's Republic of China, and their implications for the United States;
- The drivers, nature, and implications of the growing economic, technological, political, cultural, people-to-people, and security relations of the People's Republic of China's with other countries, regions, and international and regional entities (including multilateral organizations), including the relationship among the United States, Taiwan, and the People's Republic of China;
- The compliance of the People's Republic of China with its commitments to the World Trade Organization, other multilateral commitments, bilateral agreements signed with the United States, commitments made to bilateral science and technology programs, and any other commitments and agreements strategic to the United States (including agreements on intellectual property rights and prison labor imports), and United States enforcement policies with respect to such agreements;
- The implications of restrictions on speech and access to information in the People's Republic of China for its relations with the United States in economic and security policy, as well as any potential impact of media control by the People's Republic of China on United States economic interests; and
- The safety of food, drug, and other products imported from China, the measures used by the People's Republic of China Government and the United States Government to monitor and enforce product safety, and the role the United States can play (including through technical assistance) to improve product safety in the People's Republic of China.

The Commission conducted seven public hearings and one public roundtable, taking testimony from 60 expert witnesses from commercial industries, academia, think tanks, research institutions, and other backgrounds. For each of these hearings, the Commission produced a transcript (posted on its website at [www.uscc.gov](http://www.uscc.gov)). The Commission received a number of briefings by executive branch agencies and the Intelligence Community, including classified briefings on China's military modernization, China's defense and security activities in the Asia Pacific, China's advanced weapons, China's relations with Continental Southeast Asia, Northeast Asia, and Hong Kong, China's aviation industry, and China's cyber activities. The Commission is preparing a classified report to Congress on these and other topics. The Commission also received briefs by foreign diplomatic and military officials as well as U.S. and foreign nongovernmental experts.

Commissioners made official delegation visits to Taiwan, Hong Kong, South Korea, Japan, Thailand, and Burma to hear and discuss perspectives on China and its global and regional activities. In these visits, the Commission delegation met with U.S. diplomats, host government officials, business representatives, academics, journalists, and other experts.

The Commission also relied substantially on the work of our excellent professional staff and supported outside research in accordance with our mandate.

The Report includes 26 recommendations for Congressional action. Our ten most important recommendations appear on page 29 at the conclusion of the Executive Summary.

We offer this Report to Congress in the hope that it will be useful as an updated baseline for assessing progress and challenges in U.S.-China relations.

Thank you for the opportunity to serve. We look forward to continuing to work with you in the upcoming year to address issues of concern in the U.S.-China relationship.

Yours truly,

	
Carolyn Bartholomew Chairman	Dennis C. Shea Vice Chairman



**Commissioners Approving the 2017 Report**


  
Carolyn Bartholomew, Chairman

  
Dennis C. Shea, Vice Chairman

  
Robin Cleveland, Commissioner

  
Byron L. Dorgan, Commissioner

  
Carte P. Goodwin, Commissioner

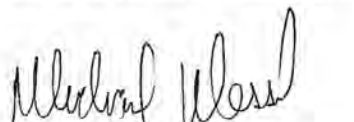
  
Glenn Hubbard, Commissioner

  
Daniel M. Slane, Commissioner

  
Jonathan N. Stivers, Commissioner

  
James M. Talent, Commissioner

  
Katherine C. Tobin, Commissioner

  
Michael R. Wessel, Commissioner

  
Larry M. Wortzel, Commissioner

## CONTENTS

---

	Page
TRANSMITTAL LETTER TO THE CONGRESS .....	iii
COMMISSIONERS APPROVING THE REPORT .....	vi
EXECUTIVE SUMMARY .....	1
KEY RECOMMENDATIONS .....	29
INTRODUCTION .....	31

### 2017 REPORT TO CONGRESS OF THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

<b>Chapter 1: U.S.-China Economic and Trade Relations</b> .....	35
Section 1: Year in Review: Economics and Trade .....	35
Key Findings .....	35
Introduction .....	36
U.S.-China Bilateral Trade .....	37
China's Domestic Economic Rebalancing .....	42
U.S.-China Bilateral Economic Engagement .....	53
United States and China at the WTO .....	58
Section 2: Chinese Investment in the United States .....	71
Key Findings .....	71
Recommendations .....	72
Introduction .....	73
Chinese Investment in the United States .....	73
Chinese Companies on U.S. Stock Exchanges .....	91
Implications for the United States .....	101
Section 3: U.S. Access to China's Consumer Market .....	112
Key Findings .....	112
Recommendations .....	113
Introduction .....	113
E-Commerce .....	114
Logistics .....	124
Financial Services .....	128
Implications for the United States .....	140
<b>Chapter 2: U.S.-China Security Relations</b> .....	153
Section 1: Year in Review: Security and Foreign Affairs .....	153
Key Findings .....	153
Introduction .....	154
Major Developments in China's Security and Foreign Affairs in 2017 .....	154
China's Global Security Activities in 2017 .....	170
U.S.-China Security Relations in 2017 .....	179
Section 2: China's Military Modernization in 2017 .....	199
Key Findings .....	199
Recommendations .....	199
Introduction .....	200
China's 2017 Defense and Security Budget .....	200
Overview of Guidance for Military Modernization .....	201
PLA Army .....	202
PLA Navy .....	203

## VIII

	Page
PLA Air Force .....	207
PLA Rocket Force .....	211
PLA Strategic Support Force .....	212
Implications for the United States .....	214
Section 3: Hotspots along China's Maritime Periphery .....	232
Key Findings .....	232
Recommendations .....	233
Introduction .....	234
Security Environment .....	235
Chinese Strategists' Thinking about Hotspots .....	239
Contingency Planning .....	245
Contingency Operations along China's Maritime Periphery .....	250
Regional Responses and Implications for the United States .....	256
<b>Chapter 3: China and the World</b> .....	281
Section 1: China and Continental Southeast Asia .....	281
Key Findings .....	281
Recommendations .....	283
Introduction .....	283
Chinese Economic Engagement with Continental Southeast Asia .....	284
China's Relations with Burma .....	294
China's Relations with Cambodia .....	305
China's Relations with Laos .....	307
China's Relations with Thailand .....	309
Implications for the United States .....	314
Section 2: China and Northeast Asia .....	326
Key Findings .....	326
Recommendations .....	327
Introduction .....	327
China-North Korea Relations .....	328
China-South Korea Relations .....	342
China-Japan Relations .....	349
South Korea-Japan Relations and Trilateral Security Cooperation .....	355
Implications for the United States .....	357
Section 3: China and Taiwan .....	371
Key Findings .....	371
Recommendations .....	372
Introduction .....	372
Cross-Strait Relations .....	373
Taiwan's Economy and Cross-Strait Trade and Investment .....	382
Taiwan's International Engagement .....	386
Taiwan Military and Security Issues .....	389
U.S.-Taiwan Relations .....	397
Implications for the United States .....	401
Section 4: China and Hong Kong .....	414
Key Findings .....	414
Recommendations .....	415
Introduction .....	415
Hong Kong's Political Developments .....	416
Beijing's Degradation of Rule of Law in Hong Kong .....	425
Declining Freedom of Expression in Hong Kong .....	427
Economic Relations with Mainland China .....	435
Implications for the United States .....	439
Section 5: China's Domestic Information Controls, Global Media Influence, and Cyber Diplomacy .....	452
Key Findings .....	452
Recommendations .....	452
Introduction .....	453
China's Domestic Information Controls .....	454
China's Global Media Influence .....	467
Beijing's Concept of "Internet Sovereignty" .....	482
Implications for the United States .....	484

## IX

	Page
<b>Chapter 4: China's High-Tech Development</b> .....	507
Section 1: China's Pursuit of Dominance in Computing, Robotics, and Biotechnology .....	507
Key Findings .....	507
Recommendations .....	508
Introduction .....	508
China's Industrial Policies .....	509
Computing .....	515
Industrial Robotics .....	523
Artificial Intelligence .....	525
Nanotechnology .....	527
Biotechnology .....	528
Implications for the United States .....	531
Section 2: China's Pursuit of Advanced Weapons .....	553
Key Findings .....	553
Introduction .....	554
Drivers of China's Advanced Weapons Programs .....	554
China's Advanced Weapons Programs .....	557
Inputs to China's Advanced Weapons Programs .....	577
Implications for the United States .....	580
<b>Comprehensive List of the Commission's Recommendations</b> .....	597
<b>Additional Views of Commissioners</b> .....	602
 <b>Appendices:</b>	
Appendix I: Charter .....	605
Appendix II: Background of Commissioners .....	613
Appendix III: Public Hearings of the Commission During 2017 .....	625
Appendix IIIA: List of Witnesses Testifying Before the Commission During 2017 .....	629
Appendix IV: List of Research Material .....	633
Appendix V: Conflict of Interest and Lobbying Disclosure Reporting .....	637
Appendix VI: Acronyms and Abbreviations .....	639
<b>2017 Commission Staff and Acknowledgements</b> .....	643

## **EXECUTIVE SUMMARY**

### **Chapter 1: U.S.-China Economic and Trade Relations**

#### **Section 1: Year in Review: Economics and Trade**

In 2017, main priorities for the Chinese government appear to be increased Party control and consolidation of political power. Indeed, the administration of the Chinese President and General Secretary of the Chinese Communist Party (CCP) Xi Jinping has begun implementing policies in pursuit of these goals to prepare for the leadership transition due to take place at 19th Party Congress in October 2017. Despite President Xi's stated commitment in 2013 to allow market forces to play "a decisive role" in the economy, genuine liberalization has not only stalled, but has also been backsliding.

To stimulate the economy, China's government continues to rely on old standbys, such as investment in infrastructure and real estate, and funding the state sector to the detriment of private enterprise and market orientation. The amount of credit the government is pumping into the economy has swelled to levels not seen since the global financial crisis, and corporate debt has continued to climb to new heights. The Chinese government is dramatically expanding investment in new technology and industries.

The hand of the state is also evident in how Beijing treats foreign companies operating in China and in the impact its trade-distorting policies have on its trade partners. Beijing's discriminatory treatment of U.S. companies and ongoing failure to uphold its World Trade Organization (WTO) obligations continue to damage the bilateral relationship. The U.S. trade deficit in goods with China totaled \$347 billion in 2016, the second-highest deficit on record. In the first eight months of 2017, the goods deficit reached \$239.1 billion, and is on track to surpass last year's deficit. U.S. companies are feeling increasingly pressured by Chinese policies that demand technology transfers as a price of admission and favor domestic competitors. According to a survey by the American Chamber of Commerce in China, 81 percent of U.S. firms doing business in China reported feeling less welcome in 2016 than they did in 2015.

#### ***Key Findings***

- In 2016 and the first half of 2017, the Chinese government has reported it met or exceeded the targets it set for gross domestic product (GDP) growth—an important deliverable in advance of the political leadership transitions at the Chinese Communist Party's 19th Party Congress scheduled for October 2017. The Chinese government has achieved this high growth through reliance on old drivers: credit and real estate. However, the government's unwillingness to allow the market to play a bigger role has resulted in deteriorating investment efficiency,

meaning higher levels of debt are necessary to generate growth. Household consumption—an essential element of China’s economic rebalancing—is growing but at a sluggish pace due to the slow rate of reform.

- China’s high and rising debt levels pose a growing threat to the country’s financial stability. China’s total debt reached \$27.5 trillion, or 257 percent of GDP, at the end of 2016. The dramatic rise in China’s debt burden can be attributed to the relentless expansion of credit the government has relied on to generate growth since the global financial crisis.
- The U.S. trade deficit in goods with China totaled \$347 billion in 2016, the second-highest deficit on record. In the first eight months of 2017, the goods deficit increased 6.2 percent year-on-year to \$239.1 billion, with U.S. exports to China reaching \$80.2 billion, an increase of 15 percent year-on-year, while imports from China grew 8.3 percent year-on-year to \$319.3 billion. In 2016, the U.S. services trade surplus with China reached a record high of \$37 billion, driven almost entirely by an increase in Chinese tourism to the United States.
- China’s foreign investment climate continues to deteriorate as government policy contributes to rising protectionism and unfair regulatory restrictions on U.S. companies operating in China. The newly implemented cybersecurity law illustrates this trend. The law contains data localization requirements and a security review process U.S. and foreign firms claim can be used to discriminatorily advantage Chinese businesses or access proprietary information from foreign firms.
- U.S. government efforts to tackle China’s trade-distorting practices continue to yield limited results. The inaugural Comprehensive Economic Dialogue, created following a meeting between President Trump and President Xi in April 2017, concluded with no concrete agreements or future agenda.
- At the World Trade Organization (WTO), the United States continues to challenge China’s non-compliance with key provisions of its accession agreement, including failure to notify subsidies. In the past year, the United States requested WTO consultations over China’s management of tariff rate quotas for rice, wheat, and corn, and subsidies to select producers of primary aluminum.

## **Section 2: Chinese Investment in the United States**

Flows of Chinese foreign direct investment (FDI) to the United States have increased dramatically in recent years, fueled by Chinese government policies encouraging FDI in pursuit of gaining market access, new technologies, and higher returns abroad. As a result, reviews of Chinese investments by the Committee on Foreign Investment in the United States (CFIUS) are growing in number and complexity. Three important trends have emerged that may impact CFIUS’s ability to review Chinese investments in the United States:



First, Chinese FDI is targeting industries deemed strategic by the Chinese government, including information and communications technology, agriculture, and biotechnology. These investments lead to the transfer of valuable U.S. assets, intellectual property, and technology to China, presenting potential risks to critical U.S. economic and national security interests. In many of these sectors, U.S. firms also lack reciprocal treatment in China and are forced to disclose valuable technologies and source code to gain access to the Chinese market.

Second, some private Chinese companies operating in strategic sectors are private only in name, with the Chinese government using an array of measures, including financial support and other incentives, as well as coercion, to influence private business decisions and achieve state goals. This complicates the job of regulators and puts U.S. companies in these sectors at a distinct disadvantage, with their Chinese counterparts making business decisions based on political interests and with the financial backing of the state.

Third, some Chinese companies are attempting to invest in sensitive U.S. industries without obeying normal U.S. regulatory procedures. Their methods may include facilitating investments through shell companies based outside of China and conducting cyber espionage campaigns to financially weaken and then acquire U.S. firms. These methods not only injure U.S. businesses, but also hinder CFI-US's ability to review investments for potential threats to U.S. national security.

Chinese firms' activities on U.S. capital markets also present challenges for U.S. financial regulators and investors. Chinese laws governing the protection of state secrets and national security prohibit Chinese firms from sharing their audit work reports with foreign regulators, preventing the Public Company Accounting Oversight Board (PCAOB) from inspecting certified public accounting firms in China and Hong Kong. This leaves U.S. investors exposed to potentially exploitative and fraudulent activities by Chinese firms listed in the United States. To date, the Securities and Exchange Commission and PCAOB have been unable to reach an agreement with Chinese regulators to address the inadequacies of China's disclosure practices. After a decade of negotiations with Chinese regulators, it is apparent that, absent a dramatic policy shift, Beijing is unlikely to cooperate with efforts to make Chinese firms more accountable to their U.S. investors.

### ***Key Findings***

- Chinese government policies, coupled with increased investor uncertainty in China, have contributed to increased investment flows to the United States in recent years. In 2017, Chinese investment flows to the United States are expected to decline relative to 2016 as the Chinese government seeks to limit capital outflows and fend off risks from mounting corporate debt.
- Sectors of the U.S. economy deemed strategic by the Chinese government are more likely to be targeted by Chinese firms for investment, while Chinese investments in nonstrategic sectors like entertainment, real estate, and hospitality are declining

amid Chinese Communist Party efforts to limit capital outflows and reduce corporate debt.

- Some Chinese firms seek to obscure their dealings in the United States through U.S.-based shell companies or attempt to drive down the value of U.S. assets through sophisticated cyber espionage campaigns. These firms are becoming more sophisticated in their attempts to circumvent Committee on Foreign Investment in the United States (CFIUS) reviews and other U.S. investment regulations.
- Greenfield investments in the United States are not subject to the CFIUS review process, which may raise national security risks. Although the number of Chinese greenfield investments in the United States remains limited compared to acquisitions of U.S. assets, federal laws and screening mechanisms do not sufficiently require federal authorities to evaluate whether a greenfield investment may pose a national security threat.
- The application of the sovereign immunity defense to commercial cases presents a potential risk for U.S. businesses and individuals, allowing Chinese state-owned enterprises (SOEs) to conduct unlawful activity in the United States without legal consequences. Some Chinese SOEs are evading legal action in the United States by invoking their status as a foreign government entity under the Foreign Sovereign Immunities Act.
- The opaque nature of China's financial system makes it impossible to verify the accuracy of Chinese companies' financial disclosures and auditing reports. Chinese businesses continue to list on U.S. stock exchanges to raise capital, despite operating outside the laws and regulations governing U.S. firms.
- U.S. regulators have struggled to deter Chinese fraud schemes on U.S. exchanges, with Chinese issuers stealing billions of dollars from U.S. investors. Efforts to prosecute the issuers of the fraudulent securities have been unsuccessful, with Chinese regulators choosing not to pursue firms or individuals for crimes committed by Chinese companies listed overseas.
- Some Chinese companies operate with little oversight under China's opaque financial system, leaving U.S. investors exposed to exploitative and fraudulent schemes perpetrated by China-based issuers. Negotiations between the Public Company Accounting Oversight Board and its counterparts in China have resulted in little progress toward securing increased cross-border transparency and accountability.

### **Section 3: U.S. Access to China's Consumer Market**

China's strong income growth, expanding middle class, and stated plans to rebalance to a more consumption-driven economy should further boost U.S. services trade with China. In particular, the rapid growth in China's e-commerce, logistics, and financial services sectors presents opportunities for U.S. companies. Services are the mainstay of the U.S. economy, accounting for 80 percent of private sector jobs. The United States maintains a sizable services trade

surplus with China, which reached \$38 billion in 2016, up from \$438 million in 2006.

Despite the potential for U.S. companies, the playing field in China's consumer market remains uneven and highlights a lack of reciprocity in market access. China maintains market access barriers that restrict U.S. services companies, including caps on foreign equity, discriminatory licensing requirements, and data localization policies. Although China has gradually opened up its services sector to foreign participation, the pace has been slow and it may be increasingly difficult for U.S. companies to become significant players. For example, while China's regulatory framework for foreign investment in the e-commerce sector has undergone significant liberalization over the last two years, China's e-commerce market already is highly saturated, with Alibaba and JD.com holding more than 80 percent market share combined. Still, China's e-commerce boom could offer opportunities for U.S. retailers and brands due to growing Chinese demand for foreign products, particularly in areas where the United States excels, such as high-quality foods and supplements, beauty products, and healthcare-related goods.

China's consumer market is being reshaped by the country's major technology companies. Armed with government support, capital reserves, and troves of consumer data, these companies came to dominate China's market by integrating social media, e-commerce, and financial services to capture increasing swaths of the consumer experience. China's restrictions on foreign participation in the country's digital ecosystem limit the ability of U.S. companies to similarly leverage Chinese consumer data. In addition, state-owned enterprises remain major players in the services sector, particularly in banking, transportation, and telecommunications. U.S. firms cannot go toe-to-toe with China's technology giants and state-owned enterprises, and in most consumer segments, are largely relegated to partnering with domestic firms. U.S. services trade with China cannot reach its full potential as long as these barriers remain.

### ***Key Findings***

- China's rebalancing to a more consumption-driven growth model should present opportunities for U.S. companies in the e-commerce, logistics, and financial services sectors. However, U.S. companies operating in China do not have a level playing field and continue to face significant market access challenges, including informal bans on entry, caps on foreign equity, licensing delays, and data localization policies.
- China is the largest e-commerce market in the world, with e-commerce sales reaching \$787 billion in 2016. According to the U.S. Department of Commerce, by 2019 an estimated one out of every three retail dollars in China will be spent online, the highest percentage in the world. Although China has traditionally provided the world with its manufactured goods, its e-commerce boom should offer increased opportunities for U.S. retailers and brands, with more and more Chinese consumers purchasing foreign goods. Demand is strong in areas where the United States excels, such as high-quality foods and supplements, beauty products, and healthcare-related goods.

- Although China's e-commerce market offers opportunities for U.S. retailers and brands, it is not without its challenges and risks. While the Chinese government has made some improvements in enforcing intellectual property rights, intellectual property issues remain a key challenge for U.S. companies operating in China. In particular, the prevalence of counterfeit goods on Chinese e-commerce platforms continues to hurt U.S. retailers and brands.
- E-commerce has been a key driver of improvements to China's \$2.2-trillion-dollar logistics sector. Yet, China's domestic logistics industry remains underdeveloped, due to the country's historical focus on improving export logistics at the expense of domestic logistics infrastructure. This has caused logistics to become a major bottleneck for China's e-commerce sector. China's efforts to develop and modernize its express delivery industry could offer U.S. logistics firms like FedEx and UPS opportunities to expand their China operations.
- Financial services have been a major driver of growth within China's services sector, increasing 11 percent annually from 2012 to 2016. However, Chinese consumers' access to financial services remains inadequate, and most Chinese consumers lack formal credit histories. Improving their access to financial services will be critical for raising domestic consumption levels. In addition, China has made limited progress in implementing reforms to improve the market orientation and efficiency of its financial sector.
- Financial services are a mainstay of the U.S. economy and a major services export to China. While China has taken some steps to expand foreign firms' access to its financial markets since joining the World Trade Organization, U.S. financial services companies continue to face significant market access barriers in China. These include informal and formal bans on entry, equity caps, licensing restrictions, and data localization requirements. China's new cybersecurity law poses additional challenges for U.S. financial institutions operating in China. As a result, U.S. firms' market share in China's financial sector has been stagnant or declining in recent years.
- China has become a global leader in financial technology. China's Internet giants have emerged as significant players not only in e-commerce and logistics, but also in China's financial services sector, particularly in payments and lending.

## **Chapter 2: U.S.-China Security Relations**

### **Section 1: Year in Review: Security and Foreign Affairs**

The year 2017 saw the continued expansion of China's military and other security activities in pursuit of national interests close to home and far afield. Beijing employed a mix of coercion and engagement to further these interests.

Throughout 2017, Beijing tightened its effective control over the South China Sea by continuing to militarize the artificial islands it occupies there and by pressuring other claimants and regional coun-

tries to accept its dominance. It has not been deterred by, and in fact has rejected, the 2016 ruling by the Permanent Court of Arbitration in The Hague, which found much of China's claims and activities in the South China Sea to be unlawful. China increased tensions in other ways, including by illegally seizing a U.S. Navy underwater unmanned vehicle. China also sought to advance its territorial claims in South Asia by building a road into a disputed portion of the China-Bhutan-India border. This led to a two-month standoff between Chinese and Indian border forces, which ultimately ended peacefully.

China also advanced its interests through its ongoing One Belt, One Road initiative, and enhanced security cooperation with countries around the world. Currently, One Belt, One Road incorporates around 60 countries and reportedly includes \$900 billion worth of current or planned projects. Championed by President Xi, the initiative is ostensibly an economic endeavor intended to bring infrastructure projects, connectivity, and economic growth to Eurasia and beyond. It also has several unspoken strategic objectives: establishing strategic access points for China around the world, primarily via port infrastructure; augmenting China's energy security with a network of pipelines and energy projects; expanding domestic and regional security and stability by countering fundamentalism and terrorism; and gaining influence and leverage (and countering U.S. influence) over other countries.

As China's economic and strategic interests expand outward, China's security engagement has followed. China was the third-largest arms exporter worldwide in aggregate terms in the time period 2012–2016, and has sold arms to 44 countries. Meanwhile, the People's Liberation Army (PLA) has increased military-to-military engagement with other militaries. In 2017, China deployed its 27th naval task group for antipiracy patrols in the Gulf of Aden, where it has conducted more than 1,000 escort missions since 2008. Further, China expanded its involvement in UN peacekeeping activities, deploying a 140-soldier helicopter unit for peacekeeping purposes for the first time (to the Darfur region of Sudan). China also opened its first overseas military base, in Djibouti, in 2017. According to Beijing, the base will mainly be used to provide assistance to Chinese forces conducting antipiracy, peacekeeping, and humanitarian missions in the region. Its strategic location—several miles from Camp Lemonnier, one of the largest and most critical U.S. military installations abroad—may enable the PLA to surveil U.S. military activities.

Despite efforts by the Xi and Trump governments to set a positive tone for U.S.-China ties, tensions over security issues remain at the forefront of the relationship, with the South China Sea, Taiwan, and especially North Korea as the primary flashpoints.

### ***Key Findings***

- China's territorial disputes in the South China Sea and in South Asia flared in 2017. China continued to rely primarily on non-military and semiofficial actors (such as the China Coast Guard and maritime militia) to advance its interests in the disputed South China Sea, straining already-unsettled relations with the

Philippines and Vietnam. The 2016 ruling by the Permanent Court of Arbitration in The Hague, which overwhelmingly sided against China's position, has not deterred Beijing. China's territorial assertiveness was also on display when Chinese armed forces attempted to consolidate control over territory disputed by Bhutan and India. Ultimately, India was more successful than the Philippines and Vietnam in countering Chinese coercion.

- China's One Belt, One Road initiative continued to expand in 2017. Although China claims the mega-project is primarily economic in nature, strategic imperatives are at the heart of the initiative. China aims to use One Belt, One Road projects to expand its access to strategically important places, particularly in the Indian Ocean; to enhance its energy security; and to increase its leverage and influence over other countries.
- The People's Liberation Army continues to extend its presence outside of China's immediate periphery by opening its first overseas military base in Djibouti, increasing its contributions to UN peacekeeping operations, and conducting more bilateral and multilateral exercises. China's arms exports continued to grow in volume and sophistication in 2017, although they remain limited to low- and middle-income countries and are dwarfed by U.S. and Russian sales in value. The People's Liberation Army's expanded exercise portfolio includes new partners, such as Burma and Nepal, as well as long-time partners Pakistan and Russia. China's defense ties with Russia continued an upward trend in 2017.
- U.S.-China security relations saw new dialogue formats emerge following the U.S. presidential transition, but were marked by growing tension due to disagreements over issues such as North Korean denuclearization and China's continued coercive actions in regional territorial disputes.

## **Section 2: China's Military Modernization in 2017**

China is pursuing military modernization efforts to improve its antiaccess/area denial, warfighting, force projection, and nuclear deterrence capabilities, in addition to developing capabilities to conduct operations in space and cyberspace. The forces under development, supported by a still-growing military budget (announced to be \$151.1 billion for 2017, but likely to be much higher), provide China the capability to conduct military operations beyond its land borders and into disputed waters along its maritime periphery in the East and South China seas. China's ongoing military modernization disrupts stability in East and Southeast Asia and creates challenges for U.S. freedom of action in the region.

The ground forces remain relevant to many PLA missions, such as defending China's land borders and responding to a Taiwan crisis. PLA Army modernization efforts are focused on developing a smaller and more mobile force that is well-suited for offensive operations and overseas missions. This ground force modernization into a "new-type Army" is focused on the development of special operations, helicopter, electronic warfare, light mechanized, and long-range artillery



units. This expanding capability could result in U.S. and Chinese forces conducting missions within the same operational space.

To extend the PLA Navy's operational presence in line with Beijing's new strategic assessment that "the traditional mentality that land outweighs sea must be abandoned," China is developing aircraft carriers and carrier aviation, large amphibious ships suited for expeditionary operations, and multi-mission surface combatants and corvette class ships, and is modernizing the submarine force. This is resulting in Chinese ships conducting missions further from China and in proximity to U.S. forces operating in the Indo-Pacific. The U.S. Navy should anticipate a larger forward operational presence by the PLA Navy in the Indo-Pacific at the outset of conflict should a crisis escalate to hostilities.

The PLA Air Force's efforts are focused on developing long-range strike, fifth-generation fighter, airborne early warning and control, aerial refueling, strategic lift, air defense, and intelligence, surveillance, and reconnaissance aircraft. These types of developments are enhancing the ability of the PLA Air Force to conduct air operations farther from China's coast. These air operations have included simulated strike training and patrols over waters between Japan and Taiwan (the Miyako Strait) and between Taiwan and the Philippines (the Bashi Channel), which are sensitive and strategic waters for U.S. allies, friends, and partners in the region.

The PLA Rocket Force continues to improve both its conventional and nuclear forces to enhance long-range strike and deterrence capabilities and is modernizing its forces to increase the reliability and effectiveness of both conventional and nuclear missile systems. One objective of missile force modernization is for China to maintain nuclear forces capable of inflicting enough damage to deter a nuclear attack. China likewise seeks to extend the range of its conventional precision strike capabilities to hold adversary assets at risk at greater distances from China's coastline in the event of a regional conflict, eroding the United States' ability to operate freely in the Western Pacific.

The Strategic Support Force—with responsibility for cyber, electronic, information, and space operations—was established in December 2015 as part of China's military reform and reorganization. This force has incorporated signals intelligence capabilities, electronic warfare and electronic countermeasures, as well as aerospace reconnaissance capabilities. Considering the type of support the Strategic Support Force is expected to provide China's ground, naval, air, and missile forces, the United States must assume it will contribute to antiaccess/area denial operations against forward-deployed U.S. troops should a conflict occur in the region.

### ***Key Findings***

- China's military modernization program seeks to advance Beijing's security interests, prevent other countries from challenging those interests, and defend China's sovereignty claims to disputed areas along its border and maritime periphery. The weapons and systems under development and those that are being fielded by China's military—such as intermediate-range ballistic missiles, bombers with long-range precision strike capabilities, and guided missile nuclear attack submarines—are

intended to provide China the capability to strike targets further from shore, such as Guam, and potentially complicate U.S. responses to crises involving China in the Indo-Pacific.

- China will continue to modernize strategic air and sea lift capabilities, which will enable China's military to conduct expeditionary operations. The continued production of the Chinese navy's amphibious lift ships and the air force's heavy lift transport aircraft will increase China's ability to deliver troops abroad and to conduct expeditionary operations beyond the first island chain, humanitarian assistance operations, and noncombatant evacuation operations.
- China's increasingly accurate and advanced missile forces are intended to erode the ability of the United States to operate freely in the region in the event of a conflict and are capable of holding U.S. forces in the region at risk.
- China's continued focus on developing counterspace capabilities indicates Beijing seeks to hold U.S. intelligence, surveillance, and reconnaissance satellites at risk in the event of conflict.
- The consolidation of space, cyber, electronic warfare, signals, and potentially human intelligence capabilities under the Strategic Support Force provides China a centralized all-source intelligence apparatus to support national-level decision makers. Furthermore, this development could strengthen the Chinese military's ability to conduct integrated joint operations by providing a wide range of collection capabilities including intelligence, surveillance, and reconnaissance support to commanders responsible for operational forces under the military's five theater commands.

### **Section 3: Hotspots along China's Maritime Periphery**

Taiwan, the South China Sea (particularly the Spratly Islands), and the East China Sea (particularly the Senkaku Islands) are major national security interests for China. They also are major sources of tension between China and its neighbors. Complex challenges related to sovereignty and control, access to strategic waterways and resources, nationalism, and alliance and competition dynamics make these areas "hotspots" that could result in armed conflict between China and its neighbors. China's expanding territorial ambitions and its desire to exploit the current so-called "period of strategic opportunity" could invite the risk of conflict, and so the PLA is preparing contingency plans accordingly.

Chinese strategic writings insist unification with Taiwan is "inevitable," and unification by force remains the primary mission for which the PLA trains. Although the risk of large-scale war is remote, brinkmanship or a crisis compounded by miscommunication or miscalculation could spiral into conflict. Cross-Strait instability, which has been exacerbated by Beijing's recent pressure campaign against Taiwan's current government, is increasing the risk of hostilities between China and Taiwan. The PLA is planning for a range of Taiwan contingency operations that likely scale from punitive missile strikes to coerce Taiwan's political leadership to a full-scale invasion of the island. However, a Taiwan landing operation is the most difficult option for the PLA and would require China taking

and holding ports and airfields, in addition to conducting amphibious landings, in an effort to seize the island.

Disputes over islands and other land features in the South China Sea could easily escalate into crises, and in fact already have (notably with China's seizure and effective blockade of Philippines-claimed Scarborough Reef in 2012 and the destructive skirmish between Chinese and Vietnamese non-naval forces over a Chinese oil rig in 2014). Should China perceive an intolerable challenge to its claimed sovereignty over one of these disputed areas, it could employ a range of options—including island landing operations, blockades, or missile strikes—to seize control of disputed features. Such operations likely would involve (perhaps even exclusively) its non-naval maritime forces, such as the China Coast Guard and maritime militia, creating operational uncertainty and “grey zone” challenges for adversaries. A conflict involving the Philippines would raise the prospect of the United States—a treaty ally of the Philippines—becoming involved.

The risk of conflict in the East China Sea shifts as overall tensions in the region ebb and flow, but the nature of the China-Japan rivalry is such that any confrontation over the disputed Senkaku Islands could quickly escalate into an armed conflict. As with a South China Sea contingency, non-naval forces likely would play a leading role with naval assets waiting over the horizon. Other potential avenues for seizing the islands could involve China feigning a naval exercise near the islands that quickly turns into an island seizure campaign, or executing a joint amphibious assault to capture and occupy the islands. A Chinese attack on the Senkakus, which are covered by the U.S.-Japan Defense Treaty, would prompt U.S. involvement.

### ***Key Findings***

- U.S. presence and alliance commitments have helped maintain regional stability in Asia. China's aggressive actions in the East China Sea, South China Sea, and Taiwan Strait threaten principles such as freedom of navigation, the use of international law to settle disputes, and free trade. If Beijing continues to increase its control over the East and South China seas, the United States could receive requests for additional assistance by allies, friends, and partners to improve their capabilities to defend themselves, along with calls for the United States to remain engaged in the region to maintain security and stability.
- With China actively preparing contingency plans for operations against U.S. allies, friends, and partners along China's maritime periphery, the United States and China could quickly become involved in a conflict if Beijing escalates. This risk becomes greater depending on the level of tensions associated with any of the following flashpoints: the Korean Peninsula, the South China Sea, the East China Sea, and cross-Strait relations.
- Chinese leaders are cautious about letting a crisis escalate into conflict, and Chinese military thinkers study “war control” as a method for limiting the scope of a conflict to minimize negative consequences and achieve a victory at minimal cost. However, if Beijing believes the risk of a response to Chinese action is low, China may be tempted to risk brinksmanship to achieve its national objectives. Furthermore, if Beijing is unable to avoid es-

calation, any crises involving the use of the People's Liberation Army (PLA) create opportunities to widen a crisis into a conflict that results in the use of force.

- China has emphasized building a military capable of responding to situations in multiple regions and has developed theater commands capable of planning and executing missions in their respective areas of responsibility. A key element of success in achieving operational objectives, however, will be managing resources across multiple theaters should China find itself challenged in multiple directions simultaneously. This could create an opportunity to dissuade Chinese aggression or potentially result in Beijing escalating or accelerating a conflict.
- The PLA presently lacks the amphibious lift to directly assault Taiwan, and would instead have to successfully seize ports and airfields for the flow of follow-on forces to conduct on-island operations. Likewise, sustaining a prolonged air and maritime blockade against Taiwan is likely to strain PLA logistical capabilities, potentially disrupt trade routes through East Asia, and inhibit freedom of navigation in the region. These are high-risk operations for China, and may be conducted only after other coercive options are exhausted.
- Military facilities currently under construction in the Spratly Islands are intended to improve the PLA's operational reach by strengthening logistical support, extending operational reach, and bolstering the military's capability to monitor potential adversaries. Once these outposts are completed, they will improve the PLA's ability to take action against Vietnamese or Filipino forces on adjacent features if so ordered. China's militarization of these features is therefore inherently destabilizing for its neighbors who have overlapping sovereignty claims.
- There are several U.S. alliances and other commitments that could be activated by a maritime hotspot conflict with Japan, the Philippines, or Taiwan. Depending on the scenario, the United States could be expected to become involved in a conflict, although China will seek to discourage this by many means, possibly to include ensuring conflict remains in the "grey zone" where U.S. defense commitments are uncertain and the onus of escalation is shifted to China's adversary.
- The forward presence of U.S. forces in East Asia, coupled with the treaty alliances and partnerships of the United States in the region, constitute the most important factor in deterring Chinese adventurism. Nevertheless, they also increase the likelihood, should deterrence fail, that the United States becomes involved in armed conflict. The Commission has documented in previous reports how the balance of military power in the region has shifted in China's direction. Should that shift continue without a change in U.S. policy, there is a danger that Chinese leaders will consider the United States an obstacle to their ambitions that must be removed. In that event, Beijing may decide to escalate a crisis when the circumstances seem favorable to the achievement of China's larger ambitions.

### **Chapter 3: China and the World**

#### **Section 1: China and Continental Southeast Asia**

China's relations with Burma (Myanmar), Cambodia, Laos, and Thailand are driven by two broad goals: taking advantage of Southeast Asia's economic potential and balancing the region's geopolitical opportunities against its security vulnerabilities. In pursuit of these goals, China has leveraged its economic importance to Southeast Asia and capitalized on regional countries' infrastructure needs. China has also forged ties with key regional political groups, particularly in Burma where China has supported different sides of Burma's ethnic conflict.

Economically, the region boasts some of the highest growth rates in the world as well as valuable mineral and agricultural resources, such as Burma's \$31 billion jade trade. China uses a number of tactics to exploit the region—including trade links, infrastructure projects, and assistance packages—in a way that benefits China's economic interests. For example, Chinese infrastructure projects in the region will help give Chinese exporters a competitive edge in regional markets and ameliorate excess capacity in China's construction sector. Chinese firms have also invested in plantations and mineral extraction projects that have harmed host countries, including jade smuggling in Burma and pesticide-heavy plantations in Laos that have left thousands of workers sick.

Geopolitically, China desires stability and leverage along its 1,370 mile border with Burma where fighting between ethnic armed groups and Burma's army has claimed the lives of Chinese citizens. China sees an opportunity to bypass its energy supply vulnerabilities in the Strait of Malacca by establishing transportation corridors through Burma and has built oil and natural gas pipelines connecting China to Burma's Indian Ocean coast, where China seeks to control a key port. China has used regional countries' membership in the Association of Southeast Nations (ASEAN) to its advantage—China's financial support and close relationship with Cambodia has been pivotal to preventing joint ASEAN opposition to China's land reclamation in the South China Sea. Finally, following the coup in Thailand, China has sought to move closer to the U.S. treaty ally, and has exceeded the United States in arms sales to Thailand, although the degree to which Thai-China ties have improved is uncertain.

China's engagement with the region has challenged U.S. commercial interests and political values. China's business and development model often runs counter to U.S. priorities, such as fostering transparent, accountable government in a region where democracy is challenged. Chinese firms exploit corruption, particularly in Cambodia where quid-pro-quo relationships between Chinese businesses and Cambodian officials thrive. These corrupt environments put U.S. firms at a disadvantage. Chinese projects also exacerbate social instability through environmental damage and community displacement. In particular, Chinese dams on the Mekong River threaten the food security of 60 million people, creating significant stability risks. Despite the region's importance to U.S. interests, U.S. assistance appears to lag significantly behind China's commitments, creating a risk that U.S. priorities will continue to be undermined by China's engagement.



***Key Findings***

- China's pursuit of strategic and economic interests in Burma (Myanmar), Thailand, Cambodia, and Laos often jeopardizes regional environmental conditions, threatens government accountability, and undermines commercial opportunities for U.S. firms.
- China has promoted a model of development in continental Southeast Asia that focuses on economic growth, to the exclusion of political liberalization and social capacity building. This model runs counter to U.S. geopolitical and business interests as Chinese business practices place U.S. firms at a disadvantage in some of Southeast Asia's fastest-growing economies, particularly through behavior that facilitates corruption.
- China pursues several complementary goals in continental Southeast Asia, including bypassing the Strait of Malacca via an overland route in Burma, constructing north-south infrastructure networks linking Kunming to Singapore through Laos, Thailand, Burma, and Vietnam, and increasing export opportunities in the region. The Chinese government also desires to increase control and leverage over Burma along its 1,370-mile-long border, which is both porous and the setting for conflict between ethnic armed groups (EAGs) and the Burmese military. Chinese firms have invested in exploiting natural resources, particularly jade in Burma, agricultural land in Laos, and hydropower resources in Burma and along the Mekong River. China also seeks closer relations with Thailand, a U.S. treaty ally, particularly through military cooperation.
- As much as 82 percent of Chinese imported oil is shipped through the Strait of Malacca making it vulnerable to disruption. To reduce this vulnerability, China has been investing in oil and natural gas pipelines across Burma, which will partially alleviate this problem, supplying China with up to 5 percent of its oil imports and 6 percent of its natural gas imports based on 2016 data.
- Chinese dams on the Mekong River threaten Laos, Cambodia, and Vietnam's food security by blocking sediment necessary for agriculture and restricting fish migration. Chinese dams are poised to block half of the sediment in the river system and the dam network on the Lower Mekong is estimated to reduce the fish stock of the entire river system by 42 percent.
- Local resistance to Chinese development has stalled or closed several important Chinese projects, including the \$3.6 billion Myitsone Dam in Burma and a railway linking Kunming to the Indian Ocean. Protests against Chinese projects have emerged over environmental concerns, use of Chinese laborers, and contract terms that primarily benefit Chinese firms. Chinese business practices have created friction in Laos and Thailand where Chinese businesses have been closed by the government.
- Japan remains a competitor in continental Southeast Asia for infrastructure development. In 2016, Japan pledged to provide \$6.8 billion in infrastructure finance for Mekong River countries. Japan typically supports infrastructure projects that run

east-west across the region while China constructs projects that run north-south.

- Cambodia has advocated for China's interests in the Association of Southeast Asian Nations (ASEAN), particularly regarding Chinese land reclamation in the South China Sea. In 2012 and 2016 Cambodia vetoed joint ASEAN resolutions containing language regarding the South China Sea objectionable to the Chinese government, reportedly in concert with Beijing. Beijing has contributed significantly more aid to Cambodia than the United States and other Western countries. Cambodia's government has also granted Chinese businesses special privileges in violation of its own regulations. These privileges appear linked to favors paid to Cambodian officials by Chinese firms.
- Laos has sought good relations with China and turned to China for infrastructure development and investment, but has grown uneasy over the influence China has gained through investment. This unease has caused Laos to rethink its relations with China. In 2016 the Lao People's Revolutionary Party removed Choummaly Sayasone, who was associated with granting economic concessions to Chinese firms as chief of the party.
- China faces a more complicated political landscape in Burma, including the National League for Democracy (NLD) government; the military, which retains considerable political power; and EAGs that control large segments of Burma and conduct military actions against the Burmese government and military. In response, China has leveraged its connections with all three groups to maximize its influence, establishing better relations with the NLD, maintaining contact with military leaders, and using its ties to EAGs to demonstrate its ability to influence Burma's peace process. In leveraging its ties with EAGs, China faces tension between securing stability in its borders and using EAGs and Burma's peace process to obtain influence over the NLD government.
- After U.S.-Thailand relations deteriorated following the 2014 coup, China and Thailand have signed a series of arms deals, including a \$393 million submarine purchase. Thailand may be following its historical tradition of balancing multiple powers in its closer military relationship with Beijing.

## **Section 2: China and Northeast Asia**

Northeast Asia—encompassing China, Japan, North Korea, and South Korea—is the locus of some of the most pressing security challenges in Asia. Two of these countries—Japan and South Korea—are U.S. treaty allies. North Korea, on the other hand, is highly antagonistic to the United States and a threat to global peace and security.

Although Beijing increasingly is frustrated and concerned by Pyongyang's missile and nuclear testing and escalatory rhetoric, China is North Korea's top trading partner, most reliable supporter, and treaty ally. China is necessarily a key player in any significant international effort to manage the North Korean threat, and took some steps to strengthen international sanctions against North Ko-

rea in 2017. It is too soon to measure China's compliance with the latest rounds of sanctions, which, if implemented fully, would significantly constrain the North Korean regime's ability to fund its nuclear and conventional weapons programs. Given China's lackluster record of previous sanctions enforcement and continued sanctions violations by Chinese companies exporting dual-use items to North Korea, however, the United States and the international community should keep their expectations low. China's reluctance to assist with the U.S.-led effort to neutralize the North Korean threat is also driven by Beijing's belief that Washington's North Korea policy is designed to strengthen U.S. regional alliances and military posture to contain China.

China-South Korea relations are evidence of this belief. After years of generally positive bilateral relations buoyed by robust trade and cooperative efforts by the countries' top leaders, the China-South Korea relationship took a negative turn starting in 2016 over the planned deployment of a U.S. Terminal High Altitude Area Defense (THAAD) missile defense system to South Korea. China indicated its displeasure with this development by mounting a massive economic retaliation campaign against South Korea, causing millions of dollars in losses and forcing one South Korean company to cut back on operations in China. Comparing China's harsh rhetorical response to THAAD and its lukewarm response to North Korea's provocations, it appears Beijing finds U.S.-South Korea missile defense cooperation to be a greater threat to Chinese interests than a nuclear-armed North Korea. China has clearly signaled to South Korea that cooperation with the United States will be met with punishment from Beijing. This puts Seoul, which already struggles to balance its relations with Washington and Beijing, in a strategically difficult position, and will necessarily complicate U.S. efforts to enhance cooperation with South Korea going forward.

China-Japan relations continue to be strained as well, with the East China Sea dispute remaining the central flashpoint. Although tensions there have declined since their peak in 2012–2013, the dispute continued to simmer in 2017 with persistent Chinese maritime operations near the Senkaku Islands and sharply increasing Chinese air operations in the East China Sea.

In the near term, Chinese aggression toward Japan and economic coercion against South Korea seem to be driving both countries toward closer security cooperation with the United States. Prospects for enhanced South Korea-Japan security cooperation are less certain, however, and longstanding tensions between the two countries complicate U.S. efforts to evolve Northeast Asia's security architecture from a "hub and spokes" model to a more integrated trilateral cooperative structure.

### ***Key Findings***

- China's and the United States' divergent approaches to North Korea reflect their fundamentally different priorities in Northeast Asia. The United States has made denuclearization its priority in its North Korea policy, whereas China appears willing to accept a nuclear North Korea rather than upset the status quo. Efforts by Washington to compromise in other areas of

the U.S.-China relationship in the hopes of winning Beijing's support in pressuring North Korea risk disappointing results.

- Chinese actors appear to have complied with some provisions of UN sanctions against North Korea and violated others. Despite restrictions on the trade in coal and other goods, China-North Korea trade is robust, with Chinese exports to North Korea increasing significantly in 2017.
- China's objections to the deployment of a U.S. Terminal High Altitude Area Defense (THAAD) missile defense battery in South Korea most likely reflect a deep-seated desire to counter perceived encirclement by the United States by limiting the expansion of the U.S.-allied missile defense system in the region, rather than substantive objections to the practical effect of THAAD's presence in South Korea on China's security environment.
- China's efforts to punish South Korea for hosting THAAD marked a turning point in South Korean attitudes toward China, which until 2016 had been fairly positive. This trend likely will lead to warming U.S.-South Korea defense relations. At the same time, however, Seoul will continue to seek positive relations with Beijing, in part because South Korea is economically dependent on China and relies on China's support to manage the North Korean situation.
- China's continued regional assertiveness and military modernization is contributing to deteriorating Japan-China relations. Japan is likely to continue pursuing military capabilities that would enable it to counter China's expanding military might, as well as North Korea's growing nuclear and missile arsenal.
- Despite North Korea's advancing nuclear and missile programs and China's growing military capabilities, South Korea and Japan have not substantially increased their bilateral defense cooperation and have taken only small steps toward greater trilateral cooperation with the United States. Poor South Korea-Japan relations could hinder the United States' ability to harness its alliances with each country to pursue U.S. interests in the region.
- Most Korean Peninsula conflict or crisis scenarios would require large-scale evacuations of U.S. and other citizens from South Korea. Planning and coordination for noncombatant evacuation operations remain a challenge for the United States, South Korea, and Japan.

### **Section 3: China and Taiwan**

Cross-Strait relations entered a period of increased tension after President Tsai Ing-wen was elected in January 2016, as Beijing steadily increased pressure on Taiwan. Despite President Tsai's cross-Strait policy of "maintaining the status quo," Beijing has been displeased with her unwillingness to endorse the "one China" framework for cross-Strait relations (a 1992 framework Taipei and Beijing endorsed during the previous administration in Taiwan that acknowledges there is "one China," but that allows each side to

maintain its own interpretation of the meaning of “one China”). The measures Beijing is employing to pressure Taiwan include suspending official and semiofficial cross-Strait communication and meetings; establishing diplomatic relations with three of Taiwan’s former diplomatic partners (The Gambia, Sao Tome and Principe, and Panama); reducing the number of Chinese group tours to Taiwan and Chinese students who can attend Taiwan universities; refusing to facilitate repatriation to Taiwan of citizens accused of telecommunications fraud in countries with which Taiwan does not have diplomatic relations; and blocking Taiwan’s participation in certain international fora, such as the International Civil Aviation Organization and the UN World Health Assembly. A complicating factor in cross-Strait relations is Taiwan’s dependence on China-bound exports. China remains Taiwan’s largest trading partner, biggest export market, and top source of imports, giving Beijing significant economic leverage over Taipei. President Tsai has sought to reduce Taiwan’s reliance on China by diversifying Taiwan’s economic ties. Central to this effort is President Tsai’s New Southbound Policy, which seeks to strengthen trade, investment, people-to-people, and other links with countries in Southeast Asia, South Asia, and Oceania. The policy already has led to increased tourism to Taiwan, with the number of visitors from New Southbound Policy target countries increasing 28.6 percent in the first six months after the policy was enacted.

China’s military modernization program remains focused on deterring Taiwan from moving toward formal independence and preparing the Chinese military for a cross-Strait conflict. Faced with a growing threat from China’s military modernization, Taiwan has sought to enhance its own military capabilities in part by indigenously developing combat ships, aircraft, and weapons systems. Advanced antiship cruise missiles, air defense missiles, and fast attack and stealthy catamaran-style patrol ships are among the newest platforms and weapons systems Taiwan has produced. In 2017, Taiwan launched programs to build submarines and advanced jet trainers. Taiwan also seeks to enhance its military capabilities through the procurement of military equipment from the United States. In June 2017, the U.S. Department of State announced its approval of seven foreign military sales and one direct commercial sale to Taiwan valued at \$1.4 billion, including AGM–154C joint stand-off weapon air-to-ground missiles and AGM–88B high-speed antiradiation missiles, among other items.

President Tsai has emphasized enhancing Taiwan’s economic relations with the United States as a top priority for her administration. Although there remain obstacles for U.S.-Taiwan trade (particularly the decade-long dispute over Taiwan’s ban on U.S. pork products), both Washington and Taipei remain committed to furthering their economic relationship. Beyond commercial and security ties, U.S.-Taiwan cooperation spans many other areas, including environmental protection, cybersecurity, education, public health, and science and technology. Taiwan’s robust democracy, civil society, and technology sector, and its vast expertise and experience in areas such as humanitarian assistance and disaster relief, make it a strong partner for the United States.



***Key Findings***

- Taiwan President Tsai Ing-wen has pursued a cross-Strait policy of “maintaining the status quo,” demonstrating goodwill toward Beijing, and reassuring her counterparts across the Taiwan Strait. However, Beijing insists she endorse the “1992 Consensus” and continues to increase its pressure on Taipei in response to her refusal to do so. At the same time, Beijing is bypassing the government of Taiwan in its pursuit of “deepening economic and social integrated development” across the Taiwan Strait. It is doing so through efforts to enhance its economic leverage over Taiwan and increase the number of young people from Taiwan traveling, studying, and working in China.
- China remains Taiwan’s largest trading partner and largest source of foreign direct investment. Taiwan’s continued economic reliance on China makes it vulnerable to political pressure from Beijing and susceptible to fluctuations in China’s economy. To help reduce this dependence, President Tsai is pursuing an agenda, referred to as the New Southbound Policy, to diversify Taiwan’s economic ties, particularly with Southeast Asia, Australia, India, New Zealand, and other South Asian countries.
- The threat to Taiwan posed by Chinese military modernization continues to grow as the cross-Strait military balance has shifted toward China. Taiwan is engaged in a robust program to enhance its defensive capabilities through its domestic defense industrial production, the procurement of U.S. weapons systems, and its transition to an all-volunteer force. However, these efforts face a major challenge from the scope and speed of the modernization of the People’s Liberation Army.
- In an attempt to delegitimize Taiwan on the global stage, Beijing’s pressure on Taipei over its participation in the international community has become more pronounced over the past year. Since December 2016, two countries have severed diplomatic relations with Taiwan and established official ties with China, and Beijing has blocked Taiwan’s participation in multiple international fora in which it has participated in recent years. Beijing has also pressured countries to downgrade unofficial ties with Taipei.
- Beijing seeks to undermine Taiwan’s democracy through collaboration with various individuals and groups in Taiwan and spreading disinformation through social media and other online tools. In July, Taiwan media reported, based on Taiwan government information, that “Chinese influence” was involved in protests and the spread of disinformation against the Tsai Administration.
- Despite uncertainties conferred by a change in administration in the United States, the trend in U.S.-Taiwan relations remains positive. President Tsai has made enhancing Taiwan’s economic relations with the United States a top priority for her Administration. Nonetheless, the two sides have not made progress resolving a long-standing dispute over imports of U.S. pork. In U.S.-Taiwan security cooperation, the Trump Administration’s approval of arms sales to Taiwan was a sign of continued support for Taiwan.

#### **Section 4: China and Hong Kong**

In 2017, 20 years after Hong Kong's handover from the United Kingdom to China, Beijing continued to erode the spirit of the "one country, two systems" policy that has guided its relationship with Hong Kong since 1997. (This policy grants Hong Kong and Macau the right to self-govern their economy and political system to a certain extent, excluding foreign affairs and defense.) The Chinese government increased its interference in the territory's political affairs, becoming more pervasive in Hong Kong's government and civil society. Several notable examples include Beijing's use of legal measures to vacate the seats of six democratically-elected legislators for altering their oaths of office before taking office; its reported involvement in the apparent extralegal abduction of a Chinese billionaire from Hong Kong; and its active efforts to ensure Carrie Lam Cheng Yuet-ngor was selected as the territory's new chief executive. Hong Kong's rule of law, widely viewed as central to its unique status and a key distinguishing characteristic from the Mainland, is being challenged on many fronts. Freedom of expression in the territory—as guaranteed by China's handover agreement with the UK and the Basic Law, Hong Kong's mini constitution—also faces mounting challenges; these range from a crackdown on prodemocracy activists to pressure on the media, universities, and others to self-censor and conform to Beijing's views.

As it has done in other aspects of Hong Kong's politics and society, Beijing has become more active in asserting its presence in Hong Kong's economy. For example, in 2017, Hong Kong-listed Chinese state-owned enterprises were ordered to include a formal role for the CCP in their articles of association, raising concerns among investors who feel the Chinese government is interfering in business operations. Integration of the mainland and Hong Kong economies continues to deepen, with the launch of the Shenzhen-Hong Kong Stock Connect and the China-Hong Kong Bond Connect serving as the latest in a series of measures aimed at attracting global investors to China's domestic markets. Hong Kong's strong rule of law and economic openness have long made it an important destination for international trade and investment. However, some observers are beginning to question Hong Kong's ability to maintain its status as Asia's premier financial center if companies and individuals lose confidence in the territory's rule of law, political autonomy, and other freedoms as they are eroded by Beijing.

Mainland China's increasing encroachment on Hong Kong's promised "high degree of autonomy" poses obstacles for the United States in carrying out its policy objectives in the territory. Hong Kong is a major destination and partner for U.S. trade and investment and plays a valuable role as a participant in important international economic organizations. In light of China's recent intrusions into Hong Kong's democratic institutions, some observers argue the territory is losing its unique characteristics that make it a close U.S. partner in the Asia Pacific. U.S. allies and partners in the region, particularly Taiwan, also are closely watching these developments with unease. The Mainland's adherence to its commitments regarding Hong Kong is necessary to ensure continued strong ties between the United States and the territory.

***Key Findings***

- Beijing's increasing pressure on Hong Kong has called into question the "one country, two systems" framework. Mainland China's interpretation of the Basic Law (Hong Kong's mini constitution) on Hong Kong lawmakers' oaths of office—while a legal case on the matter was ongoing—has raised widespread concerns about the level of autonomy in Hong Kong's judiciary. It has also caused apprehension in Hong Kong about the implications for political life and freedom of speech in the territory. Six prodemocracy legislators-elect were barred from office following the decision and two additional lawmakers face criminal charges, which could result in their seats being vacated in Hong Kong's legislature. This poses a significant threat to the representation of prodemocracy voices in the legislature.
- Mainland China continues to either disregard or ignore Hong Kong's rule of law and its related commitments to the international community. In addition to the disappearance of five Hong Kong book sellers in late 2015 (a case that remains unresolved as this Report went to print), mainland agents in January 2017 apparently abducted a Chinese-born billionaire with Canadian citizenship and close ties to senior Chinese government officials, taking him from a hotel in Hong Kong. These incidents have raised concerns about Hong Kong's legal protections.
- The 2017 chief executive election, which used the existing voting system by an election committee comprising mostly pro-Beijing electors, resulted in the Mainland's preferred candidate Carrie Lam taking the most votes. Having served as the second-most senior official under the previous administration, which was deeply unpopular, and being seen as loyal to Beijing, Chief Executive Lam is unlikely to advance prodemocracy advocates' goal of universal suffrage in chief executive elections.
- Consistent with its downward trajectory in recent years, press freedom in Hong Kong continues to decline, according to journalists in Hong Kong and leading international nongovernmental watchdogs. These observers point to mainland China's rising interference in local Hong Kong media, erosion of media autonomy, and increasing difficulty in covering sensitive stories.
- As Beijing's fears regarding Hong Kong's political dynamics appear to be rising with the increase in prodemocracy advocates pushing for greater autonomy from mainland China, pressure on prodemocracy activists is on the upswing. In the lead up to Chief Executive Lam's formal inauguration on July 1, 2017, Hong Kong authorities arrested numerous prodemocracy legislators and activists. This was followed by the August 2017 jailing of Joshua Wong and two other student leaders from the 2014 Occupy protests—escalating a wide-scale crackdown that has further eroded freedom of expression in Hong Kong.
- Concerns persist among prodemocracy advocates in Hong Kong and among international observers that the territory is sliding away from "one country, two systems" and moving ever closer to

the Mainland. In the process, they argue, Hong Kong is losing the unique characteristics and legal protections that make the territory a key U.S. partner in the Asia Pacific. As Beijing moves to tighten its control over Hong Kong, the territory also faces economic pressure from mainland China.

- Hong Kong continues on the path of greater economic integration with the Mainland. Initiatives like the Shenzhen-Hong Kong Stock Connect and the China-Hong Kong Bond Connect allow Beijing to deepen economic integration with the world, attract foreign investment, and enhance the international use of the renminbi. At the same time, signs are emerging that Hong Kong's importance as a gateway to China may be reduced in the future as China's own markets gain sufficient international standing.

### **Section 5: China's Domestic Information Controls, Global Media Influence, and Cyber Diplomacy**

In 2017, the CCP tightened its control over media and online content. Authorities shut down independent media, penalized companies for disseminating news content without authorization, and eroded the privacy of Internet users in China by forcing them to connect their online profiles to their real names. As a result of a crackdown on "unauthorized" virtual private networks (VPNs), many popular VPN apps have been removed from online stores, and some VPN distributors based in China have been prosecuted and harassed by the state. VPNs have historically been one of the only reliable methods of circumventing China's censorship of the Internet; this censorship functions as a "tax" by forcing users to spend more time and money to access blocked content. The Chinese government's nascent "social credit" program, which relies on accumulated user data to build comprehensive profiles of Chinese citizens, is set to usher in a period of pervasive personal surveillance and social engineering. Multinational corporations with operations in China also have become unsettled by the tightening information controls, which many said negatively impact their business.

Amid the crackdown on independent media, and as journalists increasingly fear the repercussions of pursuing sensitive stories, investigative reporting in China has gradually diminished. Foreign journalists and their local assistants in China now face more restrictions and harassment than at any other time in recent history. The Chinese government also delays or denies visas from foreign journalists; in at least one case in 2016, Chinese authorities held up a visa for a foreign journalist until they were satisfied that another recent hire by the same press agency would not be covering human rights. Foreign correspondents also are increasingly being summoned by local authorities for informal interrogations.

Meanwhile, Beijing has rapidly expanded its overseas media influence by growing its overseas press corps and by exerting pressure on foreign publications both indirectly and directly. In April, the Chinese government also launched a major international media campaign to discredit a Chinese whistleblower living in the United States. In August, the Turkish foreign minister vowed to eliminate anti-China media reports in that country. Chinese authorities also

(ultimately unsuccessfully) pressured Cambridge University Press to censor several of its academic publications. At the same time, China's influence over Hollywood and the U.S. entertainment industry has grown.

The Chinese government has been promoting its views of "Internet sovereignty," including in international fora, to legitimize its monitoring and control the Internet in China. This concept entails that a government has the right to monitor and control the networks in its territory and the content that Internet users there access and transmit. Beijing also advocates for a "multilateral" system of Internet governance in which national governments are the main actors. These views sharply contrast with longstanding U.S. support for the "multistakeholder" model, in which governmental, industry, academic, and other nonstate organizations have an equal role in the management of the Internet.

### ***Key Findings***

- China's current information controls, including the government's new social credit initiative, represent a significant escalation in censorship, surveillance, and invasion of privacy by the authorities.
- The Chinese state's repression of journalists has expanded to target foreign reporters and their local Chinese staff. It is now much more difficult for all journalists to investigate politically sensitive stories.
- The investment activities of large, Chinese Communist Party-linked corporations in the U.S. media industry risk undermining the independence of film studios by forcing them to consider self-censorship in order to gain access to the Chinese market.
- China's overseas influence operations to pressure foreign media have become much more assertive. In some cases, even without direct pressure by Chinese entities, Western media companies now self-censor out of deference to Chinese sensitivity.
- Beijing is promoting its concept of "Internet sovereignty" to justify restrictions on freedom of expression in China. These policies act as trade barriers to U.S. companies through both censorship and restrictions on cross-border data transfers, and they are fundamental points of disagreement between Washington and Beijing.
- In its participation in international negotiations on global Internet governance, norms in cyberspace, and cybersecurity, Beijing seeks to ensure continued control of networks and information in China and to reduce the risk of actions by other countries that are not in its interest. Fearing that international law will be used by other countries against China, Beijing is unwilling to agree on specific applications of international law to cyberspace.



## **Chapter 4: China's High Tech Development**

### **Section 1: China's Pursuit of Dominance in Computing, Robotics, and Biotechnology**

The Chinese government is implementing a comprehensive, long-term industrial strategy to ensure its global dominance in computing, robotics, artificial intelligence (AI), nanotechnology, and biotechnology. This strategy is laid out in the 13th Five-Year Plan, and the Made in China 2025 and Internet Plus initiatives and continues China's state-directed approach over the last six decades to build internationally competitive domestic firms. Beijing's ultimate goal is for domestic companies to replace foreign companies as designers and manufacturers of key technology and products first at home, then abroad. It utilizes state funding, regulations, China-specific standards, localization targets, government procurement, foreign investment restrictions, recruitment of foreign talent, close integration of civilian and military technology development, and, in some cases, industrial espionage.

China is also leveraging the openness of the United States and other market-based economies to gain access to advanced research and data, recruit a globally talented workforce, acquire and invest in leading edge firms, and freely sell their products and services abroad. The scale and volume of government resources directed toward these sectors undermines the ability of foreign firms to fairly compete in China's market and creates distorted global and domestic market conditions and rampant overproduction and overcapacity. In addition, China's high market access barriers for foreign firms, localization targets, and China-specific standards further restrict foreign competition's access to China's rapidly growing market, a major loss of market and job opportunities.

The United States remains a global technological and innovation leader in many cutting-edge, dual-use technologies due to its world-renowned universities, innovation ecosystem, federal funding of basic research and development (R&D), and recruitment of the world's brightest minds. But falling and inconsistent federal R&D spending, reduced openness to global talent, and lack of interagency coordination are undermining these drivers of U.S. innovation to China's advantage. Loss of global leadership in these key high-value-added, dual-use sectors is detrimental to U.S. long-term economic growth, weakening U.S. firms' competitive edge, and reducing the capabilities, capacity, and resilience of the U.S. defense industrial base.

#### ***Key Findings***

- China has laid out an ambitious whole-of-government plan to achieve dominance in advanced technology. This state-led approach utilizes government financing and regulations, high market access and investment barriers for foreign firms, overseas acquisitions and talent recruitment, and, in some cases, industrial espionage to create globally competitive firms.
- China's close integration of civilian and military technology development raises concerns that technology, expertise, and intellectual property shared by U.S. firms with Chinese commercial partners could be transferred to China's military.

- *Artificial intelligence:* China—led by Baidu—is now on par with the United States in artificial intelligence due in part to robust Chinese government support, establishment of research institutes in the United States, recruitment of U.S.-based talent, investment in U.S. artificial intelligence-related startups and firms, and commercial and academic partnerships.
- *Quantum information science:* China has closed the technological gap with the United States in quantum information science—a sector the United States has long dominated—due to a concerted strategy by the Chinese government and inconsistent and unstable levels of R&D funding and limited government coordination by the United States.
- *High performance computing:* Through multilevel government support, China now has the world’s two fastest supercomputers and is on track to surpass the United States in the next generation of supercomputers—exascale computers—with an expected rollout by 2020 compared to the accelerated U.S. timeline of 2021.
- *Biotechnology:* The United States’ robust biotechnology ecosystem continues to drive U.S. leadership in this sector, but China’s state-directed policies have subsidized the establishment of the world’s largest genomic sequencing firms and supported China’s rapid rise in genomics and biotechnology-related publications.
- *Robotics:* China is developing its industrial and military robotics sector through subsidization of domestic robotics firms, acquisition of foreign knowledge and technology, and recruitment of overseas expertise. This is strengthening the quality and competitiveness of China’s manufacturing and its military capabilities.
- *Nanotechnology:* While consistent federal government funding to the National Nanotechnology Initiative has kept the United States at the forefront of nanotechnology, China has become the fastest-growing country for nanotechnology publications and industrialization due to massive government funding, recruitment of overseas talent, and creation of nanotechnology science parks.
- *Cloud computing:* China has largely closed off its cloud computing market to U.S. cloud computing firms—the global leaders—with unfair market access restrictions and onerous regulations. In addition, Chinese cloud computing firms’ close ties to the Chinese government raise security concerns over the protection of U.S. customers’ sensitive data, including intellectual property and personal information.

## **Section 2: China’s Pursuit of Advanced Weapons**

China is pursuing a wide range of military technologies at the global frontier—weapons just now being developed or not yet developed by any country. Advanced systems such as maneuverable reentry vehicles, hypersonic weapons, directed energy weapons, electromagnetic railguns, counterspace weapons, and unmanned and AI-equipped weapons contribute to China’s longstanding goal of military modernization and its efforts to compete militarily with

the United States. They also go hand in hand with Beijing's desire for the country to become a leading high technology power across commercial and dual-use areas. China's government has taken a comprehensive approach to the development of key dual-use technologies, leveraging state funding, licit and illicit technological exchange, foreign investment, and talent recruitment opportunities to build national champions and advance its military capabilities.

Although information regarding China's advanced weapons programs is not always publicly available, numerous open source writings, government statements, and testing and deployment activities indicate Beijing has undertaken vigorous efforts in these areas. China revealed two antiship ballistic missile systems with reported **maneuverable reentry vehicle** capabilities in 2010 and 2015, respectively, and has taken steps toward developing the reconnaissance-strike complex necessary to successfully strike a moving target at sea, still unproven. China's **hypersonic weapons** program appears to be in developmental stages but progressing rapidly, featuring seven likely hypersonic glide vehicle tests since 2014 and a reported scramjet engine flight test in 2015. Following a deep history of research into **directed energy weapons**, China's progress includes reported advancements in developing a high-power microwave antimissile system in 2017, at least one chemical high energy laser designed to damage or blind imaging satellites as of 2006 (with likely further developments), and recent marketing of low-power solid state laser weapons. China has reportedly built experimental **electromagnetic rail-guns**, and numerous research institutes in China are studying aspects of electromagnetic launch technology. China's technology tests applicable to **counterspace weapons** include direct-ascent antisatellite missiles, ground-based directed energy weapons, and rendezvous and proximity operations; and its writings and capabilities indicate the potential for directed energy weapons based on co-orbital platforms. Finally, in addition to developing and marketing a wide range of **unmanned systems**, China has conducted research into autonomous systems such as AI-equipped cruise missiles, autonomous vehicles, and drone swarms, alongside its rapid rise in the global commercial AI sector.

While the United States appears to retain a lead in developing most of these systems according to public reports, China likely possesses the key factors (scientific knowledge, critical components, and skills and techniques) necessary to successfully develop advanced weapons. China is able to access scientific knowledge through publicly available information, academic exchanges, and strong efforts to cultivate human talent. Its advances in computing and robotics provide critical components for next frontier weapons: semiconductors are key to intelligent weapons systems; supercomputing is crucial for weapons design and testing; industrial robotics enhances the quality and efficiency of manufacturing; and national champions in the commercial robotics and AI sectors are well positioned to provide next frontier military applications. Finally, while China currently trails the United States in developing relevant skills and techniques, the only fundamental barriers to achieving these will be effort: time, will, and financial support. China appears to have

the long-term plans, consistent funding, and human talent in place to eventually overcome these barriers. China may in fact be moving toward a phase of higher-end innovation, given cutting-edge advances in emerging technologies such as artificial intelligence, high-performance computing, and quantum information science. Should the United States falter in its own efforts, China is well prepared to close the gap further than it already has.

China's advanced weapons programs present both direct implications for U.S. security interests and broader implications for long-term U.S.-China defense technological competition. Breakthroughs in any of the aforementioned advanced weapons categories would contribute to China's antiaccess/area denial capabilities and directly challenge U.S. advantages. Notable examples include the potential for antiship ballistic missiles to hold U.S. surface ships at risk; for hypersonic weapons to defeat kinetic missile defenses, if capable of sufficient speed and maneuverability; for directed energy weapons and railguns to undermine future U.S. military concepts such as using distributed low-cost platforms to assure access to contested environments; for counterspace weapons to deny key space-based systems to the U.S. military in a contingency; and for unmanned and AI-equipped weapons in large numbers to saturate U.S. air defenses, particularly by using swarm technology. China is poised to challenge U.S. technological leadership in an environment in which dual-use commercial technology increasingly contributes to military technological strength. As the United States seeks to ensure it is prepared to deter aggression and defend key interests in the Asia Pacific, such as the security of allies and partners, the peaceful resolution of disputes, and freedom of navigation, recognizing these critical challenges will be crucial.

### ***Key Findings***

- China is pursuing a range of advanced weapons with disruptive military potential. Six types that China's leaders have prioritized are maneuverable reentry vehicles, hypersonic weapons, directed energy weapons, electromagnetic railguns, counterspace weapons, and unmanned and artificial intelligence-equipped weapons.
- China's advanced weapons programs align with the People's Liberation Army's overall modernization drive over the past several decades, but appear to reflect a more careful degree of planning as to the U.S. weaknesses they are designed to exploit.
- Current technological trends increase the difficulty of preserving an advantage in developing advanced weapons. The United States for the first time faces a peer technological competitor—a country that is also one of its largest trading partners and that trades extensively with other high-tech powers—in an era in which private sector research and development with dual-use implications increasingly outpaces and contributes to military developments.
- The requirements for developing advanced weapons are fundamental scientific knowledge, unique materials, and abstract skill-based enablers (i.e., abilities, tools, and techniques). China

has clear policies to exploit government funding, commercial technological exchange, foreign investment and acquisitions, and talent recruitment to bolster its dual-use technological advances. For China, the only ultimate barrier to such advances is likely to be effort—time, will, and money—and it will be difficult for the United States and its allies and partners to deter this.

- While China has only achieved incremental innovation in military technologies in the past, its research efforts at the technological frontier indicate it may be moving from a phase of “catching-up” to pursuing “leap-ahead” technologies. China’s limited returns on science and technology investments indicate shortcomings that may render its development of innovative advanced weapons more costly or protracted, but do not rule out successful innovation.
- China’s achievement of a surprise breakthrough in one of these technologies is possible, due to the secrecy surrounding these programs and the uncertain nature of advanced weapons development in general. Such a breakthrough could have significant strategic implications for the United States, particularly in its potential to further existing access challenges and hold forward deployed U.S. forces at risk.
- Given Beijing’s commitment to its current trajectory, and the lack of fundamental barriers to advanced weapons development apart from time and funding, the United States cannot assume it will have an enduring advantage in developing weapons at the technological frontier.



### THE COMMISSION'S KEY RECOMMENDATIONS

The Commission considers 10 of its 26 recommendations to Congress to be of particular significance. The complete list of recommendations appears at the Report's conclusion on page 597.

The Commission recommends:

- Congress consider legislation updating the Committee on Foreign Investment in the United States (CFIUS) statute to address current and evolving security risks. Among the issues Congress should consider are:
  - Prohibiting the acquisition of U.S. assets by Chinese state-owned or state-controlled entities, including sovereign wealth funds.
  - Requiring a mandatory review of any transaction involving the acquisition of a controlling interest in U.S. assets by Chinese entities not falling under the above class of acquiring entities.
  - Requiring reviews of investments in U.S.-based greenfield assets by Chinese-controlled entities to assess any potential harm to U.S. national and economic security.
  - Expanding the definition of “control” to include joint ventures, venture capital funds, licensing agreements, and other arrangements or agreements that enable Chinese entities to access and/or determine the disposition of any asset.
  - Prohibiting any acquisition or investment that would confer “control” with regard to critical technologies or infrastructure. The U.S. Departments of Homeland Security, Commerce, and Defense shall prepare and regularly update a list of critical technologies or infrastructure that would not be eligible for acquisition or investment by any Chinese entities to ensure U.S. economic and national security interests are protected.
  - Including a net economic benefit test to assess the impact of acquisitions by Chinese entities in the United States to ensure they advance U.S. national economic interests.
  - Requiring that any proposed acquisition of a media property by a Chinese entity be assessed in terms of the acquiring entity's history of adhering to Chinese Communist Party propaganda objectives and its potential to influence public opinion in the United States.
  - Authorizing an independent review panel, appointed by Congress, to review the actions and activities of CFIUS on a continuing basis.
  - Allowing any CFIUS member agency to bring a transaction up for review and investigation.
- Congress amend the Foreign Sovereign Immunities Act (FSIA) of 1976 to:
  - Allow U.S. courts to hear cases against a foreign state's corporate affiliates under the commercial activity exception.
  - Require Chinese firms to waive any potential claim of sovereign immunity if they do business in the United States.

- Congress strengthen the Foreign Agents Registration Act to require the registration of all staff of Chinese state-run media entities, given that Chinese intelligence gathering and information warfare efforts are known to involve staff of Chinese state-run media organizations and in light of the present uneven enforcement of the Act.
- Congress urge the Administration to invite Taiwan to participate, at least as an observer, in U.S.-led bilateral and multilateral military and security-related exercises, including the Rim of the Pacific (RIMPAC) maritime exercise, Red Flag air-to-air combat training exercises, and Cyber Storm cybersecurity exercise, in order to support Taiwan's efforts to enhance its defense capabilities, expand opportunities for Taiwan to contribute to regional and international security, and counter China's efforts to limit Taiwan's international space.
- Congress consider legislation to ban and delist companies seeking to list on U.S. stock exchanges that are based in countries that have not signed a reciprocity agreement with the Public Company Accounting Oversight Board (PCAOB).
- Congress authorize U.S. defense spending at levels sufficient to address the growing challenge to U.S. interests posed by China's ongoing military modernization program and to ensure the United States will have the capacity to maintain readiness and presence in the Asia Pacific.
- Congress direct the National Science and Technology Council, in coordination with the National Economic Council and relevant agencies, to identify gaps in U.S. technological development vis-à-vis China, including funding, science, technology, engineering, and mathematics workforce development, interagency coordination, and utilization of existing innovation and manufacturing institutes, and, following this assessment, develop and update biennially a comprehensive strategic plan to enhance U.S. competitiveness in advanced science and technology.
- Congress reauthorize annual reporting requirements of the United States-Hong Kong Policy Act of 1992, in an effort to ensure policymakers have the most up-to-date and authoritative information about developments in Hong Kong. The report should include an assessment of whether Hong Kong has maintained a "sufficient degree of autonomy" under the "one country, two systems" policy, among other developments of interest to the United States.
- Congress direct the Office of the U.S. Trade Representative to develop criteria for the Notorious Markets List to ensure listed companies can be held accountable for engaging in or facilitating copyright piracy and trademark counterfeiting.
- Congress consider legislation conditioning the provision of market access to Chinese investors in the United States on a reciprocal, sector-by-sector basis to provide a level playing field for U.S. investors in China.

velopment is “an important historic opportunity to safeguard social stability and lasting political order.”<sup>84</sup> Following the blueprint of previous domestic initiatives to promote domestic stability with economic development, Beijing believes trade and investment with its Central and South Asian neighbors will reduce poverty, thereby encouraging peace and stability and making the region more resistant to fundamentalism and terrorism.<sup>85</sup> By fostering economic linkages between Central Asian and South Asian countries and Xinjiang,\* Beijing hopes to encourage economic development and stability domestically as well.

Chinese policymakers hope the opening of new markets for Chinese products will rejuvenate China’s infrastructure- and export-led development model. As domestic markets become saturated, encouraging companies to compete abroad will generate new returns—especially for inefficient state-owned companies—while enabling the government to postpone painful economic reforms (e.g., privatizing state companies). OBOR’s heavy emphasis on infrastructure creates an outlet for China’s tremendous excess capacity, especially in industries associated with construction, such as steel and glass, which are dominated by state-owned companies.<sup>86</sup>

By promoting Chinese companies, services, and technologies, OBOR also serves as a vehicle for entrenching Chinese standards and practices in host markets. Chinese companies deploying Chinese power grids or Chinese rail gauges across vast parts of Europe and Asia will shape international standards.<sup>87</sup> More pressing, given Chinese government’s emphasis on “technonationalism,”† is the role Chinese information and communication technology companies will play in establishing standards for a new generation of technologies. Already, Chinese telecom companies ZTE and Huawei are among major developers of 5G mobile network standards.<sup>88</sup>

***Gaining influence and leverage over other countries, and countering U.S. influence:*** As Chinese investment becomes more and more important to other countries’ economic health, Beijing’s ability to use that dependence as leverage grows. According to Nadège Rolland, a scholar of OBOR and a senior fellow for political and security affairs at the National Bureau of Asian Research:

*Economic cooperation is not just a way to boost development or to bring financial returns. It is also a tool to be used for political and strategic gain.... When Xi tells China’s neigh-*

\*Xinjiang Uyghur Autonomous Region, China’s westernmost province and home to China’s Muslim Uyghur ethnic group, has experienced varying degrees of unrest in the past several decades. As in Tibet, many residents of Xinjiang do not culturally or politically identify with China, and some Uyghur groups advocate for greater autonomy or full independence for Xinjiang. Beijing views the existence of these groups as a threat to China’s sovereignty and security and has sought to silence them while simultaneously integrating Xinjiang into the social, economic, and political fabric of greater China. U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress*, November 2015, 393.

†Technonationalism refers to the Chinese government’s goal of moving up the high-tech value-added chain and achieving dominance in key technologies by relying on domestic innovation. In pursuit of this goal, the Chinese government has relied on a full range of policy tools, including extensive subsidies to domestic companies, rules and regulations that marginalize foreign companies and demand transfers of technologies in exchange for accessing the Chinese market, financial and regulatory support for acquisition of foreign technologies and, in some cases, theft of intellectual property. The key tenet of Chinese technonationalism is that domestic—not foreign—companies should achieve dominant positions in China, and then start expanding to overseas markets. For a discussion of China’s industrial policy and technological development, see Chapter 4, Section 1, “China’s Pursuit of Dominance in Computing, Robotics, and Biotechnology.”

# EXHIBIT 10

## **Statement for the Record**

# **Worldwide Threat Assessment of the US Intelligence Community**

**Senate Armed Services Committee**



**James R. Clapper**

**Director of National Intelligence**

**February 9, 2016**



**STATEMENT FOR THE RECORD**  
**WORLDWIDE THREAT ASSESSMENT**  
**of the**  
**US INTELLIGENCE COMMUNITY**

February 9, 2016

---

**INTRODUCTION**

---

Chairman McCain, Vice Chairman Reed, Members of the Committee, thank you for the invitation to offer the United States Intelligence Community's 2016 assessment of threats to US national security. My statement reflects the collective insights of the Intelligence Community's extraordinary men and women, whom I am privileged and honored to lead. We in the Intelligence Community are committed every day to provide the nuanced, multidisciplinary intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

The order of the topics presented in this statement does not necessarily indicate the relative importance or magnitude of the threat in the view of the Intelligence Community.

Information available as of February 3, 2016 was used in the preparation of this assessment.

# TABLE OF CONTENTS

	<i>Page</i>
<hr/>	
<b>GLOBAL THREATS</b>	
<hr/>	
<b>Cyber and Technology</b>	1
<b>Terrorism</b>	4
<b>Weapons of Mass Destruction and Proliferation</b>	6
<b>Space and Counterspace</b>	9
<b>Counterintelligence</b>	10
<b>Transnational Organized Crime</b>	11
<b>Economics and Natural Resources</b>	12
<b>Human Security</b>	13
<hr/>	
<b>REGIONAL THREATS</b>	
<hr/>	
<b>East Asia</b>	16
China	16
Southeast Asia	17
North Korea	17
<b>Russia and Eurasia</b>	17
Russia	17
Ukraine, Belarus, and Moldova	19
The Caucasus and Central Asia	19
<b>Europe</b>	20
Key Partners	20
The Balkans	20
Turkey	21
<b>Middle East and North Africa</b>	21
Iraq	21
Syria	22
Libya	23
Yemen	23
Iran	24

---

Lebanon	25
Egypt	25
Tunisia	25
<b>South Asia</b>	26
Afghanistan	26
Bangladesh	27
Pakistan and India	27
<b>Sub-Saharan Africa</b>	27
Central Africa	27
Somalia	28
South Sudan	28
Sudan	28
Nigeria	28
<b>Latin America and Caribbean</b>	28
Central America	28
Cuba	29
Venezuela	29
Brazil	29

---

---

## GLOBAL THREATS

---

### CYBER AND TECHNOLOGY

#### Strategic Outlook

The consequences of innovation and increased reliance on information technology in the next few years on both our society's way of life in general and how we in the Intelligence Community specifically perform our mission will probably be far greater in scope and impact than ever. Devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US Government systems. These developments will pose challenges to our cyber defenses and operational tradecraft but also create new opportunities for our own intelligence collectors.

**Internet of Things (IoT).** “Smart” devices incorporated into the electric grid, vehicles—including autonomous vehicles—and household appliances are improving efficiency, energy conservation, and convenience. However, security industry analysts have demonstrated that many of these new systems can threaten data privacy, data integrity, or continuity of services. In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.

**Artificial Intelligence (AI).** AI ranges from “Narrow AI” systems, which seek to execute specialized tasks, such as speech recognition, to “General AI” systems—perhaps still decades away—which aim to replicate many aspects of human cognition. Implications of broader AI deployment include increased vulnerability to cyberattack, difficulty in ascertaining attribution, facilitation of advances in foreign weapon and intelligence systems, the risk of accidents and related liability issues, and unemployment. Although the United States leads AI research globally, foreign state research in AI is growing.

The increased reliance on AI for autonomous decisionmaking is creating new vulnerabilities to cyberattacks and influence operations. As we have already seen, false data and unanticipated algorithm behaviors have caused significant fluctuations in the stock market because of the reliance on automated trading of financial instruments. Efficiency and performance benefits can be derived from increased reliance on AI systems in both civilian industries and national security, as well as potential gains to cybersecurity from automated computer network defense. However, AI systems are susceptible to a range of disruptive and deceptive tactics that might be difficult to anticipate or quickly understand. Efforts to mislead or compromise automated systems might create or enable further opportunities to disrupt or damage critical infrastructure or national security networks.

**Foreign Data Science.** This field is becoming increasingly mature. Foreign countries are openly purchasing access to published US research through aggregated publication indices, and they are collecting social media and patent data to develop their own indices.

**Augmented Reality (AR) and Virtual Reality (VR).** AR and VR systems with three-dimensional imagery and audio, user-friendly software, and low price points are already on the market; their adoption will probably accelerate in 2016. AR provides users with additional communications scenarios (e.g. by using virtual avatars) as well as acquisition of new data (e.g. from facial recognition) overlaid onto reality. VR gives users experiences in man-made environments wholly separate from reality.

## **Protecting Information Resources**

**Integrity.** Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) to affect decisionmaking, reduce trust in systems, or cause adverse physical effects. Broader adoption of IoT devices and AI—in settings such as public utilities and health care—will only exacerbate these potential effects. Russian cyber actors, who post disinformation on commercial websites, might seek to alter online media as a means to influence public discourse and create confusion. Chinese military doctrine outlines the use of cyber deception operations to conceal intentions, modify stored data, transmit false data, manipulate the flow of information, or influence public sentiments—all to induce errors and miscalculation in decisionmaking.

**Infrastructure.** Countries are becoming increasingly aware of both their own weaknesses and the asymmetric offensive opportunities presented by systemic and persistent vulnerabilities in key infrastructure sectors including health care, energy, finance, telecommunications, transportation, and water. For example, the US health care sector is rapidly evolving in ways never before imagined, and the cross-networking of personal data devices, electronic health records, medical devices, and hospital networks might play unanticipated roles in patient outcomes. Such risks are only heightened by large-scale theft of health care data and the internationalization of critical US supply chains and service infrastructure.

A major US network equipment manufacturer acknowledged last December that someone repeatedly gained access to its network to change source code in order to make its products' default encryption breakable. The intruders also introduced a default password to enable undetected access to some target networks worldwide.

**Interoperability.** Most governments are exploring ways to exert sovereign control over information accessible to and used by their citizens and are placing additional legal requirements on companies as they seek to balance security, privacy, and economic concerns. We assess that many countries will implement new laws and technologies to censor information, decrease online anonymity, and localize data within their national borders. Although these regulations will restrict freedoms online and increase the operating costs for US companies abroad, they will probably not introduce obstacles that threaten the functionality of the Internet.

**Identity.** Advances in the capabilities of many countries to exploit large data sets almost certainly increase the intelligence value of collecting bulk data and have probably contributed to increased targeting of personally identifiable information. Commercial vendors, who aggregate the bulk of digitized information about persons, will increasingly collect, analyze, and sell it to both foreign and domestic customers. We assess that countries are exploiting personal data to inform a variety of counterintelligence operations.

**Accountability.** Information security professionals will continue to make progress in attributing cyber operations and tying events to previously identified infrastructure or tools that might enable rapid attribution in some cases. However, improving offensive tradecraft, the use of proxies, and the creation of cover organizations will hinder timely, high-confidence attribution of responsibility for state-sponsored cyber operations.

**Restraint.** Many actors remain undeterred from conducting reconnaissance, espionage, and even attacks in cyberspace because of the relatively low costs of entry, the perceived payoff, and the lack of significant consequences. Moscow and Beijing, among others, view offensive cyber capabilities as an important geostrategic tool and will almost certainly continue developing them while simultaneously discussing normative frameworks to restrict such use. Diplomatic efforts in the past three years have created the foundation for establishing limits on cyber operations, and the norms articulated in a 2015 report of the UN Group of Governmental Experts suggest that countries are more likely to commit to limitations on what cyber operations can target than to support bans on the development of offensive capabilities or on specific means of cyber intervention. For example, in 2015, following a US-Chinese bilateral agreement, G-20 leaders agreed that no country should conduct or sponsor cyber espionage for the purpose of commercial gain.

### Leading Threat Actors

**Russia.** Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny. Russian cyber operations are likely to target US interests to support several strategic objectives: intelligence gathering to support Russian decisionmaking in the Ukraine and Syrian crises, influence operations to support military and political objectives, and continuing preparation of the cyber environment for future contingencies.

**China.** China continues to have success in cyber espionage against the US Government, our allies, and US companies. Beijing also selectively uses cyberattacks against targets it believes threaten Chinese domestic stability or regime legitimacy. We will monitor compliance with China's September 2015 commitment to refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property with the intent of providing competitive advantage to companies or commercial sectors. Private-sector security experts have identified limited ongoing cyber activity from China but have not verified state sponsorship or the use of exfiltrated data for commercial gain.

**Iran.** Iran used cyber espionage, propaganda, and attacks in 2015 to support its security priorities, influence events, and counter threats—including against US allies in the region.

**North Korea.** North Korea probably remains capable and willing to launch disruptive or destructive cyberattacks to support its political objectives. South Korean officials have concluded that North Korea was probably responsible for the compromise and disclosure of data from a South Korean nuclear plant.

**Nonstate Actors.** Terrorists continue to use the Internet to organize, recruit, spread propaganda, collect intelligence, raise funds, and coordinate operations. In a new tactic, ISIL actors targeted and released sensitive information about US military personnel in 2015 in an effort to spur "lone-wolf" attacks. Criminals develop and use sophisticated cyber tools for a variety of purposes such as theft, extortion, and



facilitation of other criminal activities such as drug trafficking. “Ransomware” designed to block user access to their own data, sometimes by encrypting it, is becoming a particularly effective and popular tool for extortion for which few options for recovery are available. Criminal tools and malware are increasingly being discovered on state and local government networks.

## TERRORISM

The United States and its allies are facing a challenging threat environment in 2016. Sunni violent extremism has been on an upward trajectory since the late 1970s and has more groups, members, and safe havens than at any other point in history. At the same time, Shia violent extremists will probably deepen sectarian tensions in response to real and perceived threats from Sunni violent extremists and to advance Iranian influence.

The Islamic State of Iraq and the Levant (ISIL) has become the preeminent terrorist threat because of its self-described caliphate in Syria and Iraq, its branches and emerging branches in other countries, and its increasing ability to direct and inspire attacks against a wide range of targets around the world. ISIL’s narrative supports jihadist recruiting, attracts others to travel to Iraq and Syria, draws individuals and groups to declare allegiance to ISIL, and justifies attacks across the globe. The ISIL-directed November 2015 attacks in Paris and ISIL-Sinai’s claim of responsibility for the late October downing of a Russian airliner in the Sinai underscore these dynamics.

Al-Qa’ida’s affiliates have proven resilient and are positioned to make gains in 2016, despite counterterrorism pressure that has largely degraded the network’s leadership in Afghanistan and Pakistan. They will continue to pose a threat to local, regional, and even possibly global interests as demonstrated by the January 2015 attack on French satirical newspaper *Charlie Hebdo* by individuals linked to al-Qa’ida in the Arabian Peninsula (AQAP). Other Sunni terrorist groups retain the ability to attract recruits and resources.

The United States will almost certainly remain at least a rhetorically important enemy for most violent extremists in part due to past and ongoing US military, political, and economic engagement overseas. Sunni violent extremists will probably continually plot against US interests overseas. A smaller number will attempt to overcome the logistical challenges associated with conducting attacks on the US homeland. The July 2015 attack against military facilities in Chattanooga and December 2015 attack in San Bernardino demonstrate the threat that homegrown violent extremists (HVEs) also pose to the homeland. In 2014, the FBI arrested approximately one dozen US-based ISIL supporters. In 2015, that number increased to approximately five dozen arrests. These individuals were arrested for a variety of reasons, predominantly for attempting to provide material support to ISIL.

US-based HVEs will probably continue to pose the most significant Sunni terrorist threat to the US homeland in 2016. The perceived success of attacks by HVEs in Europe and North America, such as those in Chattanooga and San Bernardino, might motivate others to replicate opportunistic attacks with little or no warning, diminishing our ability to detect terrorist operational planning and readiness. ISIL involvement in homeland attack activity will probably continue to involve those who draw inspiration from

the group's highly sophisticated media without direct guidance from ISIL leadership and individuals in the United States or abroad who receive direct guidance and specific direction from ISIL members or leaders.

ISIL's global appeal continues to inspire individuals in countries outside Iraq and Syria to travel to join the group. More than 36,500 foreign fighters—including at least 6,600 from Western countries—have traveled to Syria from more than 100 countries since the conflict began in 2012. Foreign fighters who have trained in Iraq and Syria might potentially leverage skills and experience to plan and execute attacks in the West. Involvement of returned foreign fighters in terrorist plotting increases the effectiveness and lethality of terrorist attacks, according to academic studies. A prominent example is the November 2015 attacks in Paris in which the plotters included European foreign fighters returning from Syria.

ISIL's branches continue to build a strong global network that aims to advance the group's goals and often works to exacerbate existing sectarian tensions in their localities. Some of these branches will also plan to strike at Western targets, such as the downing of a Russian airliner in October by ISIL's self-proclaimed province in Egypt. In Libya, the group is entrenched in Surt and along the coastal areas, has varying degrees of presence across the country, and is well positioned to expand territory under its control in 2016. ISIL will seek to influence previously established groups, such as Boko Haram in Nigeria, to emphasize the group's ISIL identity and fulfill its religious obligations to the ISIL "caliphate."

Other terrorists and insurgent groups will continue to exploit weak governance, insecurity, and economic and political fragility in an effort to expand their areas of influence and provide safe havens for violent extremists, particularly in conflict zones. Sunni violent extremist groups are increasingly joining or initiating insurgencies to advance their local and transnational objectives. Many of these groups are increasingly capable of conducting effective insurgent campaigns, given their membership growth and accumulation of large financial and materiel caches. This trend increasingly blurs the lines between insurgent and terrorist groups as both aid local fighters, leverage safe havens, and pursue attacks against US and other Western interests.

No single paradigm explains how terrorists become involved in insurgencies. Some groups like ISIL in Syria and al-Qa'ida in the Islamic Maghreb (AQIM) in Mali have worked with local militants to incite insurgencies. Others, like Boko Haram, are the sole instigators and represent the primary threat to their respective homeland's security. Still others, including al-Shabaab, are the primary beneficiaries of an insurgency started by others. Finally, other groups, such as core al-Qa'ida, have taken advantage of the relative safe haven in areas controlled by insurgent groups to build capabilities and alliances without taking on a primary leadership role in the local conflict.

Although al-Qa'ida's presence in Afghanistan and Pakistan has been significantly degraded, it aspires to attack the US and its allies. In Yemen, the proven capability of AQAP to advance external plots during periods of instability suggests that leadership losses and challenges from the Iranian-backed Huthi insurgency will not deter its efforts to strike the West. Amid this conflict, AQAP has made territorial gains in Yemen including the seizure of military bases in the country's largest province. Al-Qa'ida nodes in Syria, Pakistan, Afghanistan, and Turkey are also dedicating resources to planning attacks. Al-Shabaab, al-Qaida's affiliate in East Africa, continues its violent insurgency in southern and central Somalia despite losses of territory and influence and conflict among senior leaders.

Iran—the foremost state sponsor of terrorism—continues to exert its influence in regional crises in the Middle East through the Islamic Revolutionary Guard Corps—Qods Force (IRGC-QF), its terrorist partner Lebanese Hizballah, and proxy groups. It also provides military and economic aid to its allies in the region. Iran and Hizballah remain a continuing terrorist threat to US interests and partners worldwide.

Terrorists will almost certainly continue to benefit in 2016 from a new generation of recruits proficient in information technology, social media, and online research. Some terrorists will look to use these technologies to increase the speed of their communications, the availability of their propaganda, and ability to collaborate with new partners. They will easily take advantage of widely available, free encryption technology, mobile-messaging applications, the dark web, and virtual environments to pursue their objectives.

Long-term economic, political, and social problems, as well as technological changes, will contribute to the terrorist threat worldwide. A record-setting 60 million internally displaced persons (IDPs) and refugees as of 2014—one half of whom are children, according to the United Nations—will stress the capacity of host nations already dealing with problems relating to assimilation and possibly make displaced populations targets for recruitment by violent extremists. Among Sunni violent extremist groups, ISIL is probably most proficient at harnessing social media to disseminate propaganda and solicit recruits among a broad audience. It is likely to continue these activities in 2016 by using videos, photos, and other propaganda glorifying life under ISIL rule and promoting the group's military successes. In addition, violent extremist supporters will probably continue to publicize their use of encrypted messaging applications on social media to let aspiring violent extremists know that secure avenues are available by which they can communicate.

The acute and enduring nature of demographic, economic, political, social, and technological factors contribute to the motivation of individuals and groups and their participation in violent extremist activities. These factors ensure that terrorism will remain one of several primary national security challenges for the United States in 2016.

## **WEAPONS OF MASS DESTRUCTION AND PROLIFERATION**

Nation-state efforts to develop or acquire weapons of mass destruction (WMD), their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and allies. Use of chemical weapons in Syria by both state and nonstate actors demonstrates that the threat of WMD is real. Biological and chemical materials and technologies, almost always dual use, move easily in the globalized economy, as do personnel with the scientific expertise to design and use them. The latest discoveries in the life sciences also diffuse rapidly around the globe.

### **North Korea Developing WMD-Applicable Capabilities**

North Korea's nuclear weapons and missile programs will continue to pose a serious threat to US interests and to the security environment in East Asia in 2016. North Korea's export of ballistic missiles and associated materials to several countries, including Iran and Syria, and its assistance to Syria's

construction of a nuclear reactor, destroyed in 2007, illustrate its willingness to proliferate dangerous technologies.

We judge that North Korea conducted a nuclear test on 6 January 2016 that it claimed was a successful test of a “hydrogen bomb.” Although we are continuing to evaluate this event, the low yield of the test is not consistent with a successful test of a thermonuclear device. In 2013, following North Korea’s third nuclear test, Pyongyang announced its intention to “refurbish and restart” its nuclear facilities, to include the uranium enrichment facility at Yongbyon and its graphite-moderated plutonium production reactor, which was shut down in 2007. We assess that North Korea has followed through on its announcement by expanding its Yongbyon enrichment facility and restarting the plutonium production reactor. We further assess that North Korea has been operating the reactor long enough so that it could begin to recover plutonium from the reactor’s spent fuel within a matter of weeks to months.

North Korea has also expanded the size and sophistication of its ballistic missile forces—from close-range ballistic missiles to intercontinental ballistic missiles (ICBMs)—and continues to conduct test launches. In May 2015, North Korea claimed that it successfully tested a ballistic missile from a submarine. Pyongyang is also committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States; it has publicly displayed its KN08 road-mobile ICBM on multiple occasions. We assess that North Korea has already taken initial steps toward fielding this system, although the system has not been flight-tested.

Although North Korea issues official statements that include its justification for building nuclear weapons and threats to use them as a defensive or retaliatory measure, we do not know the details of Pyongyang’s nuclear doctrine or employment concepts. We have long assessed that Pyongyang’s nuclear capabilities are intended for deterrence, international prestige, and coercive diplomacy.

### **China Modernizing Nuclear Forces**

The Chinese People’s Liberation Army’s (PLA’s) has established a Rocket Force—replacing the longstanding Second Artillery Corps—and continues to modernize its nuclear missile force by adding more survivable road-mobile systems and enhancing its silo-based systems. This new generation of missiles is intended to ensure the viability of China’s strategic deterrent by providing a second-strike capability. In addition, the PLA Navy continues to develop the JL-2 submarine-launched ballistic missile (SLBM) and might produce additional JIN-class nuclear-powered ballistic missile submarines. The JIN-class submarines—armed with JL-2 SLBMs—will give the PLA Navy its first long-range, sea-based nuclear capability.

### **Russian Cruise Missile Violates the INF Treaty**

Russia has developed a ground-launched cruise missile that the United States has declared is in violation of the Intermediate-Range Nuclear Forces (INF) Treaty. Russia has denied it is violating the INF Treaty. In 2013, a senior Russian administration official stated publicly that the world had changed since the INF Treaty was signed 1987 and noted that Russia was “developing appropriate weapons systems” in light of the proliferation of intermediate- and shorter-range ballistic missile technologies around the world, and Russian officials have made statements in the past regarding the unfairness of a Treaty that prohibits

Russia, but not some of its neighbors, from developing and processing ground-launched missiles with ranges between 500 to 5,500 kilometers.

### **Chemical Weapons in Syria and Iraq**

We assess that Syria has not declared all the elements of its chemical weapons program to the Chemical Weapons Convention (CWC). Despite the creation of a specialized team and months of work by the Organization for the Prohibition of Chemical Weapons (OPCW) to address gaps and inconsistencies in Syria's declaration, numerous issues remain unresolved. Moreover, we continue to judge that the Syrian regime has used chemicals as a means of warfare since accession to the CWC in 2013. The OPCW Fact-Finding Mission has concluded that chlorine had been used on Syrian opposition forces in multiple incidents in 2014 and 2015. Helicopters—which only the Syrian regime possesses—were used in several of these attacks.

We assess that nonstate actors in the region are also using chemicals as a means of warfare. The OPCW investigation into an alleged ISIL attack in Syria in August led it to conclude that at least two people were exposed to sulfur mustard. We continue to track numerous allegations of ISIL's use of chemicals in attacks in Iraq and Syria, suggesting that attacks might be widespread.

### **Iran Adhering to Deal To Preserve Capabilities and Gain Sanctions Relief**

Iran probably views the Joint Comprehensive Plan of Action (JCPOA) as a means to remove sanctions while preserving some of its nuclear capabilities, as well as the option to eventually expand its nuclear infrastructure. We continue to assess that Iran's overarching strategic goals of enhancing its security, prestige, and regional influence have led it to pursue capabilities to meet its nuclear energy and technology goals and give it the ability to build missile-deliverable nuclear weapons, if it chooses to do so. Its pursuit of these goals will dictate its level of adherence to the JCPOA over time. We do not know whether Iran will eventually decide to build nuclear weapons.

We also continue to assess that Iran does not face any insurmountable technical barriers to producing a nuclear weapon, making Iran's political will the central issue. Iran's implementation of the JCPOA, however, has extended the amount of time Iran would need to produce fissile material for a nuclear weapon from a few months to about a year. The JCPOA has also enhanced the transparency of Iran's nuclear activities, mainly through improved access by the International Atomic Energy Agency (IAEA) and investigative authorities under the Additional Protocol to its Comprehensive Safeguard Agreement.

As a result, the international community is well postured to quickly detect changes to Iran's declared nuclear facilities designed to shorten the time Iran would need to produce fissile material. Further, the JCPOA provides tools for the IAEA to investigate possible breaches of prohibitions on specific R&D activities that could contribute to the development of a nuclear weapon.

We judge that Tehran would choose ballistic missiles as its preferred method of delivering nuclear weapons, if it builds them. Iran's ballistic missiles are inherently capable of delivering WMD, and Tehran already has the largest inventory of ballistic missiles in the Middle East. Iran's progress on space launch vehicles—along with its desire to deter the United States and its allies—provides Tehran with the means and motivation to develop longer-range missiles, including ICBMs.

## Genome Editing

Research in genome editing conducted by countries with different regulatory or ethical standards than those of Western countries probably increases the risk of the creation of potentially harmful biological agents or products. Given the broad distribution, low cost, and accelerated pace of development of this dual-use technology, its deliberate or unintentional misuse might lead to far-reaching economic and national security implications. Advances in genome editing in 2015 have compelled groups of high-profile US and European biologists to question unregulated editing of the human germline (cells that are relevant for reproduction), which might create inheritable genetic changes. Nevertheless, researchers will probably continue to encounter challenges to achieve the desired outcome of their genome modifications, in part because of the technical limitations that are inherent in available genome editing systems.

## SPACE AND COUNTERSPACE

### Space

**Global Trends.** Changes in the space sector will evolve more quickly in the next few years as innovation becomes more ubiquitous, driven primarily by increased availability of technology and growing private company investment. The number of space actors is proliferating, with 80 countries participating in space activities and more expected in the next few years. New entrants from the private space sector—leveraging lowering costs in aerospace technology and innovations in other technology sectors, such as big data analytics, social media, automation, and additive manufacturing—will increase global access to space-enabled applications, such as imaging, maritime automatic identification system (AIS), weather, Internet, and communications.

**Military and Intelligence.** Foreign governments will expand their use of space services—to include reconnaissance, communications, and position, navigation, and timing (PNT)—for military and intelligence purposes, beginning to rival the advantages space-enabled services provide the United States. Russia and China continue to improve the capabilities of their military and intelligence satellites and grow more sophisticated in their operations. Russian military officials publicly tout their use of imaging and electronic-reconnaissance satellites to support military operations in Syria—revealing some of their sophisticated military uses of space services.

### Counterspace

Threats to our use of military, civil, and commercial space systems will increase in the next few years as Russia and China progress in developing counterspace weapon systems to deny, degrade, or disrupt US space systems. Foreign military leaders understand the unique advantages that space-based systems provide to the United States. Russia senior leadership probably views countering the US space advantage as a critical component of warfighting. Its 2014 Military Doctrine highlights at least three space-enabled capabilities—“global strike,” the “intention to station weapons in space,” and “strategic non-nuclear precision weapons”—as main external military threats to the Russian Federation. Russia and China are also employing more sophisticated satellite operations and are probably testing dual-use technologies in space that could be applied to counterspace missions.



***Deny and Disrupt.*** We already face a global threat from electronic warfare systems capable of jamming satellite communications systems and global navigation space systems. We assess that this technology will continue to proliferate to new actors and that our more advanced adversaries will continue to develop more sophisticated systems in the next few years. Russian defense officials acknowledge that they have deployed radar-imagery jammers and are developing laser weapons designed to blind US intelligence and ballistic missile defense satellites.

***Destroy.*** Russia and China continue to pursue weapons systems capable of destroying satellites on orbit, placing US satellites at greater risk in the next few years. China has probably made progress on the antisatellite missile system that it tested in July 2014. The Russian Duma officially recommended in 2013 that Russia resume research and development of an airborne antisatellite missile to “be able to intercept absolutely everything that flies from space.”

## COUNTERINTELLIGENCE

The United States will continue to face a complex foreign intelligence threat environment in 2016. We assess that the leading state intelligence threats to US interests will continue to be Russia and China, based on their capabilities, intent, and broad operational scope. Other states in South Asia, the Near East, East Asia, and Latin America will pose local and regional intelligence threats to US interests. For example, Iranian and Cuban intelligence and security services continue to view the United States as a primary threat.

Penetrating and influencing the US national decisionmaking apparatus and Intelligence Community will remain primary objectives for numerous foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other sensitive areas will remain a persistent threat to US interests.

Insiders who disclose sensitive US Government information without authorization will remain a significant threat in 2016. The sophistication and availability of information technology that can be used for nefarious purposes exacerbate this threat both in terms of speed and scope of impact.

Nonstate entities, including international terrorist groups and transnational organized crime organizations, will continue to employ and potentially improve their intelligence capabilities, which include human, cyber, and technical means. Like state intelligence services, these nonstate entities recruit human sources and conduct physical and technical surveillance to facilitate their activities and avoid detection and capture.

## **TRANSNATIONAL ORGANIZED CRIME**

### **Some US Drug Threats Are Growing**

Transnational drug trafficking poses a strong and in many cases growing threat to the United States at home and to US security interests abroad. Supplies of some foreign-produced drugs in the United States are rising, and some criminals who market them are growing more sophisticated.

- Mexican drug traffickers, capitalizing on the strong US demand for heroin, have increased heroin production significantly since 2007. US border seizures nearly doubled between 2010 and 2014. Some Mexican trafficking groups—which collectively supply most of the heroin consumed in the United States—have mastered production of the white heroin preferred in eastern US cities and have been boosting overall drug potency by adding fentanyl. Fentanyl, which is 30 to 50 times more potent than heroin, is sometimes used as an adulterant and mixed with lower-grade heroin to increase its effects or mixed with diluents and sold as “synthetic heroin” with or without the buyers’ knowledge.
- Mexican traffickers have probably increased their production of the stimulant methamphetamine for the US market. US border seizures of the drug rose by nearly half between 2013 and 2014.
- Traffickers in the Andean countries have increased their manufacture of cocaine. Producers in Colombia—from which most US cocaine originates—increased output by nearly a third in 2014 over the prior year. Cocaine output will probably rise again in 2016 as previously planted coca crops fully mature.
- US availability of some new psychoactive substances—so-called “designer drugs” typically produced in Asia—has been increasing; UN scientists have identified more than 500 unique substances.

### **Transnational Organized Crime Groups Target Vulnerable States**

Transnational organized crime groups will pose a persistent and at times sophisticated threat to the wealth, health, and security of people around the globe. Criminal groups’ untaxed and unregulated enterprises drain state resources, crowd out legitimate commerce, increase official corruption, and impede economic competitiveness and fair trade. On occasion, transnational organized crime groups threaten countries’ security, spur increases in social violence, or otherwise reduce governability.

- Profit-minded criminals generally do not seek the reins of political power but rather to suborn, co-opt, or bully government officials in order to create environments in which criminal enterprise can thrive.
- Foreign-based transnational criminals are increasingly using online information systems to breach sovereign borders virtually, without the need to send criminal operatives abroad to advance illicit businesses.
- Organized crime and rebel groups in Africa and elsewhere are likely to increase their involvement in wildlife trafficking to fund political activities, enhance political influence, and purchase weapons. Illicit trade in wildlife, timber, and marine resources endangers the environment, threatens good

governance and border security in fragile regions, and destabilizes communities whose economic well-being depends on wildlife for biodiversity and ecotourism. Increased demand for ivory and rhino horn in East Asia has triggered unprecedented increases in poaching in Sub-Saharan Africa.

Human trafficking exploits and abuses individuals and challenges international security. Human traffickers leverage corrupt officials, porous borders, and lax enforcement to orchestrate their illicit trade. This exploitation of human lives for profit continues to occur in every country in the world—undermining the rule of law and corroding legitimate institutions of government and commerce. Trafficking in persons has become a lucrative source of revenue for transnational organized crime groups and terrorist organizations and is estimated to produce tens of billions of dollars annually. For example, terrorist or armed groups—such as ISIL, the Lord's Resistance Army, and Boko Haram—engage in kidnapping for the purpose of sexual slavery, sexual exploitation, and forced labor. These activities might also contribute to the funding and sustainment of such groups.

We assess that the ongoing global migration crises—a post-WWII record 60 million refugees and internally displaced persons—will fuel an increase in the global volume of human trafficking victims as men, women, and children undertake risky migration ventures and fall prey to sex trafficking, forced labor, debt bondage and other trafficking crimes. This continuing rise in global displacement and dangerous migration, both forced and opportunistic movements within countries and across national borders, will probably allow criminal groups and terrorist organizations to exploit vulnerable populations.

## **ECONOMICS AND NATURAL RESOURCES**

Global economic growth will probably remain subdued, in part because of the deceleration of China's economy. During 2015, preliminary figures indicate that worldwide GDP growth slipped to 3.1 percent, down from 3.4 percent the previous year, although advanced economies as a group enjoyed their strongest GDP growth since 2010 at nearly 2 percent. However, developing economies, which were already dealing with broad and sharp commodity-price declines that began in 2014, saw the first net capital outflows to developed countries since the late 1980s.

GDP growth for these economies was 4 percent in 2015, the lowest since 2009. The International Monetary Fund (IMF) is forecasting a slight growth upturn in 2016 but downgraded its forecast in January for both developed and developing economies. Adverse shocks such as financial instability in emerging markets, a steeper-than-expected slowdown in China's growth, or renewed uncertainty about Greece's economic situation, might prevent the predicted gradual increase in global growth.

### **Macroeconomic Stability**

Continued solid performance by the United States and the resumption of growth for many European states, even as the region continues to wrestle with the Greek debt crisis, will probably help boost growth rates for developed economies. However, increasing signs of a sustained deceleration of Chinese economic growth—particularly in sectors that are the most raw-material intensive—contributed to a continued decline in energy and commodity prices worldwide in 2015. Emerging markets and developing countries' difficulties were compounded by the declines in foreign investment inflows and increases in

resident capital outflows. The prospect of higher growth and interest rates in the United States is spurring net capital outflows from these countries, estimated to be more than \$700 billion in 2015, compared to an average yearly inflow of more than \$400 billion from 2009 to 2014. The global slowdown in trade is also contributing to a more difficult economic environment for many developing economies and might worsen if efforts to advance trade liberalization through the World Trade Organization (WTO) and regional trade deals stall.

### **Energy and Commodities**

Weak energy and commodity prices have been particularly hard on key exporters in Latin America; Argentina and Brazil experienced negative growth and their weakened currencies contributed to domestic inflation. A steeply declining economy in Venezuela—the result of the oil-price decline and years of poor economic policy and profligate government spending—will leave Caracas struggling to avoid default in 2016. Similarly, in Africa, declining oil revenues and past mismanagement have contributed to Angolan and Nigerian fiscal problems, currency strains, and deteriorating external balances. Falling prices have also forced commodity-dependent exporters, such as Ghana, Liberia, and Zambia, to make sharp budget cuts to contain deficits. Persian Gulf oil exporters, which generally have more substantial financial reserves, have nonetheless seen a sharp increase in budget deficits.

Declining energy prices and substantial increases in North American production have also discouraged initiatives to develop new resources and expand existing projects—including in Brazil, Canada, Iraq, and Saudi Arabia. They typically take years to complete, potentially setting the stage for shortfalls in coming years when demand recovers.

### **Arctic**

Diminishing sea ice is creating increased economic opportunities in the region and simultaneously raising Arctic nations' concerns about safety and the environment. Harsh weather and longer-term economic stakes have encouraged cooperation among the countries bordering the Arctic. As polar ice recedes and resource extraction technology improves, however, economic and security concerns will raise the risk of increased competition between Arctic and non-Arctic nations over access to sea routes and resources. Sustained low oil prices would reduce the attractiveness of potential Arctic energy resources. Russia will almost certainly continue to bolster its military presence along its northern coastline to improve its perimeter defense and control over its exclusive economic zone (EEZ). It will also almost certainly continue to seek international support for its extended continental shelf claim and its right to manage ship traffic within its EEZ. Moscow might become more willing to disavow established international processes or organizations concerning Arctic governance and act unilaterally to protect these interests if Russian-Western relations deteriorate further.

## **HUMAN SECURITY**

### **Environmental Risks and Climate Change**

Extreme weather, climate change, environmental degradation, related rising demand for food and water, poor policy responses, and inadequate critical infrastructure will probably exacerbate—and potentially

spark—political instability, adverse health conditions, and humanitarian crises in 2016. Several of these developments, especially those in the Middle East, suggest that environmental degradation might become a more common source for interstate tensions. We assess that almost all of the 194 countries that adopted the global climate agreement at the UN climate conference in Paris in December 2015 view it as an ambitious and long-lasting framework.

- The UN World Meteorological Organization (WMO) report attributes extreme weather events in the tropics and sub-tropical zones in 2015 to both climate change and an exceptionally strong El Niño that will probably persist through spring 2016. An increase in extreme weather events is likely to occur throughout this period, based on WMO reporting. Human activities, such as the generation of greenhouse gas emissions and land use, have contributed to extreme weather events including more frequent and severe tropical cyclones, heavy rainfall, droughts, and heat waves, according to a November 2015 academic report with contributions from scientists at the National Oceanic and Atmospheric Administration (NOAA). Scientists have more robust evidence to identify the influence of human activity on temperature extremes than on precipitation extremes.
- The Paris climate change agreement establishes a political expectation for the first time that all countries will address climate change. The response to the deal has been largely positive among government officials and nongovernmental groups, probably because the agreement acknowledges the need for universal action to combat climate change along with the development needs of lower-income countries. However, an independent team of climate analysts and the Executive Secretary of the UN climate forum have stated that countries' existing national plans to address climate change will only limit temperature rise to 2.7 degrees Celsius by 2100.

## Health

Infectious diseases and vulnerabilities in the global supply chain for medical countermeasures will continue to pose a danger to US national security in 2016. Land-use changes will increase animal-to-human interactions and globalization will raise the potential for rapid cross-regional spread of disease, while the international community remains ill prepared to collectively coordinate and respond to disease threats. Influenza viruses, coronaviruses such as the one causing Middle Eastern Respiratory Syndrome (MERS), and hemorrhagic fever viruses such as Ebola are examples of infectious disease agents that are passed from animals to humans and can quickly pose regional or global threats. Zika virus, an emerging infectious disease threat first detected in the Western Hemisphere in 2014, is projected to cause up to 4 million cases in 2016; it will probably spread to virtually every country in the hemisphere. Although the virus is predominantly a mild illness, and no vaccine or treatment is available, the Zika virus might be linked to devastating birth defects in children whose mothers were infected during pregnancy. Many developed and developing nations remain unable to implement coordinated plans of action to prevent infectious disease outbreaks, strengthen global disease surveillance and response, rapidly share information, develop diagnostic tools and countermeasures, or maintain the safe transit of personnel and materials.

- Human encroachment into animal habitats, including clearing land for farm use and urbanization, is recognized as a contributing factor in the emergence of new infectious diseases. The populations of Asia and Africa are urbanizing and growing faster than those of any other region, according to the

UN. Emerging diseases against which humans have no preexisting immunity or effective therapies pose significant risks of becoming pandemics.

### **Atrocities and Instability**

Risks of atrocities, large-scale violence, and regime-threatening instability will remain elevated in 2016. A vicious cycle of conflict resulting from weak governance, the rise of violent non-state actors, insufficient international capacity to respond to these complex challenges, and an increase in global migration all contribute to global security risks. Weak global growth, particularly resulting from the cascading effect of slower Chinese growth that will hurt commodity exporters, will also exacerbate risk.

- Regional spillover will probably spread. For example, the long-term impact of civil war in Syria is reinforcing sectarian differences in Iraq, and the flight of Syrians to Turkey, Jordan, and Lebanon, and then onward to Europe is sowing regional tensions and straining national governments.
- As of 2015, the central governments of seven states are unable to project authority and provide goods and services throughout at least 50 percent of their respective territory; this number is the largest at any point in the past 60 years.
- The risk of waning support for universal human rights norms is increasing as authoritarian regimes push back against human rights in practice and in principle.

### **Global Displacement**

Europe will almost certainly continue to face record levels of arriving refugees and other migrants in 2016 unless the drivers causing this historic movement toward the continent change significantly in 2016, which we judge is unlikely. Migration and displacement will also probably be an issue within Asia and Africa as well as the Americas. In total, about 60 million people are displaced worldwide, according to the UN High Commissioner for Refugees (UNHCR). These 60 million consist of approximately 20 million refugees, 38 million internally displaced persons (IDPs), and approximately 2 million stateless persons, also according to UNHCR statistics.

- Wars, weak border controls, and relatively easy and affordable access to routes and information are driving this historic increase in mobility and displacement.

The growing scope and scale of human displacement will probably continue to strain the response capacity of the international community and drive a record level of humanitarian requests. At the same time, host and transit countries will struggle to develop effective responses and, in some cases, manage domestic fears of terrorists exploiting migrant flows after the Paris attacks in November 2015.

- In 2015, the UN received less than half of its requested funding for global assistance, suggesting that the UN's 2016 request is also likely to be underfunded.



---

## REGIONAL THREATS

---

Emerging trends suggest that geopolitical competition among the major powers is increasing in ways that challenge international norms and institutions. Russia, in particular, but also China seek greater influence over their respective neighboring regions and want the United States to refrain from actions they perceive as interfering with their interests—which will perpetuate the ongoing geopolitical and security competition around the peripheries of Russia and China, to include the major sea lanes. They will almost certainly eschew direct military conflict with the United States in favor of contests at lower levels of competition—to include the use of diplomatic and economic coercion, propaganda, cyber intrusions, proxies, and other indirect applications of military power—that intentionally blur the distinction between peace and wartime operations.

Although major power competition is increasing, the geopolitical environment continues to offer opportunities for US cooperation. In addition, despite the prospect for increased competition, the major powers, including Russia and China, will have incentives to continue to cooperate with the United States on issues of shared interest that cannot be solved unilaterally. A future international environment defined by a mix of competition and cooperation among major powers, however, will probably encourage ad-hoc approaches to global challenges that undermine existing international institutions.

### EAST ASIA

#### China

China will continue to pursue an active foreign policy—especially within the Asia Pacific—highlighted by a firm stance on competing territorial claims in the East and South China Seas, relations with Taiwan, and its pursuit of economic engagement across East Asia. Regional tension will continue as China pursues construction at its expanded outposts in the South China Sea and because competing claimants might pursue actions that others perceive as infringing on their sovereignty. Despite the meeting between China's and Taiwan's Presidents in November 2015, Chinese leaders will deal with a new president from a different party in Taiwan following elections in January. China will also pursue efforts aimed at fulfilling its "One Belt, One Road" initiative to expand China's economic role and outreach across Asia.

China will continue to incrementally increase its global presence. Mileposts have included symbolic and substantive developments, such as the IMF's decision in November 2016 to incorporate the renminbi into its Special Drawing Rights currency basket and China's opening of the Asian Infrastructure Investment Bank in early 2016. China will increasingly be a factor in global responses to emerging problems, as illustrated by China's participation in UN peacekeeping operations, WHO's Ebola response, and infrastructure construction in Africa and Pakistan.

Amid new economic challenges, Chinese leaders are pursuing an ambitious agenda of economic, legal, and military reforms aimed at bolstering the country's long-term economic growth potential, improving

government efficiency and accountability, and strengthening the control of the Communist Party. The scope and scale of the reform agenda—coupled with an ongoing anti-corruption campaign—might increase the potential for internal friction within China’s ruling Communist Party. Additionally, China’s leaders, who have declared slower economic growth to be the “new normal,” will nonetheless face pressure to stabilize growth at levels that still support strong job creation.

## **Southeast Asia**

Regional integration via the Association of Southeast Asian Nations (ASEAN) made gains in 2015 with the establishment of the ASEAN Community. However, ASEAN cohesion on economic and security issues will continue to face challenges stemming from differing development levels among ASEAN members and their varying threat perceptions of China’s regional ambitions and assertiveness in the South China Sea.

Democracy in many Southeast Asian nations remains fragile. Elites—rather than the populace—retain a significant level of control and often shape governance reforms to benefit their individual interests rather than to promote democratic values. Corruption and cronyism continue to be rampant in the region, and the rising threat of ISIL might provide some governments with a new rationale to not only address the terrorist threat but also curb opposition movements, like some leaders in the region did in the post 9/11 environment. The new National League for Democracy-led government in Burma is poised to continue the country’s democratic transition process, but given its lack of governing experience, the learning curve will be steep. The Burmese constitution also ensures that the military will retain a significant level of power in the government, hampering the NLD to put its own stamp on the ongoing peace process. In Thailand, the military-led regime is positioned to remain in power through 2017.

## **North Korea**

Since taking the helm of North Korea in December 2011, Kim Jong Un has further solidified his position as the unitary leader and final decision authority through purges, executions, and leadership shuffles. Kim and the regime have publicly emphasized—and codified—North Korea’s focus on advancing its nuclear weapons program, developing the country’s troubled economy, and improving the livelihood of the North Korean people, while maintaining the tenets of a command economy. Despite efforts at diplomatic outreach, Kim continues to challenge the international community with provocative and threatening behavior in pursuit of his goals, as prominently demonstrated in the November 2014 cyberattack on Sony, the August 2015 inter-Korean confrontation spurred by the North’s placement of landmines that injured two South Korean soldiers, and the fourth nuclear test in January 2016.

# **RUSSIA AND EURASIA**

## **Russia**

Moscow’s more assertive foreign policy approach, evident in Ukraine and Syria, will have far-reaching effects on Russia’s domestic politics, economic development, and military modernization efforts.

President Vladimir Putin has sustained his popular approval at or near record highs for nearly two years after illegally annexing Crimea. Nevertheless, the Kremlin's fears of mass demonstration remain high, and the government will continue to rely on repressive tactics to defuse what it sees as potential catalysts for protests in Russia. The Kremlin's fear of instability and its efforts to contain it will probably be especially acute before the September 2016 Duma election.

The Russian economy will continue to shrink as a result of longstanding structural problems—made worse by low energy prices and economic sanctions—and entered into recession in 2015. A consensus forecast projects that GDP will contract by 3.8 percent in 2015 and will probably decline between 2-3 percent in 2016 if oil prices remain around \$40 per barrel or only 0.6 percent if oil returns to \$50 per barrel. Real wages declined throughout most of 2015 and the poverty rate and inflation have also worsened.

We assess that Putin will continue to try to use the Syrian conflict and calls for cooperation against ISIL to promote Russia's Great Power status and end its international isolation. Moscow's growing concern about ISIL and other extremists has led to direct intervention on the side of Bashar al-Asad's regime and efforts to achieve a political resolution to the Syrian conflict on Russia's terms. Since the terrorist attacks in Paris and over the Sinai, Russia has redoubled its calls for a broader anti-terrorism coalition. Meanwhile, growing Turkish-Russian tensions since Turkey's shootdown of a Russian jet in November 2015 raise the specter of miscalculation and escalation.

Despite Russia's economic slowdown, the Kremlin remains intent on pursuing an assertive foreign policy in 2016. Russia's willingness to covertly use military and paramilitary forces in a neighboring state continues to cause anxieties in states along Russia's periphery, to include NATO allies. Levels of violence in eastern Ukraine have decreased, but Moscow's objectives in Ukraine—maintaining long-term influence over Kyiv and frustrating Ukraine's attempts to integrate into Western institutions—will probably remain unchanged in 2016.

Since the crisis began in Ukraine in 2014, Moscow has redoubled its efforts to reinforce its influence in Eurasia. Events in Ukraine raised Moscow's perceived stakes for increasing its presence in the region to prevent future regime change in the former Soviet republics and for accelerating a shift to a multipolar world in which Russia is the uncontested regional hegemon in Eurasia. Moscow will therefore continue to push for greater regional integration, raising pressure on neighboring states to follow the example of Armenia, Belarus, Kazakhstan, and Kyrgyzstan and join the Moscow-led Eurasian Economic Union.

Moscow's military foray into Syria marks its first use of significant expeditionary combat power outside the post-Soviet space in decades. Its intervention underscores both the ongoing and substantial improvements in Russian military capabilities and the Kremlin's confidence in using them as a tool to advance foreign policy goals. Despite its economic difficulties, Moscow remains committed to modernizing its military.

Russia continues to take information warfare to a new level, working to fan anti-US and anti-Western sentiment both within Russia and globally. Moscow will continue to publish false and misleading information in an effort to discredit the West, confuse or distort events that threaten Russia's image, undercut consensus on Russia, and defend Russia's role as a responsible and indispensable global power.

## Ukraine, Belarus, and Moldova

The implementation timeline for the Minsk agreements has been extended through 2016, although opposition from **Ukraine**, Russia, and the separatists on key remaining Minsk obligations might make progress slow and difficult in 2016. Sustained violence along the Line of Contact delineating the separatist-held areas will probably continue to complicate a political settlement, and the potential for escalation remains.

Ukraine has made progress in its reform efforts and its moves to bolster ties to Western institutions. Ukraine will continue to face serious challenges, however, including sustaining progress on key reforms and passing constitutional amendments—required under the Minsk agreements to devolve political power and fiscal authority to the regions.

**Belarus** continues its geopolitical balancing act, attempting to curry favor with the West without antagonizing Russia. President Lukashenko released several high-profile political prisoners in August 2015 and secured reelection to a fifth term in October 2015 without cracking down on the opposition as he has in previous elections. These developments prompted the EU and the United States to implement temporary sanctions relief, providing a boost to a Belarusian economy.

**Moldova** faces a turbulent year in 2016. Popular discontent over government corruption and misrule continues to reverberate after a banking scandal sparked large public protests, and political infighting brought down a government coalition of pro-European parties in October 2015. Continued unrest is likely. The breakaway pro-Russian region is also struggling economically and will remain dependent on Russian support.

## The Caucasus and Central Asia

Even as **Georgia** progresses with reforms, Georgian politics will almost certainly be volatile as political competition increases. Economic challenges are also likely to become a key political vulnerability for the government before the 2016 elections. Rising frustration among Georgia's elites and the public with the slow pace of Western integration and increasingly effective Russian propaganda raise the prospect that Tbilisi might slow or suspend efforts toward greater Euro-Atlantic integration. Tensions with Russia will remain high, and we assess that Moscow will raise the pressure on Tbilisi to abandon closer EU and NATO ties.

Tensions between **Armenia** and **Azerbaijan** over the separatist region of Nagorno-Karabakh remained high in 2015. Baku's sustained military buildup coupled with declining economic conditions in Azerbaijan are raising the potential that the conflict will escalate in 2016. Azerbaijan's aversion to publicly relinquishing its claim to Nagorno-Karabakh proper and Armenia's reluctance to give up territory it controls will continue to complicate a peaceful resolution.

**Central Asian** states remain concerned about the rising threat of extremism to the stability of their countries, particularly in light of a reduced Coalition presence in Afghanistan. Russia shares these concerns and is likely to use the threat of instability in Afghanistan to increase its involvement in Central Asian security affairs. However, economic challenges stemming from official mismanagement, low commodity prices, declining trade and remittances associated with Russia's weakening economy, and

ethnic tensions and political repression, are likely to present the most significant instability threat to these countries.

## **EUROPE**

### **Key Partners**

European governments will face continued political, economic, and security challenges deriving from mass migration to Europe, terrorist threats, a more assertive Russia, and slow economic recovery. Differences among national leaders over how best to confront the challenges are eroding support for deeper EU integration and will bolster backing for populist leaders who favor national prerogatives over EU-wide remedial strategies.

The European Commission expects 1.5 million migrants to arrive in Europe in 2016—an influx that is prompting European officials to focus on improving border security, particularly at the Schengen Zone's external borders, and putting the free movement of people within the EU at risk. Several European governments are using military forces in domestic security roles.

The European Commission has warned against drawing a link between terrorists and refugees, but populist and far-right leaders throughout Europe are preying on voters' security fears by highlighting the potential dangers of accepting migrants fleeing war and poverty. Some EU leaders are citing the November 2015 terrorist attacks in Paris to justify erecting fences to stem the flow of people.

European countries will remain active and steadfast allies on the range of national security threats that face both the United States and Europe—from energy and climate change to countering violent extremism and promoting democracy. Although the majority of NATO allies have successfully halted further declines in defense spending, European military modernization efforts will take several years before marked improvement begins to show.

Europe also continues to insist on full implementation of the Minsk agreement to stop violence in Ukraine. However, European governments differ on the proper extent of engagement with Moscow.

Europe's economic growth, which the EU projects will be moderate, could falter if emerging market economies slow further, which would decrease the demand for European exports. The EU continues to struggle to shake off the extended effects of its economic recession, with lingering worries over high unemployment, weak demand, and lagging productivity. Greece also remains a concern for the EU. The agreement between Greece and its creditors is an important step forward for restoring trust among the parties and creating the conditions for a path forward for Greece within the Eurozone. Developing the details of the agreement and its full implementation remain challenges.

### **The Balkans**

Ethnic nationalism and weak institutions in the Balkans remain enduring threats to stability. Twenty years after the end of the Bosnian War and the signing of the Dayton Agreement, Bosnia and Herzegovina

remains culturally and administratively divided, weighed down by a barely functional and inefficient bureaucracy. The country, one of Europe's poorest, has endured negative GDP growth since the 2008 international financial crisis and is reliant on the support of international institutions including the IMF. Youth unemployment, estimated at 60 percent, is the world's highest.

Kosovo has made progress toward full, multiethnic democracy, although tensions between Kosovo Albanians and Kosovo Serbs remain. In Macedonia, an ongoing political crisis and concerns about radicalization among ethnic Albanian Muslims threatens to aggravate already-tense relations between ethnic majority Macedonians and the country's minority Albanians, fifteen years after a violent interethnic conflict between the two groups ended. Social tensions in the region might also be exacerbated if the Western Balkans becomes an unwilling host to significant migrant populations.

## **Turkey**

Turkey remains a partner in countering ISIL and minimizing foreign fighter flows. Ankara will continue to see the Kurdistan Workers' Party (PKK) as its number one security threat and will maintain military and political pressure on the PKK, as well as on the Democratic Union Party (PYD) and its armed affiliate People's Protection Units (YPG), which Turkey equates with the PKK. Turkey is extremely concerned about the increasing influence of the PYD and the YPG along its borders, seeing them as a threat to its territorial security and its efforts to control Kurdish separatism within its borders.

Turkey is concerned about Russia's involvement in the region in support of Asad, the removal of whom Turkey sees as essential to any peace settlement. Turkey is also wary of increased Russian cooperation with the Kurds and greater Russian influence in the region that could counter Turkey's leadership role. The Russian-Iranian partnership and Iran's attempts to expand Shiite influence in the region are also security concerns for Turkey.

The refugee flow puts significant strain on Turkey's economy, which has amounted to \$9 billion according to a statement by Turkish President Recep Tayyip Erdogan. Refugees have also created infrastructure and social strains, particularly regarding access to education and employment. Turkey tightened its borders in 2015 and is working to stanch the flow of migrants to Europe and address refugee needs.

## **MIDDLE EAST AND NORTH AFRICA**

### **Iraq**

In Iraq, anti-ISIL forces will probably make incremental battlefield gains through spring 2016. Shia militias and Kurdish forces in northern Iraq have recaptured Bayji and Sinjar, respectively, from the Islamic State of Iraq and the Levant (ISIL). In western Iraq, the Iraqi Security Forces (ISF) have retaken most of the greater Ramadi area from ISIL and will probably clear ISIL fighters from the city's urban core in the coming month.

ISIL's governance of areas it controls is probably faltering as airstrikes take a toll on the group's sources of income, hurting ISIL's ability to provide services, and causing economic opportunities for the population



to dwindle. Even so, the Iraqi Sunni population remains fearful of the Shia-dominated government in Baghdad. This fear has been heightened as Iranian-backed Shia militias play a lead role in retaking Sunni-majority areas, suggesting Iraq's Sunnis will remain willing to endure some deprivation under ISIL rule.

Prime Minister Haydar al-Abadi will probably continue to struggle to advance his reforms—which aim to combat corruption and streamline government—because of resistance from Iraqi elites who view the reforms as threatening to their entrenched political interests. Meanwhile, the drop in oil prices is placing strain on both Baghdad's and Irbil's budgets, constraining their ability to finance counter-ISIL operations and limiting options to address potential economically driven unrest.

## Syria

We assess that foreign support will allow Damascus to make gains in some key areas against the opposition and avoid further losses, but it will be unable to fundamentally alter the battlespace. Increased Russian involvement, particularly airstrikes, will probably help the regime regain key terrain in high priority areas in western Syria, such as Aleppo and near the coast, where it suffered losses to the opposition in summer 2015. ISIL is under threat on several fronts in Syria and Iraq from increased Coalition and government operations.

Manpower shortages will continue to undermine the Syrian regime's ability to accomplish strategic battlefield objectives. The regime still lacks the personnel needed to capture and hold key areas and strategically defeat the opposition or ISIL. Damascus increasingly relies on militias, reservists, and foreign supporters—such as Iran and Lebanese Hizballah—to generate manpower, according to press reporting.

The Syrian regime and most of the opposition are participating in UN-mediated talks that started in early February in Geneva. Both sides probably have low expectations for the negotiations, with the opposition calling for ceasefires and humanitarian assistance as a precondition. The negotiations, without a ceasefire agreement, will not alter the battlefield situation.

The humanitarian situation in Syria continues to deteriorate. In December 2015 and January 2016, the number of Syrian refugees registered or in the process of registering in the Middle East and North Africa rose by nearly 102,000 from 4.3 million to 4.4 million, according to UN data. The refugees are putting significant strain on countries surrounding Syria as well as on Europe. Turkey hosts more than 2.2 million refugees; Lebanon has about 1.1 million; Jordan has more than 630,000; Iraq has 245,000. Approximately 500,000 have fled to Europe, according to the UN. The more than 4 million refugees and 6.5 million estimated internally displaced persons (IDPs) account for 49 percent of Syria's preconflict population.

- Estimates of fatalities in Syria since the start of the civil war vary, but most observers calculate that at least 250,000 men, women, and children on all sides of the conflict have lost their lives since 2011.
- On 22 December, the UN Security Council unanimously adopted resolution 2258, which renews the UN's authority to utilize cross-border deliveries for humanitarian assistance to Syria through 10

January 2017. Since July 2014, the UN has provided food to 2.4 million people, water and sanitation to 1.3 million people, and medical supplies to 4.1 million people through its cross-border deliveries.

- Separately, the Syrian Government began requiring in mid-November that aid agencies get humanitarian assistance notarized by the Syrian embassies in the country of product origin. This requirement previously applied only to commercial goods and might delay future UN food deliveries within Syria, according to the UN.

## Libya

We assess that insecurity and conflict in Libya will persist in 2016, posing a continuing threat to regional stability. The country has been locked in civil war between two rival governments and affiliated armed groups. The 17 December signing of a UN-brokered agreement to form a Government of National Accord (GNA) resulted from a year-long political dialogue that sought to end the ongoing civil war and reconcile Libya's rival governments. However, the GNA will face a number of obstacles in establishing its authority and security across the country. The GNA still faces the difficult task of forming a capable, centralized security force. It will also be challenged to confront terrorist groups such as ISIL, which has exploited the conflict and political instability in the country to expand its presence.

- The rival governments—the internationally recognized Tobruk-based House of Representatives (House) and the Tripoli-based General National Congress (GNC) have participated in UN-brokered peace talks since fall 2014. Reaction to the deal and the proposed GNA has been mixed, and hardliners on both sides have opposed the agreement.
- (U) On 25 January, the House voted to approve the UN-brokered deal with conditions but rejected a controversial article granting the GNA's Presidency Council interim control of the military. The House also rejected the GNA's proposed cabinet and demanded a smaller ministerial slate.
- Libya's economy has deteriorated because of the conflict. Oil exports—the primary source of government revenue—have fallen significantly from the pre-revolution level of 1.6 billion barrels per day. Libya's oil sector also faces continued threats from terrorist groups; ISIL attacked oil production and export facilities in February 2015, September 2015, and January 2016.

Meanwhile, extremists and terrorists have exploited the security vacuum to plan and launch attacks in Libya and throughout the region. The permissive security environment has enabled ISIL to establish one of its most developed branches outside of Syria and Iraq. As of late 2015, ISIL's branch in Libya maintained a presence in Surt, Benghazi, Tripoli, Ajdabiya, and other areas of the country, according to press reports. Members of ISIL in Libya continue to stage attacks throughout the country.

## Yemen

The Yemen conflict will probably remain in a strategic stalemate through mid-2016. Negotiations between the Saudi-led coalition and the Huthi-aligned forces remain stalled, but neither side is able to achieve decisive results through military force. Huthi-aligned forces almost certainly remain committed to fighting following battlefield setbacks in the Aden and Marib Governorates in 2015 and probably intend to retake lost territory in those areas.

Nonetheless, regional stakeholders on both sides of Yemen's conflict, including Iran, which continues to back the Huthis, are signaling willingness to participate in peace talks. Even a cease-fire of a few days or weeks would facilitate the entry and distribution of commercial and humanitarian goods inside Yemen, where at least 21 million people—80 percent of the population—require assistance, according to the UN.

AQAP and ISIL's affiliates in Yemen have exploited the conflict and the collapse of government authority to gain new recruits and allies and expand their territorial control. In December, AQAP seized the southern city of Zinjibar, adding to its capture of the coastal city of Mukalla to the east.

## Iran

Since January, Tehran met the demands for implementation of the Joint Comprehensive Plan of Action (JCPOA), exchanged detainees, and released 10 US sailors. Despite these developments, the Islamic Republic of Iran presents an enduring threat to US national interests because of its support to regional terrorist and militant groups and the Asad regime, as well as its development of advanced military capabilities. Tehran views itself as leading the "axis of resistance"—which includes the Asad regime and subnational groups aligned with Iran, especially Lebanese Hezbollah and Iraqi Shia militants. Their intent is to thwart US, Saudi, and Israeli influence, bolster its allies, and fight ISIL's expansion. Tehran might even use American citizens detained when entering Iranian territories as bargaining pieces to achieve financial or political concessions in line with their strategic intentions.

Iran's involvement in the Syrian, Iraqi, and Yemeni conflicts deepened in 2015. In Syria, Iran more openly acknowledged the deaths of Iranian "martyrs," increased Iranian troop levels, and took more of a frontline role against "terrorists." In Iraq, Iranian combat forces employed rockets, artillery, and drones against ISIL. Iran also supported Huthi rebels in Yemen by attempting to ship lethal aid to the Huthis. Tehran will almost certainly remain active throughout the Persian Gulf and broader Middle East in 2016 to support its regional partners and extend its regional influence. Iranian officials believe that engaging adversaries away from its borders will help prevent instability from spilling into Iran and reduce ISIL's threat to Iran and its regional partners. Iran has also increased cooperation with Russia in the region.

Supreme Leader Khamenei continues to view the United States as a major threat to Iran, and we assess that his views will not change, despite implementation of the JCPOA deal. In October 2015, Khamenei publicly claimed the United States was using the JCPOA to "infiltrate and penetrate" Iran. His statement prompted the Iranian hardliner-dominated security services to crack down on journalists and businessmen with suspected ties to the West. The crackdown was intended by hardliners to demonstrate to President Ruhani and to Washington that a broader opening to the West following JCPOA would not be tolerated. Iran released several US citizens in January 2016 who were being held in Iran; however, it might attempt to use any additional US citizens as bargaining chips for US concessions.

Iran's military and security services are keen to demonstrate that their regional power ambitions have not been altered by the JCPOA deal. One week prior to JCPOA Adoption Day, Iran publicized the launch of its new "long-range" and more accurate ballistic missile called the "Emad." Iran also publicizes development of its domestically produced weapons systems, submarines and surface combatants, artillery, and UAVs to deter potential adversaries and strengthen its regional influence and prestige.

Iran's involvement in the Syrian and Iraqi conflicts has enabled its forces to gain valuable on-the-ground experience in counterinsurgency operations.

## **Lebanon**

Lebanon will continue to struggle with the fallout from the civil war in neighboring Syria and faces a range of interlocking political, security, humanitarian, and economic challenges. The spillover from the Syrian conflict has had negative consequences on almost all aspects of life in Lebanon, from rising sectarianism to major strains on infrastructure and public services, further straining the country's delicate political balance.

- Lebanon's most immediate security threat is from Syrian-based extremists on its northeastern border. The Lebanese army has carried out multiple operations against Nusra Front and ISIL to secure the border and prevent against the flow of terrorists into the country. Beirut also faces threats from Sunni extremists in the country who are retaliating against Lebanese Hizballah's military involvement in the Syrian civil war.
- The influx of about 1.1 million Sunni Syrian refugees to Lebanon has altered the country's sectarian demographics and is badly straining public services and burdening the economy. The Lebanese economy will probably remain stagnant throughout 2016, as protracted regional instability and political gridlock at home continue to erode the country's competitiveness.

## **Egypt**

Egypt faces a persistent threat of terrorist and militant activity directed primarily at state security forces in both the Sinai Peninsula and in mainland Egypt. The security services have initiated a counterterrorism campaign to disrupt and detain Sinai-based militants; however, terrorist groups still retain the ability to conduct attacks.

- ISIL's branch in Sinai (ISIL-Sinai) has conducted dozens of lethal attacks on military and security personnel, some of which suggest sophisticated and coordinated attack planning, according to press reports.
- ISIL-Sinai claimed responsibility for the downing of a Russian aircraft in the Sinai in October 2015, which, if true, would demonstrate the expanding threat from ISIL and its regional branches.
- The continued threat of terrorism places further strain on Egypt's economy by harming Egypt's tourism industry, a key source of revenue. The country is also grappling with high poverty and unemployment rates.

## **Tunisia**

Tunisia's first post-transitional democratic government since the 2011 Arab Spring revolution is marking its first year in office. Since the revolution, the country has overcome deep political divisions to reach consensus on key political issues, develop a new constitution, and elect a new government, according to

press and academic reports. Despite the government's significant strides in its democratic transition, Tunisia faces challenges in consolidating these achievements.

- Tunisia is confronting a threat from terrorist groups exploiting Libya's permissive environment to plan and launch attacks, as well as from groups operating within Tunisia's borders, according to press reports. The perpetrators of the terrorist attack on the Bardo Museum in Tunis in March 2015 and hotels in Sousse in June—both claimed by ISIL—trained at a terrorist camp in Libya, according to press reports.
- The government inherited high unemployment, particularly among youth, and a high budget deficit according to press reports. The Bardo and Sousse terrorist attacks have disrupted tourism, a critical source of revenues and jobs.

## **SOUTH ASIA**

### **Afghanistan**

The Kabul Government will continue to face persistent hurdles to political stability in 2016, including eroding political cohesion, assertions of authority by local powerbrokers, recurring financial shortfalls, and countrywide, sustained attacks by the Taliban. Political cohesion will remain a challenge for Kabul as the National Unity Government will confront larger and more divisive issues later in 2016, including the implementation of election reforms, long-delayed parliamentary elections, and a potential change by a Loya Jirga that might fundamentally alter Afghanistan's constitutional order. Kabul will be unable to effectively address its dire economic situation or begin to curb its dependence on foreign aid until it first contains the insurgency, which is steadily chipping away at Afghanistan's security. In this environment, international financial aid will remain the most important external determinant of the Kabul government's strength. We assess that fighting in 2016 will be more intense than 2015, continuing a decade-long trend of deteriorating security that will compound these challenges. The fighting will continue to threaten US personnel, our Allies, and international partners—including Afghans—particularly in Kabul and other urban population centers. The Afghan National Security Forces (ANSF), with the help of anti-Taliban powerbrokers and international funding, will probably maintain control of most major population centers. However, the forces will very likely cede control of some rural areas. Without international funding, the ANSF will probably not remain a cohesive or viable force.

The Taliban has largely coalesced and is relatively cohesive under the leadership of new Taliban Senior Leader Mullah Akhtar Mohammad Mansur despite some early opposition. The Taliban's two-week seizure of the provincial capital of Kunduz provided an important boost to Mansur's leadership. The Taliban will continue to test the overstretched ANSF faced with problematic logistics, low morale, and weak leadership.

The Islamic State of Iraq and the Levant (ISIL) announced in January 2015 the formation of its Khorasan branch in South Asia, an amalgamation of primarily disaffected and rebranded former Afghan Taliban and Tehrik-e Taliban Pakistan (TTP) members. Despite quick early growth in 2015, ISIL's Khorasan branch

will probably remain a low-level threat to Afghan stability as well as to US and Western interests in the region in 2016.

## **Bangladesh**

Prime Minister Sheikh Hasina's continuing efforts to undermine the political opposition in Bangladesh will probably provide openings for transnational terrorist groups to expand their presence in the country. Hasina and other government officials have insisted publically that the killings of foreigners are the work of the Bangladesh Nationalist Party and the Bangladesh Jamaat-e Islami political parties and are intended to discredit the government. However, ISIL claimed responsibility for 11 high-profile attacks on foreigners and religious minorities. Other extremists in Bangladesh—including Ansarullah Bangla Team and al-Qa'ida in the Indian Subcontinent (AQIS)—have claimed responsibility for killing at least 11 progressive writers and bloggers in Bangladesh since 2013.

## **Pakistan and India**

Relations between Pakistan and India remain tense despite the resumption of a bilateral dialogue in December. Following a terrorist attack in early January on Pathankot Air Force base in India, which New Delhi blames on a Pakistani-based group, India's engagement with Pakistan will probably hinge in 2016 on Islamabad's willingness to take action against those in Pakistan linked to the attack.

# **SUB-SAHARAN AFRICA**

## **Central Africa**

Prospects for delayed elections in the **Democratic Republic of the Congo**, originally scheduled for 2016, increase the risk of political tensions and perhaps violence. Violence might also break out in the **Republic of Congo** where a controversial October 2015 constitutional referendum paved the way for long-serving President Denis Sassou-Nguesso to run for a new term in 2016 elections. Both governments have resorted to heavy-handed tactics to stifle opposition and subdue or prevent election-related protests.

In **Burundi**, violence related to President Pierre Nkurunziza's controversial reelection in July 2015 will almost certainly continue as a simmering crisis. The conflict might expand and intensify if increased attacks between the government and armed opposition provoke a magnified response from either side or if the security services fracture into divided loyalties.

The **Central African Republic** held peaceful presidential and parliamentary elections in late December, although they were marred by logistical issues. A run-off will probably take place in mid-February between the two top candidates, and we do not know how the armed spoilers and losing candidates will react. The risk of continued ethno-religious clashes between Christians and Muslims throughout the country remains high despite the presence of international peacekeeping forces, which are increasingly targets of violence.



## **Somalia**

The Somali Federal Government's authority will probably remain largely confined to the capital in 2016, and Mogadishu will continue to rely on the African Union Mission in Somalia (AMISOM) as a security guarantor against al-Shabaab as it prepares for elections in 2016.

## **South Sudan**

Implementation of the peace agreement between Juba and opposition elements will be slow as spoilers from both sides seek to stall progress. The return of former opposition members to Juba will almost certainly cause jockeying for positions of power. Localized fighting will continue and probably spread to previously unaffected areas, causing the humanitarian situation to worsen. Economic conditions will probably deteriorate further as inflation remains high and prices for staple goods rise, fueling dissatisfaction with the government.

## **Sudan**

President Bashir consolidated power following his reelection in April 2015, but the regime will continue attempts at a national dialogue, which will probably not placate a divided political opposition. The regime will almost certainly confront a range of challenges, including public dissatisfaction over a weakened economy. Divisions among armed opponents will almost certainly inhibit their ability to make significant gains against Khartoum. However, elements of the opposition will continue to wage insurgencies in the Southern Kordofan and Blue Nile states and Darfur. Sudan, listed as a state sponsor of terror since 1993, cut diplomatic ties with Iran in January following an attack on the Saudi Embassy in Tehran. Since 2014, Sudan's relations with Iran have cooled as Khartoum has grown closer to Riyadh.

## **Nigeria**

President Muhammadu Buhari and the Nigerian government will confront a wide range of challenges in 2016, many of which are deeply rooted and have no "quick fixes." His tasks include reviving a struggling economy – Africa's largest – diversifying sources of government revenue beyond oil, reining in corruption, addressing mounting state debts, reforming redundant parastatal organizations, and developing the power, agriculture, and transportation sectors. Nigeria will continue to face internal threats from Boko Haram, which pledged loyalty to the Islamic State in Iraq and the Levant (ISIL) in March 2015. Despite losing territory in 2015, Boko Haram will probably remain a threat to Nigeria throughout 2016 and will continue its terror campaign within the country and in neighboring Cameroon, Niger, and Chad.

# **LATIN AMERICA AND CARIBBEAN**

## **Central America**

Strong family ties to the United States—as well as gang violence, a lack of jobs, and a worsening drought in Central America's northern tier—will sustain high rates of migration to the United States in 2016. Weak institutions, divided legislatures, low levels of tax collection, and high debts will constrain efforts to

improve rule of law, tackle corruption, and alleviate poverty. Homicide rates in the region remain among the highest in the world and spiked in El Salvador to levels not seen since the country's civil war from 1979 to 1992. The people hardest hit by the drought include most of the region's subsistence farmers, who constitute 25 to 40 percent of the population in Guatemala and Honduras. The prolonged drought will probably affect 3.5 million people in the region in 2016.

### **Cuba**

Cuban leaders will remain focused on preserving political control as they prepare for a probable presidential transition in 2018. Economic reforms to reduce the state role in the economy and promote private economic activity will continue at a slow pace, in part because of probable resistance from senior leaders and government officials concerned that rapid changes might provoke popular unrest. Living standards will remain poor. Along with fears among the Cuban population that the United States will repeal the 1966 Cuban Adjustment Act, the statute allowing Cuban nationals to apply to become lawful permanent US residents, these trends sustain the increasing migration of undocumented Cubans. Migration is particularly acute across the US southwest border where 31,000 Cubans crossed in FY2015, a 76-percent increase over the prior year.

### **Venezuela**

The opposition alliance won a much-coveted majority in the December 2015 national assembly elections, setting the stage for a political showdown in 2016 between the legislative and executive branches. The opposition will seek to implement its policy agenda, which might include pursuing a presidential recall referendum. Economic issues will also figure prominently on the domestic agenda for 2016. Caracas will probably encounter fiscal pressures as it seeks to avoid a default on its sovereign debt in 2016; the economy is suffering from a severe recession that the IMF projects will cause it to contract by at least 8 percent in 2016. Venezuela's government has declined to release complete official figures on macroeconomic indicators, such as inflation and growth.

### **Brazil**

Brazil's investigation into corruption at state-controlled oil company Petrobras will probably continue through 2016. Scores of Petrobras officials, construction firm executives, and politicians have been jailed since the probe was launched in March 2014. Brazil lost its investment-grade rating in December 2015 after the second credit agency in three months downgraded the country's debt to junk status. Further damaging revelations from the probe might prolong political gridlock in Brazil. Meanwhile, preparations are underway in Brazil to address infrastructure, logistics, and security issues involved in hosting the 2016 Summer Olympics in Rio. Organizers are using past Olympics as models, cooperating with foreign governments, and building upon Brazil's experience organizing a large and sustained security posture such as when it hosted the World Cup in 2014.

# EXHIBIT 11



# Foreign Economic Espionage in Cyberspace

2018



NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER



## Scope Note

This report is submitted in compliance with the National Defense Authorization Act for Fiscal Year 2015, Section 1637, which requires that the President annually submit to Congress a report on foreign economic espionage and industrial espionage in cyberspace during the 12-month period preceding the submission of the report.

### Definitions of Key Terms

---

For the purpose of this report, key terms were defined according to definitions provided in Section 1637 of the National Defense Authorization Act for Fiscal Year 2015.

***Economic or Industrial Espionage*** means (a) stealing a trade secret or proprietary information or appropriating, taking, carrying away, or concealing, or by fraud, artifice, or deception obtaining, a trade secret or proprietary information without the authorization of the owner of the trade secret or proprietary information; (b) copying, duplicating, downloading, uploading, destroying, transmitting, delivering, sending, communicating, or conveying a trade secret or proprietary information without the authorization of the owner of the trade secret or proprietary information; or (c) knowingly receiving, buying, or possessing a trade secret or proprietary information that has been stolen or appropriated, obtained, or converted without the authorization of the owner of the trade secret or proprietary information.

***Cyberspace*** means (a) the interdependent network of information technology infrastructures; and (b) includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

### Contributors

---

The National Counterintelligence and Security Center (NCSC) compiled this report, with close support from the Cyber Threat Intelligence Integration Center (CTIIC), and with input and coordination from many U.S. Government organizations, including the Central Intelligence Agency (CIA), Defense Cyber Crime Center (DC3), Defense Intelligence Agency (DIA), Defense Security Service (DSS), Department of Energy (DoE), Department of Defense (DoD), Department of Homeland Security (DHS), Department of State (DoS), Department of Treasury (Treasury), Federal Bureau of Investigation (FBI), National Cyber Investigative Joint Task Force (NCIJTF), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and Office of the Director of National Intelligence (ODNI).



## I. The Strategic Threat of Cyber Economic Espionage

Foreign economic and industrial espionage against the United States continues to represent a significant threat to America's prosperity, security, and competitive advantage. Cyberspace remains a preferred operational domain for a wide range of industrial espionage threat actors, from adversarial nation-states, to commercial enterprises operating under state influence, to sponsored activities conducted by proxy hacker groups. Next-generation technologies such as Artificial Intelligence (AI) and the Internet-of-Things (IoT) will introduce new vulnerabilities to U.S. networks for which the cybersecurity community remains largely unprepared. Building an effective response demands understanding economic espionage as a worldwide, multi-vector threat to the integrity of the U.S. economy and global trade.

The United States remains a global center for research, development, and innovation across multiple high-technology sectors. Federal research institutions, universities, and corporations are regularly targeted by online actors seeking all manner of proprietary information and the overall long-term trend remains worrisome.

While next generation technologies will introduce a range of qualitative advances in data storage, analytics, and computational capacity, they also present potential vulnerabilities for which the cybersecurity community remains largely unprepared. The solidification of cloud computing over the past decade as a global information industry standard, coupled with the deployment of technologies such as AI and IoT, will introduce unforeseen vulnerabilities to U.S. networks.

- **Cloud networks and IoT infrastructure are rapidly expanding the global online operational space.** Threat actors have already demonstrated how cloud can be used as a platform for cyber exploitation. As IoT and AI applications expand to empower everything from "smart homes" to "smart cities", billions of potentially unsecured network nodes will create an incalculably larger exploitation space for cyber threat actors.
- **Lack of industry standardization during this pivotal first-generation deployment period will likely hamper the development of comprehensive security solutions in the near-term.**
- **Building an effective response demands understanding economic espionage as a worldwide, multi-vector threat to the integrity of both the U.S. economy and global trade.** Whereas cyberspace is a preferred operational domain for economic espionage, it is but one of many. Sophisticated threat actors, such as adversarial nation-states, combine cyber exploitation with supply chain operations, human recruitment, and the acquisition of knowledge by foreign students in U.S. universities, as part of a strategic technology acquisition program.





OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE



# EXHIBIT 12

S. HRG. 115-278

# OPEN HEARING ON WORLDWIDE THREATS

---

HEARING  
BEFORE THE  
SELECT COMMITTEE ON INTELLIGENCE  
OF THE  
UNITED STATES SENATE  
ONE HUNDRED FIFTEENTH CONGRESS  
SECOND SESSION

---

TUESDAY, FEBRUARY 13, 2018

---

Printed for the use of the Select Committee on Intelligence



Available via the World Wide Web: <http://www.govinfo.gov>

---

U.S. GOVERNMENT PUBLISHING OFFICE

28-947 PDF

WASHINGTON : 2018

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

RICHARD BURR, North Carolina, *Chairman*  
MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho  
MARCO RUBIO, Florida  
SUSAN COLLINS, Maine  
ROY BLUNT, Missouri  
JAMES LANKFORD, Oklahoma  
TOM COTTON, Arkansas  
JOHN CORNYN, Texas

DIANNE FEINSTEIN, California  
RON WYDEN, Oregon  
MARTIN HEINRICH, New Mexico  
ANGUS KING, Maine  
JOE MANCHIN, West Virginia  
KAMALA HARRIS, California

MITCH McCONNELL, Kentucky, *Ex Officio*  
CHUCK SCHUMER, New York, *Ex Officio*  
JOHN McCain, Arizona, *Ex Officio*  
JACK REED, Rhode Island, *Ex Officio*

---

CHRIS JOYNER, *Staff Director*  
MICHAEL CASEY, *Minority Staff Director*  
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

FEBRUARY 13, 2018

OPENING STATEMENTS

Burr, Hon. Richard, Chairman, a U.S. Senator from North Carolina .....	1
Mark R. Warner, Vice Chairman, a U.S. Senator from Virginia .....	3

WITNESS

Daniel R. Coats, Director of National Intelligence; Accompanied by: Michael Pompeo, Director of the Central Intelligence Agency; Admiral Michael Rogers, Director of the National Security Agency; Lieutenant General Robert Ashley, Director of the Defense Intelligence Agency; Chris Wray, Director of the Federal Bureau of Investigation; and Robert Cardillo, Director of the National Geospatial-Intelligence Agency .....	5
Prepared statement .....	12

SUPPLEMENTAL MATERIAL

Responses of Daniel R. Coats to Questions for the Record .....	78
--	----





## OPEN HEARING ON WORLDWIDE THREATS

---

TUESDAY, FEBRUARY 13, 2018

U.S. SENATE,  
SELECT COMMITTEE ON INTELLIGENCE,  
*Washington, DC.*

The Committee met, pursuant to notice, at 9:35 a.m. in Room SH-216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Present: Burr (presiding), Warner, Risch, Rubio, Collins, Blunt, Lankford, Cotton, Cornyn, Feinstein, Wyden, Heinrich, King, Manchin, Harris, and Reed.

### OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman BURR. I'd like to call this hearing on worldwide threats to order, and I'd like to welcome our distinguished witnesses today:

Director of National Intelligence Dan Coats;  
Director of the Central Intelligence Agency Mike Pompeo;  
Director of the Defense Intelligence Agency General Robert Ashley;  
Director of the Federal Bureau of Investigation Chris Wray;  
Director of the National Security Agency, Admiral Mike Rogers;  
And Director of the Geospatial Intelligence Agency Robert Cardillo.

We've got a long day in front of us and I thank all of you for being here. I know how forward you look to this one occasion on an annual basis. Since 1995, this Committee has met in open forum to discuss the security threats facing the United States of America. This has never been, nor will it ever be, a comfortable conversation to have.

The threats this country face are complex, evolving, and without easy answers. They exist in multiple domains. They're asymmetrical and they're conventional. They can be launched from across the ocean or be planned in the heart of our homeland. Nonetheless, this conversation serves a vital purpose and it's essential that it takes place in the public square, with as much detail and candor as is possible.

In my view, that is the true value and public service of this hearing. It provides the American people with insight that they just don't normally get. Those insights are about the spectrum of threats we're up against as a Nation. But, importantly, those insights are also about the work that the intelligence community does to push back on those threats. This is work that is both time-

and labor-intensive. It can be frustrating, heartbreaking, and dangerous. It's often thankless, but because of the tireless dedication and patriotism of men and women who make up our intelligence community, it gets done on behalf of the American people every single day.

To this point, I encourage all the witnesses this morning to not only address the threats to our Nation, but to talk about what their organizations are doing to help secure this country and, to the degree they can in an unclassified setting.

Director Coats, your testimony for the record ties together the expertise, capabilities, and wisdom of the entire intelligence community. I encourage everyone to familiarize themselves with its contents. It's lengthy and it's detailed, and it's a testament to the broad range of talents our IC brings to the table. It's also a compelling reminder of why this country invests so substantially in its intelligence apparatus.

Director Pompeo, when we held this hearing last year I invited you to share your assessments of things on the Korean Peninsula. I'm going to ask you again for your insights on the state of North Korea's nuclear and missile program and, importantly, what's going on politically with North Korea's leadership. Perhaps you can help us differentiate between a genuine effort to reconcile with South Korea and an opportunistic attempt to drive a wedge between Washington and Seoul.

General Ashley, the work just never seems to end for our Defense Department. I would value your latest assessment of the battlefield situations in Syria and Afghanistan. Last week we had U.S. advisors and Kurdish allies come under fire in eastern Syria. This prompted a retaliatory strike that killed dozens of pro-regime forces.

In Afghanistan, a string of terrorist attacks in Kabul left 150 dead last month, suggesting to me that, after 16 years of war, the insurgency is nowhere near folding and the government remains hard-pressed to provide the security needed for its own people. I'd particularly value your unvarnished appraisal of where progress is being made in Afghanistan and where it's not.

Admiral Rogers, cyber is clearly the most challenging threat vector this country faces. It's also one of the most concerning, given how many aspects of our daily lives in the United States can be disrupted by a well-planned, well-executed cyber-attack. I'd appreciate your assessment of how well we're doing when it comes to protecting the Nation's most critical computer networks. From the systems that guide our military to the networks that ensure the Nation's energy supply, they are all essential to the functionality of a modern America, and I fear that they're increasingly vulnerable to state and non-state actors.

Director Wray, I'm keenly interested in hearing your assessment of the threat posed by the spread of foreign technology in the United States. This Committee has worked diligently to sound the alarm bells when it comes to the counterintelligence and information security risks that come prepackaged with the goods and services of certain overseas vendors.

The focus of my concern today is China, and specifically Chinese telecom, like Huawei and ZTE, that are widely understood to have

extraordinary ties to the Chinese government. I hope you'll share your thoughts on this, and I also ask you to provide your insights into how foreign commercial investments and acquisitions are jeopardizing the Nation's most sensitive technologies.

Lastly, I'd like to spend a moment on the counterintelligence threat to our national academic, research, and laboratory construct. What's the scale of the problem and what's the FBI doing to fight it?

Finally, Director Cardillo, we've come to associate NGA with the modernization of the intelligence community. The adversaries of this country are investing in innovating faster and with fewer constraints than we have. The threats we face are multidimensional, decentralized, and global. NGA has played an essential role in pushing the envelope with new ways of tackling problems, like having more data than you can feasibly analyze.

As the IC edges closer to automation, machine learning, and eventually artificial intelligence, the computer learning and computer vision work at NGA will be a bridge to help us get there. I look forward to your thoughts on what's next at NGA and how the intelligence community as a whole can make better use of innovation and technology to advance intelligence disciplines that have not changed much in the past 60 years. Our adversaries aren't going to wait for us to catch up.

I'll close there because we have a lot to get to, but I want to thank you and, more importantly, I want to thank those who are not here with you, those who carry out the lion's share of the work on behalf of the American people, the intelligence community. The folks you represent are important to this Committee. We can't do our oversight without the work they perform.

Before turning to the distinguished Vice Chairman, I'd like to highlight for my colleagues: We will reconvene at 2:30 this afternoon in a closed session to hear from the same witnesses in a classified setting. I would ask Members to please reserve anything that remotely gets into a classified question for the afternoon session.

With that, Vice Chairman.

**OPENING STATEMENT OF HON. MARK R. WARNER, VICE  
CHAIRMAN, A U.S. SENATOR FROM VIRGINIA**

Vice Chairman WARNER. Thank you, Mr. Chairman, and let me also welcome all of you here and echo the Chairman's comments. Thank you all for your service and we hope you will convey back to all the brave men and women who work for you, that this Committee will always have your back.

I think this open hearing comes at an extraordinarily important time. Our Nation's intelligence agencies stand at the forefront of our defense against continuing threats from terrorist groups, extremist ideology, rogue regimes, nuclear proliferation, and regional instability.

We all know—and we discussed this at length—in recent years we've also seen the rise of nations who view themselves at least as competitors, if not as adversaries, of the United States. They've begun to use, utilize, new asymmetric weapons to undercut our democratic institutions, to steal our most sensitive intellectual property.

Let me start with Russia. Obviously, certain questions remain with respect to the true extent of the Russian interference in the 2016 elections, and we'll continue to work through them in a bipartisan way on this Committee. However, I think you'll find a broad bipartisan consensus on this Committee on a number of critical issues:

First, that Russia engaged in a coordinated attack to undermine our democracy;

Second, that effort included targeting of State and local elections, electoral activities, in 21 states;

And third, the Russian effort, in a new area, utilized our social media platforms to push and spread misinformation at an unprecedented scale.

Now, we've had more than a year to get our act together and address the threat posed by Russia and implement a strategy to deter further attacks. But I believe, unfortunately, we still don't have a comprehensive plan.

Two weeks ago, Director Pompeo publicly stated that he had every expectation that Russia will try to influence our upcoming elections. Secretary of State Tillerson just last week said that we're already seeing Russian efforts to meddle in the 2018 elections. But I believe, in many ways, we're no better prepared than we were in 2016. Make no mistake, this threat did not begin in 2016, and it certainly didn't end with the election. What we are seeing is a continuous assault by Russia to target and undermine our democratic institutions, and they're going to keep coming at us.

Despite all this, the President, inconveniently, continues to deny the threat posed by Russia. He didn't increase sanctions on Russia when he had a chance to do so. He hasn't even tweeted a single concern.

This threat I believe demands a whole-of-government response, and that response needs to start with leadership at the top.

At the same time, other threats to our institutions come from right here at home. There have been some, aided and abetted by Russian internet bots and trolls, who've attacked the basic integrity of the FBI and the Justice Department. This is a dangerous trend. This campaign of innuendo and misinformation should alarm all of us, regardless of our partisan affiliation.

In addition to this ongoing threat from Russia, I'm concerned that China has developed an all-of-society, not just all-of-government, but all-of-society, approach to gain access to our sensitive technologies and intellectual property. I'm paying a great deal of attention to the rise of China's tech sector. In particular, I'm worried about the close relationship between the Chinese government and Chinese technology firms, particularly in the area of commercialization of our surveillance technology and efforts to shape telecommunication equipment markets.

I want to ensure that the IC is tracking the direction that China's tech giants are heading, and especially the extent to which they are beholden to the Chinese government. In recent years we've seen major technology firms whose rise is attributed in part to their illicit access to U.S. technology and IP. These companies now represent some of the leading market players globally. Most Americans have not heard of all of these companies, but as they

enter Western economic markets we want to ensure that they play by the rules. We need to make sure that this is not a new way for China to gain access to sensitive technology.

There are a number of other concerns I hope to raise both in the hearing this morning and in the closed hearing this afternoon. Let me just briefly mention two. First, how is the IC poised to track foreign influence that relies on social media and misinformation? Just last week, the Chairman and I had a good management with our UK parliamentary colleagues investigating this issue. Russian trolls and bots continue to push divisive content both in the United States and against all our allies in Europe, not only the UK, but, as we talked before, France, Germany, Netherlands. We also heard recent indications of Russian activities in Mexico. The IC needs to stay on top of this issue and I am worried that we don't have a clear line of assignment.

Let me also raise another issue. I believe we need to do more to reform the broken security clearance system, which GAO recently placed on its list of high-risk government programs in need of reform. We've seen close to 700,000 folks now waiting in line, folks that need to serve our country, whether in government or in the private sector, who have been just waiting way too long to get their security clearances. It's obviously hampering your recruitment and retention, and it's costing us millions of dollars in inefficiency.

Again, thank you to all of you for your service. Please convey our best wishes to the men and women who work with you, and I look forward to our hearing.

Thank you, Mr. Chairman.

Chairman BURR. Thank you, Vice Chairman.

I'm going to recognize Director Coats and he is the only one who will give official testimony. All members of the panel are open for questions. I will recognize our Members by order of seniority for up to five minutes.

With that, Director Coats, the floor is yours.

**STATEMENT OF DANIEL R. COATS, DIRECTOR OF NATIONAL INTELLIGENCE; ACCOMPANIED BY: MICHAEL POMPEO, DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY; ADMIRAL MICHAEL ROGERS, DIRECTOR OF THE NATIONAL SECURITY AGENCY; LIEUTENANT GENERAL ROBERT ASHLEY, DIRECTOR OF THE DEFENSE INTELLIGENCE AGENCY; CHRIS WRAY, DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION; AND ROBERT CARDILLO, DIRECTOR OF THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY**

Director COATS. Mr. Chairman, thank you. I want to start by apologizing for my raspy voice. I've been fighting through some of the crud that's going around, that several of us have endured. I may have to clear my throat a few times, which I apologize for.

But it strikes me, listening to your opening remarks and the Vice Chairman's opening remarks that we have continued to have a very interactive presence with this Committee. The issues that you and the Vice Chairman have raised and that others will raise are issues that we talk about continuously with you, and we want to continue to work with you carefully by both sides of the aisle here,

as we go forward looking at what the intelligence community can provide for this Committee and the issues that we find in common.

Vice Chairman Warner, Members of the Committee: We thank you for the opportunity to be with you here today. There have been some changes on the panel since we were here last year. This will be Admiral Rogers' last visit before this Committee on the threat assessment issue. He deeply regrets not having to come before you in the future years, as he's enjoyed this process so very much.

Chairman BURR. We're considering an emeritus status so that he can be annually invited back.

[Laughter.]

Director COATS. We have two new members, Director Wray and General Ashley, who have been looking forward to this day, I'm sure, with great anticipation.

I say all that because what you are looking at here is a team, a team that works together in terms of how we provide the American people, Congress, and policymakers with the intelligence that they need. So it's an honor for us to be here, and I think this team reflects the hard work of the intelligence community in their testimonies and their answers to questions today.

Before I begin the sobering portion of my remarks, let me take a moment to acknowledge a positive development for the intelligence community and express our thanks to Members of this Committee for their support in the renewing of the authorities in the recent 702 authorization. This is, as we have told you, our most important legislative issue because it is our most important collection issue against foreign terrorists and threats to America, and we appreciate the work that the Committee has done and others have done, and particularly this team has done, in reaching that goal.

As you will hear during these remarks, we face a complex, volatile, and challenging threat environment. The risk of inter-state conflict is higher than at any time since the end of the Cold War, all the more alarming because of the growing development and use of weapons of mass destruction by state and non-state actors.

Our adversaries as well as other malign actors are using cyber and other instruments of power to shape societies and markets, international rules and institutions, and international hot spots to their advantage. We have entered a period that can best be described as a race for technological superiority against our adversaries, who seek to sow division in the United States and weaken U.S. leadership, and non-state actors, including terrorists and criminal groups, are exploiting weak state capacity in Africa, the Middle East, Asia, and Latin America, causing instability and violence both within states and among states.

In the interest of saving time for your questions, I will not cover every topic in my opening remarks. I think that will be a relief to the Committee. We are submitting a written statement, however, for the record with additional details.

Let me turn to global threats, and I'd like to start with the cyber threat, which is one of my greatest concerns and top priorities. Frankly, the United States is under attack, under attack by entities that are using cyber to penetrate virtually every major action that takes place in the United States. From U.S. businesses to the



Federal Government to State and local governments, the United States is threatened by cyber-attacks every day.

While Russia, China, Iran, and North Korea pose the greatest cyber threats, other nation-states, terrorist organizations, transnational criminal organizations, and ever more technically capable groups and individuals use cyber operations to achieve strategic and malign objectives. Some of these actors, including Russia, are likely to pursue even more aggressive cyber-attacks with the intent of degrading our democratic values and weakening our alliances. Persistent and disruptive cyber operations will continue against the United States and our European allies, using elections as opportunities to undermine democracy, sow discord, and undermine our values.

Chinese cyber espionage and cyber-attack capabilities will continue to support China's national security and economic priorities. Iran will try to penetrate U.S. and allied networks for espionage and lay the groundwork for future cyber-attacks. And North Korea will continue to use cyber operations to raise funds, launch attacks, and gather intelligence against the United States. Terrorists will use the internet to raise funds and promote their malign messages. Criminals will exploit cyber tools to finance their operations.

My next topic for you is weapons of mass destruction, WMD. Overall, state efforts to modernize, develop, or acquire WMD, their delivery systems, or the underlying technologies constitute a major threat to the United States and to our allies. North Korea will be the most volatile and confrontational WMD threat in the coming year. In addition to its ballistic missile tests and growing number of nuclear warheads for these missiles, North Korea will continue its longstanding chemical and biological warfare programs.

Russia will remain the most capable WMD power and is expanding its nuclear weapon capabilities. China will continue to expand its weapons of mass destruction options and diversify its nuclear arsenal. Iran's implementation of the Joint Comprehensive Plan of Action, the JCPOA, has extended the time it would take to develop a nuclear weapon from several months to about a year, provided Iran continues to adhere to the deal's major provisions.

Pakistan is developing new types of nuclear weapons, including short-range tactical weapons. And state and non-state actors, including the Syrian regime and ISIS, the remnants of ISIS in Syria, continue to possess and, in some cases, have used chemical weapons in Syria and Iraq, and we continue to be concerned about some of these actors' pursuit of biological weapons.

Turning now to terrorism, the terrorism threat is pronounced and spans the sectarian spectrum from ISIS and Al-Qaeda to Lebanese Hezbollah and other affiliated terrorist organizations, as well as the state-sponsored activities of Iran. U.S.-based home-grown violent extremists, including inspired and self-radicalized individuals, represent the primary and most different to detect Sunni terrorism threat in the United States.

ISIS' claim to having a functioning caliphate that governs populations is all but thwarted. However, ISIS remains a threat and will likely focus on regrouping in request and Syria, particularly in ungoverned portions of those countries, enhancing its global presence, championing its cause, planning international attacks, and

encouraging members and sympathizers to attack their home countries.

Meanwhile, Al-Qaeda almost certainly will remain a major actor in global terrorism as it continues to prioritize a long-term approach and the organization remains intent on attacking the United States and U.S. interests abroad.

Now, moving on, as if we don't have enough threats here on Earth, we need to look to the heavens: threats in space. The global expansion of the space industry will extend space-enabled capabilities and situational awareness to nation-state and commercial space actors in the coming years. Russia and China will continue to expand to space-based reconnaissance, communications, and navigation systems in terms of numbers of satellites, breadth of capability, and applications for use. Both Russian and Chinese counter-space weapon will mature over the next few years, as each country pursues anti-satellite weapons as a means to reduce U.S. and allied military effectiveness and perceptions of U.S. military advantage in space.

The final functional topic is transnational organized crime, which poses a growing threat to U.S. and allied interests. These criminal groups will supply the dominant share of illicit drugs, fueling record mortality rates among our population. They will continue to traffic in human life. They will deplete national resources and siphon money from governments and the global economy.

I'd like to briefly go around the world on regional topics, starting with East Asia. You know, if you went out and hired a private plane and launched from Los Angeles and went around the world and stopped at every hot spot in this world, you would make multiple dozens of stops. That's the kind of threat that we face.

But let me start with East Asia. North Korea continues to pose an ever more increasing threat to the United States and its interests. Pyongyang has repeatedly stated that it does not intend to negotiate its nuclear weapons and missiles away, because the regime views nuclear weapons as critical to its security. Kim also probably sees nuclear ICBMs as leverage to achieve his long-term strategic ambition to end Seoul's alliance with Washington and to eventually dominate the peninsula.

In the wake of its ICBM tests last year, we expect to see North Korea press ahead with additional missile tests this year, and its foreign minister has threatened an atmospheric nuclear test over the Pacific. Pyongyang is committed to fielding a long-range nuclear-armored missile capable of posing a direct threat to the United States, and modest improvements in North Korea's conventional capabilities will continue to pose an ever greater threat to South Korea, Japan, and U.S. targets in those countries.

China will increasingly seek to expand its regional influence and shape even this and outcomes globally. It will take a firm stance on its claims to the East China Sea and South China Sea, its relations with Taiwan and its regional economic engagement. China also intends to use its "One Belt, One Road" initiative to increase its reach to geostrategic locations across Eurasia, Africa, and the Pacific.

From East Asia we head to South Asia. In Afghanistan, Kabul continues to bear the brunt of the Taliban-led insurgency, as dem-

onstrated by recent attacks in the city. Afghan National Security Forces face unsteady performance, but, with coalition support, probably will maintain control of most major population centers.

Complicating the Afghanistan situation, however, is our assessment that Pakistan-based militant groups continue to take advantage of their safe havens to conduct attacks in India and Afghanistan, including U.S. interests therein.

Pakistani military leaders continue to walk a delicate line. Ongoing Pakistani military operations against the Taliban and associated groups probably reflect the desire to appear more proactive and responsive to our requests for more actions against these groups. However, the actions taken thus far do not reflect a significant escalation of the pressure against these groups and are unlikely to have a lasting effect.

In the last month, the Administration has designed—excuse me—designated eight militants affiliated with the Taliban, Haqqani Network, and other Pakistani militant groups, and we assess that Pakistan will maintain ties to these militants while restricting counter-terrorism cooperation with the United States.

Next is Russia, where President Putin will continue to rely on assertive foreign policies to shape outcomes beyond Russia's borders. Putin will resort to more authoritarian tactics to maintain control amid challenges to his rule.

With respect to Russia influence efforts, let me be clear: The Russians utilize this tool because it's relatively cheap, it's low-risk, it offers what they perceive as plausible deniability, and it's proven to be effective at sowing division. We expect Russia to continue using propaganda, social media, false flag personas, sympathetic spokesmen, and other means to influence, to try to build on its wide range of operations and exacerbate social and political fissures in the United States. There should be no doubt that Russia perceives its past efforts have been successful and views the 2018 U.S. midterm elections as a potential target for Russian influence operations.

From Russia I'll turn to the Middle East and North Africa. This region will be characterized by political turmoil, economic fragility, and civil and proxy wars in the coming year. Iran will remain the most prominent state sponsor of terrorism and adversary in the Middle East, especially in Iraq, Syria, and Yemen. Iran will seek to expand its regional influence and will exploit the fight against ISIS to solidify partnerships and translate battlefield gains into political, security, and economic agreements.

We also assess that Iran will continue to develop military capabilities that threaten U.S. forces and U.S. allies in the region. For example, Iran has the largest ballistic missile force in the Middle East. The Islamic Revolutionary Guard Corps navy and its unsafe and unprofessional interactions pose a risk to U.S. naval and allied naval operations in the Persian Gulf. And Lebanese Hezbollah, with the support of Iran, has deployed thousands of fighters to Syria and provides direction to other militant and terrorist groups, all fomenting regional instability. Iran's provocative and assertive behavior, as we saw most recently this past weekend in northern Israel, increases the potential for escalation.

Turkey will seek to thwart Kurdish ambitions in the Middle East and the ongoing Turkish incursion into northern Syria is complicating ongoing counter-ISIS activities in the region and increases the risk to U.S. forces located in the area.

Syria will face unrest and fighting through 2018, even as Damascus recaptures urban areas and violence decreases in some areas.

Iraq is likely to face a lengthy period of political turmoil and conflict. The social and political challenges that gave rise to ISIS remain and Iran has exploited those challenges to deepen its influence in Iraq's military and security elements, diplomatic and political arms.

The war in Yemen between the Iranian-backed Houthis and the Saudi-led coalition is likely to continue and will worsen the already tragic humanitarian crisis for 70 percent of the population of about 20 million people in need of assistance. The situation in Yemen is emblematic of a far larger problem: The number of people displaced by conflict around the world is the highest that it's been since the end of World War II.

Turning to Europe, where I want to draw your attention to two significant developments that are likely to continue to impact European politics and foreign policy in the coming year, let me state first: The continent's center of gravity appears to be shifting to France, where President Macron has taken a more assertive role in addressing European global challenges. The results of the recent German election I think enforce that assessment.

Second, recent efforts by some governments in Central and Eastern Europe to undermine judicial independence and parliamentary oversight and increase government control over public media are weakening the rule of law. These steps could presage further democratic decline and offer opportunity for Chinese and Russian influence.

There are many more topics I could discuss. I haven't even gotten to the Western Hemisphere or Africa. But I would like to close with a discussion of one additional threat, this one internal and somewhat personal. I am concerned that our increasing fractious political process, particularly with respect to Federal spending, is threatening our ability to properly defend our Nation, both in the short term and especially in the long term. The failure to address our long-term fiscal situation has increased the national debt to over \$20 trillion and growing. This situation is unsustainable, as I think we all know, and represents a dire threat to our economic and national security.

Former Chairman of the Joint Chiefs of Staff Mike Mullen first identified the national debt as the greatest threat to our national security. Since then he has been joined by numerous respected national security leaders of both parties, including former Secretaries of State Madeleine Albright and Henry Kissinger, as well as former Defense Secretaries Bob Gates and Leon Panetta; and our current Defense Secretary Jim Mattis agrees with this assessment.

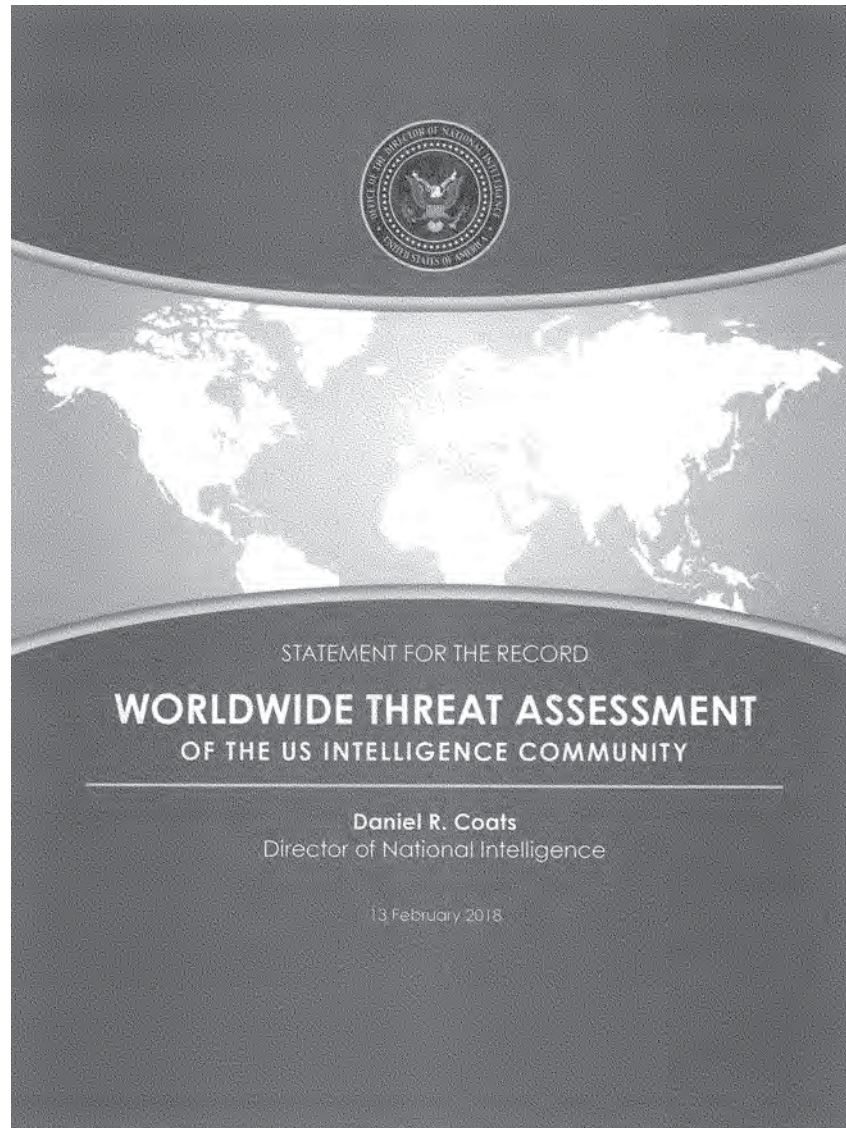
Many of you know I have spent a lot of time in my last term in the Senate working on this issue and, unfortunately, the problem continues to grow. So I would urge all of us to recognize the need to address this challenge and to take action as soon as possible, be-

fore a fiscal crisis occurs that truly undermines our ability to ensure our national security.

With that, I and the rest of the panel are happy to take your questions. We appreciate the opportunity to be with you today. Thank you, Mr. Chairman.

[The prepared statement of Director Coats follows:]







13

## **STATEMENT FOR THE RECORD**

### **WORLDWIDE THREAT ASSESSMENT of the US INTELLIGENCE COMMUNITY**

February 13, 2018

#### **INTRODUCTION**

Chairman Burr, Vice Chairman Warner, Members of the Committee, thank you for the invitation to offer the United States Intelligence Community's 2018 assessment of threats to US national security. My statement reflects the collective insights of the Intelligence Community's extraordinary women and men, whom I am privileged and honored to lead. We in the Intelligence Community are committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

The order of the topics presented in this statement does not necessarily indicate the relative importance or magnitude of the threat in the view of the Intelligence Community.

Information available as of 8 February 2018 was used in the preparation of this assessment.

## CONTENTS

INTRODUCTION .....	2
CONTENTS .....	3
FOREWORD .....	4
GLOBAL THREATS .....	5
CYBER THREATS .....	5
WEAPONS OF MASS DESTRUCTION AND PROLIFERATION .....	7
TERRORISM .....	9
COUNTERINTELLIGENCE AND FOREIGN DENIAL AND DECEPTION .....	11
EMERGING AND DISRUPTIVE TECHNOLOGY .....	12
TECHNOLOGY ACQUISITIONS AND STRATEGIC ECONOMIC COMPETITION .....	12
SPACE AND COUNTERSPACE .....	13
TRANSNATIONAL ORGANIZED CRIME .....	13
ECONOMICS AND ENERGY .....	15
HUMAN SECURITY .....	16
REGIONAL THREATS .....	18
EAST ASIA .....	18
MIDDLE EAST AND NORTH AFRICA .....	19
SOUTH ASIA .....	22
RUSSIA AND EURASIA .....	23
EUROPE .....	25
AFRICA .....	26
THE WESTERN HEMISPHERE .....	27

## FOREWORD

*Competition among countries will increase in the coming year as major powers and regional aggressors exploit complex global trends while adjusting to new priorities in US foreign policy. The risk of interstate conflict, including among great powers, is higher than at any time since the end of the Cold War. The most immediate threats of regional interstate conflict in the next year come from North Korea and from Saudi-Iranian use of proxies in their rivalry. At the same time, the threat of state and nonstate use of weapons of mass destruction will continue to grow.*

- Adversaries and malign actors will use all instruments of national power—including information and cyber means—to shape societies and markets, international rules and institutions, and international hot spots to their advantage.
- China and Russia will seek spheres of influence and to check US appeal and influence in their regions. Meanwhile, US allies' and partners' uncertainty about the willingness and capability of the United States to maintain its international commitments may drive them to consider reorienting their policies, particularly regarding trade, away from Washington.
- Forces for geopolitical order and stability will continue to fray, as will the rules-based international order. New alignments and informal networks—outside traditional power blocs and national governments—will increasingly strain international cooperation.

*Tension within many countries will rise, and the threat from Sunni violent extremist groups will evolve as they recoup after battlefield losses in the Middle East.*

- Slow economic growth and technology-induced disruptions in job markets are fueling populism within advanced industrial countries and the very nationalism that contributes to tension among countries.
- Developing countries in Latin America and Sub-Saharan Africa face economic challenges, and many states struggle with reforms to tamp down corruption. Terrorists and criminal groups will continue to exploit weak state capacity in Africa, the Middle East, and Asia.
- Challenges from urbanization and migration will persist, while the effects of air pollution, inadequate water, and climate change on human health and livelihood will become more noticeable. Domestic policy responses to such issues will become more difficult—especially for democracies—as publics become less trusting of authoritative information sources.

## GLOBAL THREATS

### CYBER THREATS

*The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits. The risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war.*

- In 2016 and 2017, state-sponsored cyber attacks against Ukraine and Saudi Arabia targeted multiple sectors across critical infrastructure, government, and commercial networks.
- Ransomware and malware attacks have spread globally, disrupting global shipping and production lines of US companies. The availability of criminal and commercial malware is creating opportunities for new actors to launch cyber operations.
- We assess that concerns about US retaliation and still developing adversary capabilities will mitigate the probability of attacks aimed at causing major disruptions of US critical infrastructure, but we remain concerned by the increasingly damaging effects of cyber operations and the apparent acceptance by adversaries of collateral damage.

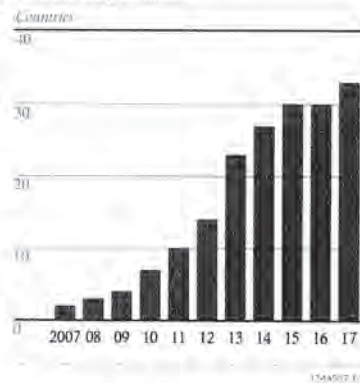
### Adversaries and Malign Actors Poised for Aggression

*Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year.*

These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations. Nonstate actors will continue to use cyber operations for financial crime and to enable propaganda and messaging.

- The use of cyber attacks as a foreign policy tool outside of military conflict has been mostly limited to sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing more aggressive cyber attacks that pose growing threats to the United States and US partners.

Countries With Cyber Attack Capabilities





*Russia. We expect that Russia will conduct bolder and more disruptive cyber operations during the next year, most likely using new capabilities against Ukraine.* The Russian Government is likely to build on the wide range of operations it is already conducting, including disruption of Ukrainian energy-distribution networks, hack-and-leak influence operations, distributed denial-of-service attacks, and false flag operations. In the next year, Russian intelligence and security services will continue to probe US and allied critical infrastructures, as well as target the United States, NATO, and allies for insights into US policy.

*China. China will continue to use cyber espionage and bolster cyber attack capabilities to support national security priorities.* The IC and private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral US-China cyber commitments of September 2015. Most detected Chinese cyber operations against US private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide. China since 2015 has been advancing its cyber attack capabilities by integrating its military cyber attack and espionage resources in the Strategic Support Force, which it established in 2015.

*Iran. We assess that Iran will continue working to penetrate US and Allied networks for espionage and to position itself for potential future cyber attacks, although its intelligence services primarily focus on Middle Eastern adversaries—especially Saudi Arabia and Israel.* Tehran probably views cyberattacks as a versatile tool to respond to perceived provocations, despite Iran's recent restraint from conducting cyber attacks on the United States or Western allies. Iran's cyber attacks against Saudi Arabia in late 2016 and early 2017 involved data deletion on dozens of networks across government and the private sector.

*North Korea. We expect the heavily sanctioned North Korea to use cyber operations to raise funds and to gather intelligence or launch attacks on South Korea and the United States.* Pyongyang probably has a number of techniques and tools it can use to achieve a range of offensive effects with little or no warning, including distributed denial of service attacks, data deletion, and deployment of ransomware.

- North Korean actors developed and launched the WannaCry ransomware in May 2017, judging from technical links to previously identified North Korean cyber tools, tradecraft, and operational infrastructure. We also assess that these actors conducted the cyber theft of \$81 million from the Bank of Bangladesh in 2016.

*Terrorists and Criminals. Terrorist groups will continue to use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations.* Given their current capabilities, cyber operations by terrorist groups mostly likely would result in personally identifiable information (PII) disclosures, website defacements, and denial-of-service attacks against poorly protected networks. Transnational criminals will continue to conduct for-profit cyber-enabled crimes, such as theft and extortion against US networks. We expect the line between criminal and nation-state activity to become increasingly blurred as states view cyber criminal tools as a relatively inexpensive and deniable means to enable their operations.

## WEAPONS OF MASS DESTRUCTION AND PROLIFERATION

*State efforts to modernize, develop, or acquire weapons of mass destruction (WMD), their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and its allies.* Both state and nonstate actors have already demonstrated the use of chemical weapons in Iraq and Syria. Biological and chemical materials and technologies—almost always dual-use—move easily in the globalized economy, as do personnel with the scientific expertise to design and use them for legitimate and illegitimate purposes. Information about the latest discoveries in the life sciences also diffuses rapidly around the globe, widening the accessibility of knowledge and tools for beneficial purposes and for potentially nefarious applications.

### Russia

Russia has developed a ground-launched cruise missile (GLCM) that the United States has declared is in violation of the Intermediate-Range Nuclear Forces (INF) Treaty. Despite Russia's ongoing development of other Treaty-compliant missiles with intermediate ranges, Moscow probably believes that the new GLCM provides sufficient military advantages to make it worth risking the political repercussions of violating the INF Treaty. In 2013, a senior Russian administration official stated publicly that the world had changed since the INF Treaty was signed in 1987. Other Russian officials have made statements complaining that the Treaty prohibits Russia, but not some of its neighbors, from developing and possessing ground-launched missiles with ranges between 500 and 5,500 kilometers.

### China

The Chinese People's Liberation Army (PLA) continues to modernize its nuclear missile force by adding more survivable road-mobile systems and enhancing its silo-based systems. This new generation of missiles is intended to ensure the viability of China's strategic deterrent by providing a second-strike capability. China also has tested a hypersonic glide vehicle. In addition, the PLA Navy continues to develop the JL-2 submarine-launched ballistic missile (SLBM) and might produce additional JIN-class nuclear-powered ballistic missile submarines. The JIN-class submarines—armed with JL-2 SLBMs—give the PLA Navy its first long-range, sea-based nuclear capability. The Chinese have also publicized their intent to form a triad by developing a nuclear-capable next-generation bomber.

### Iran and the Joint Comprehensive Plan of Action

Tehran's public statements suggest that it wants to preserve the Joint Comprehensive Plan of Action because it views the JCPOA as a means to remove sanctions while preserving some nuclear capabilities. Iran recognizes that the US Administration has concerns about the deal but expects the other participants—China, the EU, France, Germany, Russia, and the United Kingdom—to honor their commitments. Iran's implementation of the JCPOA has extended the amount of time Iran would need to produce enough fissile material for a nuclear weapon from a few months to about one year, provided Iran continues to adhere to the deal's major provisions. The JCPOA has also enhanced the transparency of Iran's nuclear activities, mainly by fostering improved access to Iranian nuclear facilities for the IAEA and its investigative authorities under the Additional Protocol to its Comprehensive Safeguards Agreement.



Iran's ballistic missile programs give it the potential to hold targets at risk across the region, and Tehran already has the largest inventory of ballistic missiles in the Middle East. Tehran's desire to deter the United States might drive it to field an ICBM. Progress on Iran's space program, such as the launch of the Simorgh SLV in July 2017, could shorten a pathway to an ICBM because space launch vehicles use similar technologies.

#### **North Korea**

*North Korea will be among the most volatile and confrontational WMD threats to the United States over the next year.* North Korea's history of exporting ballistic missile technology to several countries, including Iran and Syria, and its assistance during Syria's construction of a nuclear reactor—destroyed in 2007—illustrate its willingness to proliferate dangerous technologies.

In 2017 North Korea, for the second straight year, conducted a large number of ballistic missile tests, including its first ICBM tests. Pyongyang is committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States. It also conducted its sixth and highest yield nuclear test to date.

We assess that North Korea has a longstanding BW capability and biotechnology infrastructure that could support a BW program. We also assess that North Korea has a CW program and probably could employ these agents by modifying conventional munitions or with unconventional, targeted methods.

#### **Pakistan**

Pakistan continues to produce nuclear weapons and develop new types of nuclear weapons, including short-range tactical weapons, sea-based cruise missiles, air-launched cruise missiles, and longer-range ballistic missiles. These new types of nuclear weapons will introduce new risks for escalation dynamics and security in the region.

#### **Syria**

We assess that the Syrian regime used the nerve agent sarin in an attack against the opposition in Khan Shaykhun on 4 April 2017, in what is probably the largest chemical weapons attack since August 2013. We continue to assess that Syria has not declared all the elements of its chemical weapons program to the Chemical Weapons Convention (CWC) and that it has the capability to conduct further attacks. Despite the creation of a specialized team and years of work by the Organization for the Prohibition of Chemical Weapons (OPCW) to address gaps and inconsistencies in Syria's declaration, numerous issues remain unresolved. The OPCW-UN Joint Investigative Mechanism (JIM) has attributed the 4 April 2017 sarin attack and three chlorine attacks in 2014 and 2015 to the Syrian regime. Even after the attack on Khan Shaykhun, we have continued to observe allegations that the regime has used chemicals against the opposition.

#### **ISIS**

We assess that ISIS is also using chemicals as a means of warfare. The OPCW-UN JIM concluded that ISIS used sulfur mustard in two attacks in 2015 and 2016, and we assess that it has used chemical weapons in numerous other attacks in Iraq and Syria.

## TERRORISM

Sunni violent extremists—most notably ISIS and al-Qa'ida—pose continuing terrorist threats to US interests and partners worldwide, while US-based homegrown violent extremists (HVEs) will remain the most prevalent Sunni violent extremist threat in the United States. Iran and its strategic partner Lebanese Hizballah also pose a persistent threat to the United States and its partners worldwide.

### Sunni Violent Extremism

*Sunni violent extremists are still intent on attacking the US homeland and US interests overseas, but their attacks will be most frequent in or near conflict zones or against enemies that are more easily accessible.*

- Sunni violent extremist groups are geographically diverse; they are likely to exploit conflict zones in the Middle East, Africa, and Asia, where they can co-mingle terrorism and insurgency.
- ISIS and al-Qa'ida and their respective networks will be persistent threats, as will groups not subordinate to them, such as the Haqqani Taliban Network.

### Sunni Violent Extremists' Primary Operating Areas as of 2017



### ISIS

*Over the next year, we expect that ISIS is likely to focus on regrouping in Iraq and Syria, enhancing its global presence, championing its cause, planning international attacks, and encouraging its members and sympathizers to attack in their home countries. ISIS's claim of having a functioning caliphate that governs populations is all but thwarted.*

- ISIS core has started—and probably will maintain—a robust insurgency in Iraq and Syria as part of a long-term strategy to ultimately enable the reemergence of its so-called caliphate. This activity will challenge local CT efforts against the group and threaten US interests in the region.

- ISIS almost certainly will continue to give priority to transnational terrorist attacks. Its leadership probably assesses that, if ISIS-linked attacks continue to dominate public discourse, the group's narrative will be buoyed, it will be difficult for the counter-ISIS coalition to portray the group as defeated, and the coalition's will to fight will ultimately weaken.
- Outside Iraq and Syria, ISIS's goal of fostering interconnectivity and resiliency among its global branches and networks probably will result in local and, in some cases, regional attack plans.

#### **Al-Qa'ida**

*Al-Qa'ida almost certainly will remain a major actor in global terrorism because of the combined staying power of its five affiliates. The primary threat to US and Western interests from al-Qa'ida's global network through 2018 will be in or near affiliates' operating areas. Not all affiliates will have the intent and capability to pursue or inspire attacks in the US homeland or elsewhere in the West.*

- Al-Qa'ida's affiliates probably will continue to dedicate most of their resources to local activity, including participating in ongoing conflicts in Afghanistan, Somalia, Syria, and Yemen, as well as attacking regional actors and populations in other parts of Africa, Asia, and the Middle East.
- Al-Qa'ida leaders and affiliate media platforms almost certainly will call for followers to carry out attacks in the West, but their appeals probably will not create a spike in inspired attacks. The group's messaging since at least 2010 has produced few such attacks.

#### **Homegrown Violent Extremists**

*Homegrown violent extremists (HVEs) will remain the most prevalent and difficult-to-detect Sunni terrorist threat at home, despite a drop in the number of attacks in 2017. HVE attacks are likely to continue to occur with little or no warning because the perpetrators often strike soft targets and use simple tactics that do not require advanced skills or outside training.*

- HVEs almost certainly will continue to be inspired by a variety of sources, including terrorist propaganda as well as in response to perceived grievances related to US Government actions.

#### **Iran and Lebanese Hizballah**

Iran remains the most prominent state sponsor of terrorism, providing financial aid, advanced weapons and tactics, and direction to militant and terrorist groups across the Middle East and cultivating a network of operatives across the globe as a contingency to enable potential terrorist attacks.

Lebanese Hizballah has demonstrated its intent to foment regional instability by deploying thousands of fighters to Syria and by providing weapons, tactics, and direction to militant and terrorist groups. Hizballah probably also emphasizes its capability to attack US, Israeli, and Saudi Arabian interests.



## COUNTERINTELLIGENCE AND FOREIGN DENIAL AND DECEPTION

*The United States will face a complex global foreign intelligence threat environment in 2018. We assess that the leading state intelligence threats to US interests will continue to be Russia and China, based on their services' capabilities, intent, and broad operational scope.* Other states in the Near East, South Asia, East Asia, and Latin America will pose local and regional intelligence threats to US interests. For example, Iranian and Cuban intelligence and security services continue to view the United States as a primary threat.

Penetrating the US national decisionmaking apparatus and the Intelligence Community will remain primary objectives for numerous foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other areas will remain a persistent threat to US interests.

Nonstate entities, including international terrorists and transnational organized crime groups, are likely to continue to employ and improve their intelligence capabilities, including human, technical, and cyber means. As with state intelligence services, these nonstate entities recruit sources and perform physical and technical surveillance to facilitate their illicit activities and to avoid detection and capture.

Trusted insiders who disclose sensitive or classified US Government information without authorization will remain a significant threat in 2018 and beyond. The sophistication and availability of information technology that increases the scope and impact of unauthorized disclosures exacerbate this threat.

### Russia and Influence Campaigns

*Influence operations, especially through cyber means, will remain a significant threat to US interests as they are low-cost, relatively low-risk, and deniable ways to retaliate against adversaries, to shape foreign perceptions, and to influence populations.* Russia probably will be the most capable and aggressive source of this threat in 2018, although many countries and some nonstate actors are exploring ways to use influence operations, both domestically and abroad.

*We assess that the Russian intelligence services will continue their efforts to disseminate false information via Russian state-controlled media and covert online personas about US activities to encourage anti-US political views.* Moscow seeks to create wedges that reduce trust and confidence in democratic processes, degrade democratization efforts, weaken US partnerships with European allies, undermine Western sanctions, encourage anti-US political views, and counter efforts to bring Ukraine and other former Soviet states into European institutions.

- Foreign elections are critical inflection points that offer opportunities for Russia to advance its interests both overtly and covertly. The 2018 US mid-term elections are a potential target for Russian influence operations.
- At a minimum, we expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokespeople, and other means of influence to try to exacerbate social and political fissures in the United States.

## EMERGING AND DISRUPTIVE TECHNOLOGY

*New technologies and novel applications of existing technologies have the potential to disrupt labor markets and alter health, energy, and transportation systems.* We assess that technology developments—in the biotechnology and communications sectors, for example—are likely to outpace regulation, which could create international norms that are contrary to US interests and increase the likelihood of technology surprise. Emerging technology and new applications of existing technology will also allow our adversaries to more readily develop weapon systems that can strike farther, faster, and harder and challenge the United States in all warfare domains, including space.

- The widespread proliferation of artificial intelligence (AI)—the field of computer science encompassing systems that seek to imitate aspects of human cognition by learning and making decisions based on accumulated knowledge—is likely to prompt new national security concerns; existing machine learning technology, for example, could enable high degrees of automation in labor-intensive activities such as satellite imagery analysis and cyber defense. Increasingly capable AI tools, which are often enabled by large amounts of data, are also likely to present socioeconomic challenges, including impacts on employment and privacy.
- New biotechnologies are leading to improvements in agriculture, health care, and manufacturing. However, some applications of biotechnologies may lead to unintentional negative health effects, biological accidents, or deliberate misuse.
- The global shift to advanced information and communications technologies (ICT) will increasingly test US competitiveness because aspiring suppliers around the world will play a larger role in developing new technologies and products. These technologies include next-generation, or 5G, wireless technology; the internet of things; new financial technologies; and enabling AI and big data for predictive analysis. Differences in regulatory and policy approaches to ICT-related issues could impede growth and innovation globally and for US companies.
- Advanced materials could disrupt the economies of some commodities-dependent exporting countries while providing a competitive edge to developed and developing countries that create the capacity to produce and use the new materials. New materials, such as nanomaterials, are often developed faster than their health and environmental effects can be assessed. Advances in manufacturing, particularly the development of 3D printing, almost certainly will become even more accessible to a variety of state and nonstate actors and be used in ways contrary to our interests.

## TECHNOLOGY ACQUISITIONS AND STRATEGIC ECONOMIC COMPETITION

*Persistent trade imbalances, trade barriers, and a lack of market-friendly policies in some countries probably will continue to challenge US economic security. Some countries almost certainly will continue to acquire US intellectual property and propriety information illicitly to advance their own economic and national security objectives.*

- China, for example, has acquired proprietary technology and early-stage ideas through cyber-enabled means. At the same time, some actors use largely legitimate, legal transfers and



relationships to gain access to research fields, experts, and key enabling industrial processes that could, over time, erode America's long-term competitive advantages.

#### **SPACE AND COUNTERSPACE**

Continued global space industry expansion will further extend space-enabled capabilities and space situational awareness to nation-state, nonstate, and commercial space actors in the coming years, enabled by the increased availability of technology, private-sector investment, and growing international partnerships for shared production and operation. All actors will increasingly have access to space-derived information services, such as imagery, weather, communications, and positioning, navigation, and timing for intelligence, military, scientific, or business purposes. Foreign countries—particularly China and Russia—will continue to expand their space-based reconnaissance, communications, and navigation systems in terms of the numbers of satellites, the breadth of their capability, and the applications for use.

Both Russia and China continue to pursue antisatellite (ASAT) weapons as a means to reduce US and allied military effectiveness. Russia and China aim to have nondestructive and destructive counterspace weapons available for use during a potential future conflict. We assess that, if a future conflict were to occur involving Russia or China, either country would justify attacks against US and allied satellites as necessary to offset any perceived US military advantage derived from military, civil, or commercial space systems. Military reforms in both countries in the past few years indicate an increased focus on establishing operational forces designed to integrate attacks against space systems and services with military operations in other domains.

Russian and Chinese destructive ASAT weapons probably will reach initial operational capability in the next few years. China's PLA has formed military units and begun initial operational training with counterspace capabilities that it has been developing, such as ground-launched ASAT missiles. Russia probably has a similar class of system in development. Both countries are also advancing directed-energy weapons technologies for the purpose of fielding ASAT weapons that could blind or damage sensitive space-based optical sensors, such as those used for remote sensing or missile defense.

Of particular concern, Russia and China continue to launch "experimental" satellites that conduct sophisticated on-orbit activities, at least some of which are intended to advance counterspace capabilities. Some technologies with peaceful applications—such as satellite inspection, refueling, and repair—can also be used against adversary spacecraft.

Russia and China continue to publicly and diplomatically promote international agreements on the nonweaponization of space and "no first placement" of weapons in space. However, many classes of weapons would not be addressed by such proposals, allowing them to continue their pursuit of space warfare capabilities while publicly maintaining that space must be a peaceful domain.

#### **TRANSNATIONAL ORGANIZED CRIME**

*Transnational organized criminal groups and networks will pose serious and growing threats to the security and health of US citizens, as well as to global human rights, ecological integrity, government revenues, and efforts to deal with adversaries and terrorists. In the most severe cases abroad, criminal enterprises will*



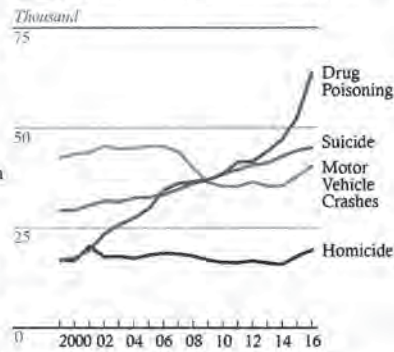
*contribute to increased social violence, erode governments' authorities, undermine the integrity of international financial systems, and harm critical infrastructure.*

#### Drug Trafficking

*Transnational organized criminal groups supply the dominant share of illicit drugs consumed in the United States, fueling high mortality rates among US citizens.*

- Americans in 2016 died in record numbers from drug overdoses, 21 percent more than in 2015.
- Worldwide production of cocaine, heroin, and methamphetamine is at record levels. US mortality from potent synthetic opioids doubled in 2016, and synthetic opioids have become a key cause of US drug deaths.
- Mexican criminal groups will continue to supply much of the heroin, methamphetamine, cocaine, and marijuana that cross the US-Mexico border, while China-based suppliers ship fentanyl and fentanyl precursors to Mexico-, Canada-, and US-based distributors or sell directly to consumers via the Internet.

Causes of US Premature Deaths, 1999-2016



Source: U.S. Commission on Disease Control and Prevention

1P13002 10.11

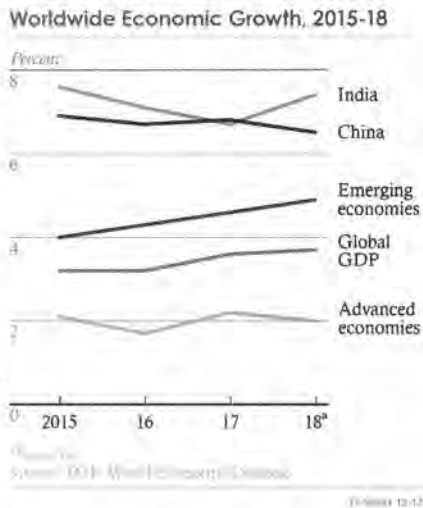
#### Broader Threats From Transnational Crime

*Transnational organized criminal groups, in addition to engaging in violence, will continue to traffic in human beings, deplete natural resources, and siphon money from governments and the global economy.*

- Human trafficking will continue in virtually every country. International organizations estimate that about 25 million people are victims.
- The FBI assesses that US losses from cybercrime in 2016 exceeded \$1.3 billion, and some industry experts predict such losses could cost the global economy \$6 trillion by 2021.
- Criminal wildlife poaching, illegal fishing, illicit mining, and drug-crop production will continue to threaten economies, biodiversity, food supply security, and human health. For example, academic studies show that illicit mining alone adds some 650 to 1,000 tons of toxic mercury to the ecosystem each year.
- Transnational organized criminal groups probably will generate more revenue from illicit activity in the coming year, which the UN last estimated at \$1.6-\$2.2 trillion for 2014.

## ECONOMICS AND ENERGY

*Global growth in 2018—projected by the IMF to rise to 3.9 percent—is likely to become more broadly based, but growth remains weak in many countries, and inflation is below target in most advanced economies.* The relatively favorable outlook for real economic growth suggests little near-term risk of unfavorable deficit-debt dynamics among the advanced economies. Supportive financial conditions and improving business sentiment will help to drive economic activity in advanced countries. China's growth may decelerate as the property sector cools and if Beijing accelerates economic reforms. India's economy is expected to rebound after headwinds from taxation changes and demonetization, and the continuing upswing in emerging and developing economies could be tempered by capital outflows from a stronger dollar and monetary policy normalization in the United States and Europe.



*Oil-exporting countries continue to suffer from the late-2014 oil price drop, and their economic woes are likely to continue, with broader negative implications.* Subdued economic growth, combined with sharp increases in North American oil and gas production, probably will continue putting downward pressure on global energy prices, harming oil-exporting economies. The US Energy Information Administration forecasts that 2018 West Texas Intermediate and Brent prices will average \$58 and \$62 per barrel, respectively, far below the average annual prices of \$98 and \$109 in 2013.

- Low oil prices and production declines—along with poor economic policies—have pushed Venezuela and the state-owned oil company, Petroleos de Venezuela, to miss debt payments, putting them in selective default.
- Saudi Arabia and other Persian Gulf oil exporters have experienced sharp increases in budget deficits, forcing governments to issue debt and enact politically unpopular fiscal reforms, such as cuts to subsidies, social programs, and government jobs.
- In Africa, declining oil revenue, mismanagement, and inadequate policy responses to oil price shocks have contributed to Angolan and Nigerian fiscal problems, currency strains, and deteriorating foreign exchange reserves.
- OPEC member countries and select non-OPEC producers, including Russia, in early 2017 committed to cut oil production in order to lift prices, with compliance likely to be offset somewhat as Libya or Nigeria—both are exempt from the deal—are able to resume production.

## HUMAN SECURITY

*Governance shortfalls, violent conflict, environmental stresses, and increased potential for a global health crisis will create significant risks to human security, including high levels of human displacement and migration flows.*

### Governance and Political Turbulence

*Domestic and foreign challenges to democracy and institutional capacity will test governance quality globally in 2018*, especially as competitors manipulate social media to shape opinion. Freedom House reported the 11th consecutive year of decline in “global freedom” in 2017, and nearly one-quarter of the countries registering declines were in Europe.

- While the number of democracies has remained steady for the past decade, some scholars suggest the quality of democracy has declined.
- We note that more governments are using propaganda and misinformation in social media to influence foreign and domestic audiences.
- The number and sophistication of government efforts to shape domestic views of politics have increased dramatically in the past 10 years. In 2016, Freedom House identified 30 countries, including the Philippines, Turkey, and Venezuela, whose governments used social media to spread government views, to drive agendas, and to counter criticism of the government online.

*Poor governance, weak national political institutions, economic inequality, and the rise of violent nonstate actors all undermine states’ abilities to project authority and elevate the risk of violent—even regime-threatening—instability and mass atrocities.*

### Environment and Climate Change

*The impacts of the long-term trends toward a warming climate, more air pollution, biodiversity loss, and water scarcity are likely to fuel economic and social discontent—and possibly upheaval—through 2018.*

- The past 115 years have been the warmest period in the history of modern civilization, and the past few years have been the warmest years on record. Extreme weather events in a warmer world have the potential for greater impacts and can compound with other drivers to raise the risk of humanitarian disasters, conflict, water and food shortages, population migration, labor shortfalls, price shocks, and power outages. Research has not identified indicators of tipping points in climate-linked earth systems, suggesting a possibility of abrupt climate change.
- Worsening air pollution from forest burning, agricultural waste incineration, urbanization, and rapid industrialization—with increasing public awareness—might drive protests against authorities, such as those recently in China, India, and Iran.
- Accelerating biodiversity and species loss—driven by pollution, warming, unsustainable fishing, and acidifying oceans—will jeopardize vital ecosystems that support critical human systems. Recent estimates suggest that the current extinction rate is 100 to 1,000 times the natural extinction rate.



- Water scarcity, compounded by gaps in cooperative management agreements for nearly half of the world's international river basins, and new unilateral dam development are likely to heighten tension between countries.

#### Human Displacement

*Global displacement almost certainly will remain near record highs during the next year, raising the risk of disease outbreaks, recruitment by armed groups, political upheaval, and reduced economic productivity.* Conflicts will keep many of the world's refugees and internally displaced persons from returning home.

#### Health

*The increase in frequency and diversity of reported disease outbreaks—such as dengue and Zika—probably will continue through 2018, including the potential for a severe global health emergency that could lead to major economic and societal disruptions, strain governmental and international resources, and increase calls on the United States for support. A novel strain of a virulent microbe that is easily transmissible between humans continues to be a major threat, with pathogens such as H5N1 and H7N9 influenza and Middle East Respiratory Syndrome Coronavirus having pandemic potential if they were to acquire efficient human-to-human transmissibility.*

- The frequency and diversity of disease outbreaks have increased at a steady rate since 1980, probably fueled by population growth, travel and trade patterns, and rapid urbanization. Ongoing global epidemics of HIV/AIDS, malaria, and tuberculosis continue to kill millions of people annually.
- Increasing antimicrobial resistance, the ability of pathogens—including viruses, fungi, and bacteria—to resist drug treatment, is likely to outpace the development of new antimicrobial drugs, leading to infections that are no longer treatable.
- The areas affected by vector-borne diseases, including dengue, are likely to expand, especially as changes in climatological patterns increase the reach of the mosquito.
- The World Bank has estimated that a severe global influenza pandemic could cost the equivalent of 4.8 percent of global GDP—more than \$3 trillion—and cause more than 100 million deaths.

## REGIONAL THREATS

### EAST ASIA

#### China

*China will continue to pursue an active foreign policy—especially in the Asia Pacific region—highlighted by a firm stance on its sovereignty claims in the East China Sea (ECS) and South China Sea (SCS), its relations with Taiwan, and its pursuit of economic engagement across the region.* Regional tension will persist due to North Korea's nuclear and missile programs and simmering tension over territorial and maritime disputes in the ECS and SCS. China will also pursue efforts aimed at fulfilling its ambitious Belt and Road Initiative to expand China's economic reach and political influence across Eurasia, Africa, and the Pacific through infrastructure projects.

#### North Korea

North Korea's weapons of mass destruction program, public threats, defiance of the international community, confrontational military posturing, cyber activities, and potential for internal instability pose a complex and increasing threat to US national security and interests.

*In the wake of accelerated missile testing since 2016, North Korea is likely to press ahead with more tests in 2018, and its Foreign Minister said that Kim may be considering conducting an atmospheric nuclear test over the Pacific Ocean.* Pyongyang's commitment to possessing nuclear weapons and fielding capable long-range missiles, all while repeatedly stating that nuclear weapons are the basis for its survival, suggests that the regime does not intend to negotiate them away.

Ongoing, modest improvements to North Korea's conventional capabilities continue to pose a serious and growing threat to South Korea and Japan. Despite the North Korean military's many internal challenges and shortcomings, Kim Jong Un continues to expand the regime's conventional strike options with more realistic training, artillery upgrades, and close-range ballistic missiles that improve North Korea's ability to strike regional US and allied targets with little warning.

#### Southeast Asia

*Democracy and human rights in many Southeast Asian countries will remain fragile in 2018 as autocratic tendencies deepen in some regimes and rampant corruption and cronyism undermine democratic values.* Countries in the region will struggle to preserve foreign policy autonomy in the face of Chinese economic and diplomatic coercion.

- Cambodian leader Hun Sen will repress democratic institutions and civil society, manipulate government and judicial institutions, and use patronage and political violence to guarantee his rule beyond the 2018 national election. Having alienated Western partners, Hun Sen will rely on Beijing's political and financial support, drawing Cambodia closer to China as a result.
- The crisis resulting from the exodus of more than 600,000 Rohingyas from Burma to Bangladesh will threaten Burma's fledgling democracy, increase the risk of violent extremism, and provide openings for Beijing to expand its influence.



- *In the Philippines, President Duterte will continue to wage his signature campaign against drugs, corruption, and crime.* Duterte has suggested he could suspend the Constitution, declare a “revolutionary government,” and impose nationwide martial law. His declaration of martial law in Mindanao, responding to the ISIS-inspired siege of Marawi City, has been extended through the end of 2018.
- *Thailand’s leaders have pledged to hold elections in late 2018, but the new Constitution will institutionalize the military’s influence.*

## MIDDLE EAST AND NORTH AFRICA

### Iran

*Iran will seek to expand its influence in Iraq, Syria, and Yemen, where it sees conflicts generally trending in Tehran’s favor, and it will exploit the fight against ISIS to solidify partnerships and translate its battlefield gains into political, security, and economic agreements.*

- Iran’s support for the Popular Mobilization Committee (PMC) and Shia militants remains the primary threat to US personnel in Iraq. We assess that this threat will increase as the threat from ISIS recedes, especially given calls from some Iranian-backed groups for the United States to withdraw and growing tension between Iran and the United States.
- In Syria, Iran is working to consolidate its influence while trying to prevent US forces from gaining a foothold. Iranian-backed forces are seizing routes and border crossings to secure the Iraq-Syria border and deploying proregime elements and Iraqi allies to the area. Iran’s retaliatory missile strikes on ISIS targets in Syria following ISIS attacks in Tehran in June were probably intended in part to send a message to the United States and its allies about Iran’s improving military capabilities. Iran is pursuing permanent military bases in Syria and probably wants to maintain a network of Shia foreign fighters in Syria to counter future threats to Iran. Iran also seeks economic deals with Damascus, including deals on telecommunications, mining, and electric power repairs.
- In Yemen, Iran’s support to the Huthis further escalates the conflict and poses a serious threat to US partners and interests in the region. Iran continues to provide support that enables Huthi attacks against shipping near the Bab al Mandeb Strait and land-based targets deep inside Saudi Arabia and the UAE, such as the 4 November and 19 December ballistic missile attacks on Riyadh and an attempted 3 December cruise missile attack on an unfinished nuclear reactor in Abu Dhabi.

*Iran will develop military capabilities that threaten US forces and US allies in the region, and its unsafe and unprofessional interactions will pose a risk to US Navy operations in the Persian Gulf.*

Iran continues to develop and improve a range of new military capabilities to target US and allied military assets in the region, including armed UAVs, ballistic missiles, advanced naval mines, unmanned explosive boats, submarines and advanced torpedoes, and antiship and land-attack cruise missiles. Iran has the largest ballistic missile force in the Middle East and can strike targets up to 2,000 kilometers from Iran’s borders. Russia’s delivery of the SA-20c SAM system in 2016 has provided Iran with its most advanced long-range air defense system.

- Islamic Revolutionary Guard Corps (IRGC) Navy forces operating aggressively in the Persian Gulf and Strait of Hormuz pose a risk to the US Navy. Most IRGC interactions with US ships are professional, but as of mid-October, the Navy had recorded 14 instances of what it describes as “unsafe and/or unprofessional” interactions with Iranian forces during 2017, the most recent interaction occurring last August, when an unarmed Iranian drone flew close to the aircraft carrier USS Nimitz as fighter jets landed at night. The Navy recorded 36 such incidents in 2016 and 22 in 2015. Most involved the IRGC Navy. We assess that these interactions, although less frequent, will continue and that they are probably intended to project an image of strength and, possibly, to gauge US responses.

*Iranian centrist and hardline politicians increasingly will clash as they attempt to implement competing visions for Iran’s future.* This contest will be a key driver in determining whether Iran changes its behavior in ways favorable to US interests.

- Centrists led by President Hasan Ruhani will continue to advocate greater social progress, privatization, and more global integration, while hardliners will view this agenda as a threat to their political and economic interests and to Iran’s revolutionary and Islamic character.
- Supreme Leader Ali Khamenei’s views are closer to those of the hardliners, but he has supported some of Ruhani’s efforts to engage Western countries and to promote economic growth. The Iranian economy’s prospects—still driven heavily by petroleum revenue—will depend on reforms to attract investment, strengthen privatization, and grow nonoil industries, which Ruhani will continue pursuing, much to the dismay of hardliners. National protests over economic grievances in Iran earlier this year have drawn more attention to the need for major reforms, but Ruhani and his critics are likely to use the protests to advance their political agendas.
- Khamenei has experienced health problems in the past few years, and, in an effort to preserve his legacy, he probably opposes moving Iran toward greater political and economic openness. As their relationship has deteriorated since the presidential election last June, Ruhani has tried to mend relations with Khamenei as well as his allies, but, in doing so, he risks failing to make progress on reforms in the near-term.

#### Syria

*The conflict has decisively shifted in the Syrian regime’s favor, enabling Russia and Iran to further entrench themselves inside the country. Syria is likely to experience episodic conflict through 2018, even as Damascus recaptures most of the urban terrain and the overall level of violence decreases.*

- *The Syrian opposition’s seven-year insurgency is probably no longer capable of overthrowing President Bashar al-Asad or overcoming a growing military disadvantage.* Rebels probably retain the resources to sustain the conflict for at least the next year.
- ISIS is likely on a downward trajectory in Syria; yet, despite territorial losses, it probably possesses sufficient resources, and a clandestine network in Syria, to sustain insurgency operations through 2018.



- Moscow probably cannot force President Asad to agree to a political settlement that he believes significantly weakens him, unless Moscow is willing to remove Asad by force. While Asad may engage in peace talks, he is unlikely to negotiate himself from power or offer meaningful concessions to the opposition.
- Russia and Iran are planning for a long-term presence, securing military basing rights and contracts for reconstruction and oil and gas exploitation. Iran is also seeking to establish a land corridor from Iran through Syria to Lebanon. The Kurdish People's Protection Unit—the Syrian militia of the Kurdistan Workers' Party (PKK)—probably will seek some form of autonomy but will face resistance from Russia, Iran, and Turkey.
- As of October 2017, there were more than 5 million Syrian refugees in neighboring countries, and an estimated 6.3 million internally displaced. Reconstruction could cost at least \$100 billion and take at least 10 years to complete. Asad's battered economy will likely continue to require significant subsidies from Iran and Russia to meet basic expenses.

#### Iraq

*Iraq is likely to face a lengthy period of political turmoil and conflict as it struggles to rebuild, reconstitute the Iraqi state, maintain pressure on ISIS, and rein in the Iranian-backed Shia militias that pose an enduring threat to US personnel.*

- The Iraqi Government, which has accrued \$120 billion in debt, requires substantial external assistance to cover hundreds of millions of dollars in humanitarian-aid shortfalls and a World Bank estimated \$88.2 billion to restore heavily damaged infrastructure, industry, and service sectors in areas retaken from ISIS.
- Prime Minister Haydar al-Abadi's forceful reassertion of Baghdad's authority after the Kurdistan Regional Government's (KRG) independence referendum in September illustrates the divisions among Iraqi leaders over the future of the state. The move to curb Kurdish autonomy was popular among many Arab Shia and Sunnis and may prompt Iraqi leaders to be uncompromising in political reconciliation discussions in order to consolidate votes in the run-up to elections planned for next spring.
- ISIS will remain a terrorist and insurgent threat, and the group will seek to exploit Sunni discontent to conduct attacks and try to regain Iraqi territory. Baghdad will struggle to reorient the Iraqi Security Forces (ISF) from conventional warfare to counterinsurgency and counterterrorism against ISIS while consolidating state control of territory and integrating the Iranian-backed and Shia-dominated Popular Mobilization Committee (PMC).
- There is an increasing risk that some Shia militants will seek to attack US targets in Iraq because they believe that the US security presence is no longer needed, want to reassert Iraqi sovereignty, and support Iran's goal of reducing US influence in Iraq.

Baghdad will have to contend with longstanding and war-hardened ethnosectarian divisions between Shia, Sunnis, and Kurds that were kept in check by the threat from ISIS. Despite ISIS's loss of territory, the social and political challenges that gave rise to the group remain and threaten the cohesion of the Iraqi state.

### Yemen

The war in Yemen is likely to continue for the foreseeable future because the Iranian-backed Huthis and the Saudi-led coalition remain far apart on terms for ending the conflict. The death of former Yemeni President Ali Abdallah Salih is only likely to further complicate the conflict as the Huthis and others scramble to win over those who previously backed Salih. We assess that the Huthis will continue to pursue their goals militarily and that, as a result, US allies and interests on the Arabian Peninsula will remain at risk of Huthi missile attacks until the conflict is resolved.

- Continued fighting almost certainly will worsen the vast humanitarian crisis, which has left more than 70 percent of the population—or about 20 million people—in need of assistance and aggravated a cholera outbreak that has reached nearly 1 million confirmed cases. Relief operations are hindered by security and bureaucratic constraints established by both the Huthi-Salih alliance and the Saudi-led coalition and by international funding shortages.

## SOUTH ASIA

### Afghanistan

*The overall situation in Afghanistan probably will deteriorate modestly this year in the face of persistent political instability, sustained attacks by the Taliban-led insurgency, unsteady Afghan National Security Forces (ANSF) performance, and chronic financial shortfalls.* The National Unity Government probably will struggle to hold long-delayed parliamentary elections, currently scheduled for July 2018, and to prepare for a presidential election in 2019. The ANSF probably will maintain control of most major population centers with coalition force support, but the intensity and geographic scope of Taliban activities will put those centers under continued strain. Afghanistan's economic growth will stagnate at around 2.5 percent per year, and Kabul will remain reliant on international donors for the great majority of its funding well beyond 2018.

### Pakistan

*Pakistan will continue to threaten US interests by deploying new nuclear weapons capabilities, maintaining its ties to militants, restricting counterterrorism cooperation, and drawing closer to China.* Militant groups supported by Islamabad will continue to take advantage of their safe haven in Pakistan to plan and conduct attacks in India and Afghanistan, including against US interests. Pakistan's perception of its eroding position relative to India, reinforced by endemic economic weakness and domestic security issues, almost certainly will exacerbate long-held fears of isolation and drive Islamabad's pursuit of actions that run counter to US goals for the region.

South Asian Threats Challenge  
US Security Interests in 2018



**India-Pakistan Tension**

*Relations between India and Pakistan are likely to remain tense, with continued violence on the Line of Control and the risk of escalation if there is another high-profile terrorist attack in India or an uptick in violence on the Line of Control.*

**India-China Tension**

*We expect relations between India and China to remain tense and possibly to deteriorate further, despite the negotiated settlement to their three-month border standoff in August, elevating the risk of unintentional escalation.*

**Bangladesh-Burma Rohingya Crisis**

*The turmoil resulting from more than 600,000 Rohingyas fleeing from Burma to Bangladesh increases regional tension and may expand opportunities for terrorist recruitment in South and Southeast Asia. Further operations by Burmese security forces against Rohingya insurgents or sustained violence by ethnic Rakhine militias probably would make it difficult to repatriate Burmese from Bangladesh.*

**RUSSIA AND EURASIA****Russia**

*In his probable next term in office, President Vladimir Putin will rely on assertive and opportunistic foreign policies to shape outcomes beyond Russia's borders. He will also resort to more authoritarian tactics to maintain control amid challenges to his rule.*

Moscow will seek cooperation with the United States in areas that advance its interests. Simultaneously, Moscow will employ a variety of aggressive tactics to bolster its standing as a great power, secure a "sphere of influence" in the post-Soviet space, weaken the United States, and undermine Euro-Atlantic unity. The highly personalized nature of the Russian political system will enable Putin to act decisively to defend Russian interests or to pursue opportunities he views as enhancing Russian prestige and power abroad.

Russia will compete with the United States most aggressively in Europe and Eurasia, while applying less intense pressure in "outer areas" and cultivating partnerships with US rivals and adversaries—as well as with traditional US partners—to constrain US power and accelerate a shift toward a "multipolar" world. Moscow will use a range of relatively low-cost tools to advance its foreign policy objectives, including influence campaigns, economic coercion, cyber operations, multilateral forums, and measured military force. Russia's slow

**Economic and Military Affiliations in Russia's Neighborhood**



economic growth is unlikely to constrain Russian foreign policy or by itself trigger concessions from Moscow in Ukraine, Syria, or elsewhere in the next year.

President Putin is likely to increase his use of repression and intimidation to contend with domestic discontent over corruption, poor social services, and a sluggish economy with structural deficiencies. He will continue to manipulate the media, distribute perks to maintain elite support, and elevate younger officials to convey an image of renewal. He is also likely to expand the government's legal basis for repression and to enhance his capacity to intimidate and monitor political threats, perhaps using the threat of "extremism" or the 2018 World Cup to justify his actions.

In 2018, Russia will continue to modernize, develop, and field a wide range of advanced nuclear, conventional, and asymmetric capabilities to balance its perception of a strategic military inferiority vis-a-vis the United States.

#### **Ukraine**

*Ukraine remains at risk of domestic turmoil, which Russia could exploit to undermine Kyiv's pro-West orientation.* These factors will threaten Ukraine's nascent economic recovery and potentially lead to changes in its foreign policy that further inflame tension between Russia and the West.

- Popular frustrations with the pace of reforms, depressed standards of living, perceptions of worsening corruption, and political polarization ahead of scheduled presidential and legislative elections in 2019 could prompt early elections.
- Opposition leaders will seek to capitalize on popular discontent to weaken President Petro Poroshenko and the ruling coalition ahead of elections in 2019.

*The conflict in eastern Ukraine is likely to remain stalemated and marked by fluctuating levels of violence. A major offensive by either side is unlikely in 2018, although each side's calculus could change if it sees the other as seriously challenging the status quo.* Russia will continue its military, political, and economic destabilization campaign against Ukraine to stymie and, where possible, reverse Kyiv's efforts to integrate with the EU and strengthen ties to NATO. Kyiv will strongly resist concessions to Moscow but almost certainly will not regain control of Russian-controlled areas of eastern Ukraine in 2018. Russia will modulate levels of violence to pressure Kyiv and shape negotiations in Moscow's favor.

- Russia will work to erode Western unity on sanctions and support for Kyiv, but the Kremlin is coping with sanctions at existing levels.

#### **Belarus, the Caucasus, Central Asia, Moldova**

*The Kremlin will seek to maintain and, where possible, expand its influence throughout the former Soviet countries that it asserts are in its self-described sphere of influence.*

Russia views Belarus as a critical buffer between itself and NATO and will seek to spoil any potential warming between Minsk and the West. Belarus President Aleksandr Lukashenko will continue close security cooperation with Moscow but will continue to aim for normalized relations with the West as a check on Russia's influence.

Russia's continued occupation of 20 percent of Georgia's territory and efforts to undermine its Western integration will remain the primary sources of Tbilisi's insecurity. The ruling Georgian Dream party is likely to seek to stymie the opposition and reduce institutional constraints on its power.

Tension over the disputed region of Nagorno-Karabakh could devolve into a large-scale military conflict between Armenia and Azerbaijan, which could draw in Russia to support its regional ally. Both sides' reluctance to compromise, mounting domestic pressures, Azerbaijan's steady military modernization, and Armenia's acquisition of new Russian equipment sustain the risk of large-scale hostilities in 2018.

Russia will pressure Central Asia's leaders to reduce engagement with Washington and support Russian-led economic and security initiatives, while concerns about ISIS in Afghanistan will push Moscow to strengthen its security posture in the region. Poor governance and weak economies raise the risk of radicalization—especially among the many Central Asians who travel to Russia or other countries for work—presenting a threat to Central Asia, Russia, and Western societies. China will probably continue to expand outreach to Central Asia—while deferring to Russia on security and political matters—because of concern that regional instability could undermine China's economic interests and create a permissive environment for extremists, which, in Beijing's view, could enable Uighur militant attacks in China.

Moldova's ostensibly pro-European ruling coalition—unless it is defeated in elections planned for November—probably will seek to curb Russian influence and maintain a veneer of European reform while avoiding changes that would damage the coalition's grip on power. The current Moldovan Government probably will move forward on implementing Moldova's EU Association Agreement against the will of openly pro-Russian and Russian-backed President Igor Dodon. Settlement talks over the breakaway region of Transnistria will continue, but progress likely will be limited to small issues.

## EUROPE

*The European Union and European national governments will struggle to develop common approaches to counter a variety of security challenges, including instability on their periphery, irregular migration to their region, heightened terrorist threats, and Russian influence campaigns, undercutting Western cohesion.*

- These concerns are spurring many countries to increase defense spending and enhance capabilities.
- European governments will need to strengthen their counterterrorism regimes to deal with a diverse threat, including ISIS aspirants and returning foreign fighters.

Turkey's counterterrorism cooperation with the United States against ISIS is likely to continue, but thwarting Kurdish regional ambitions will be a foreign policy priority. President Recep Tayyip Erdogan is likely to employ polarizing rhetoric, straining bilateral relations and cooperation on shared regional goals.

**AFRICA**

*Nigeria—the continent's largest economy—will face a security threat from Boko Haram and ISIS West Africa (ISIS-WA) while battling internal challenges from criminal, militant, and secessionist groups.* ISIS-WA and Boko Haram are regional menaces, conducting cross-border attacks in Nigeria, Cameroon, Chad, and Niger and posing a threat to Western interests. Meanwhile, militant and secessionist groups in the southern and central areas of Nigeria are capitalizing on longstanding social and economic grievances as the country nears the 2019 presidential election.

*Politically fragile governments in Africa's Sahel region will remain vulnerable to terror attacks in 2018, despite efforts to coordinate their counterterror operations.* ISIS and al-Qa'ida-allied groups, along with other violent extremists, will attempt to target Western and local government interests in the region, and a stalled peace process is likely to undercut the presidential election in Mali.

*The Ethiopian and Kenyan Governments are likely to face opposition from publics agitating for redress of political grievances. Somalia's recently elected government probably will struggle to project its authority and implement security reforms amid the drawdown of African Union forces in 2018, while al-Shabaab—the most potent terrorist threat to US interests in East Africa—probably will increase attacks.*

*Clashes between the South Sudanese Government and armed opposition groups will continue, raising the risk of additional mass atrocities as both sides use ethnic militias and hate speech and the government continues its crackdown on ethnic minorities.* The South Sudanese are the world's fastest growing refugee population, and the significant humanitarian challenges stemming from the conflict, including severe food insecurity, will strain the resources of neighboring countries hosting refugees.

*Sudan is likely to continue some aspects of its constructive engagement with the United States following the suspension of sanctions because it has given priority to shedding its international pariah status and reviving its economy.* Khartoum probably will acquiesce to some US requests, such as increasing counterterrorism cooperation and improving humanitarian access, but will be reluctant to take any steps that it perceives jeopardize its national security interests.

*Political unrest and security threats across the region are likely to intensify as the Presidents of Burundi and the Democratic Republic of the Congo (DRC) face public and armed opposition to their rule and the Central African Republic (CAR) struggles to cope with a nationwide surge in conflict.* Over-stretched UN missions in CAR and DRC are unlikely to stem the rising challenges from their concurrent humanitarian and security crises.



## THE WESTERN HEMISPHERE

*A key feature of the 2018 political environment in Latin America almost certainly will be popular frustration with low economic growth, corruption scandals, and the specter of endemic criminal activity in some countries.* Larger and increasingly sophisticated middle classes—with greater access to social media—are demanding more accountability from their governments. Presidential elections, including those in Mexico and Colombia, will occur at a time when support for political parties and governing institutions is at record lows and could bolster the appeal of outsider candidates.

### Mexico

Mexicans are focused on presidential and legislative elections scheduled for July 2018, in which corruption, high violence, and a tepid economy will be key issues. The Mexican Government has made slow progress implementing rule-of-law reforms and will continue to rely on the military to lead counternarcotics efforts. Mexico's \$1.1 trillion economy benefits from strong economic fundamentals, but uncertainty over trade relationships and higher-than-expected inflation could further slow economic growth. President Enrique Peña Nieto is focusing on domestic priorities, including recovery from the September 2017 earthquakes and managing impacts from potential US policy shifts ahead of the elections. In recent years, Mexican US-bound migration has been net negative but might increase if economic opportunity at home declined.

### Central America

Insecurity and lack of economic opportunities likely will remain the principal drivers of irregular migration from the Northern Triangle countries of El Salvador, Guatemala, and Honduras. Homicide rates in these countries remain high, and gang-related violence is still prompting Central Americans to flee.

### Venezuela

Economic woes and international diplomatic pressure probably will put political pressure on the Venezuelan Government in 2018. Living standards have declined and shortages of basic goods are driving the increase in Venezuelans seeking asylum in the United States and the region. Venezuela's negotiations with creditors probably will lead to messy legal battles. Venezuela almost certainly will seek to minimize further disruptions to oil production and exports to maintain its critical oil export earnings. Oil prices have increased slightly this year, but crude oil production continues to decline.

### Colombia

President Juan Manuel Santos will seek to cement implementation of the Revolutionary Armed Forces of Colombia (FARC) peace accord, as campaigning intensifies for the May 2018 presidential election. The FARC's new political-party status and the uncertainty around the transitional justice reforms will be a factor in the political environment ahead of elections. Substantial budget constraints will slow major programs or policy changes. The influx of FARC dissidents, drug traffickers, and other illegal actors into remote areas will challenge security forces during the next 12 months. Cocaine production in Colombia is at an all-time high, and crop substitution and eradication programs are facing stiff local resistance.

**Cuba**

Havana will seek to manage President Raul Castro's planned retirement in April 2018. Castro's successor will inherit a stagnant economy and a stalled economic reform process.

**Haiti**

As President Jovenel Moise begins his second year in office, he will confront competing interests within his government, a vocal opposition, and a fragile economy. Crime and protest activity will test the Haitian National Police following the departure of the UN Stabilization Mission in October 2017 and the transition to a police-only UN mission.



Chairman BURR. Dan, thank you very much for that very thorough overview of the world and what's at play.

I'll recognize Members based upon seniority for up to five minutes. The Chair recognizes himself.

Admiral Rogers, according to the statement for the record the intelligence community assesses that most detected Chinese cyber operations against the United States' private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks nationwide. Rate the intelligence community's performance when it comes to notifying cleared defense contractors and other sensitive private sector actors about malicious cyber activities on their networks.

Admiral ROGERS. First, in all honesty, you're asking me to rate a function for which I don't have responsibility or day-to-day execution. So I'll give an opinion, but it's not informed by day-to-day experience per se. This is an issue both at NSA and at Cyber Command, although I try to work very aggressively because, as you have outlined, it's a tremendous concern for us in the Department.

Clearly, I think we are not where we need to be. The challenge I think is we've got multiple areas of knowledge and insight across the Federal Government, within the private sector, and how do we bring this together in an integrated team, with some real-time flow back and forth? That is not where we are today, but that's where we've got to get to.

Chairman BURR. In your estimation, are we doing enough to warn the private sector of the threat that's out there?

Admiral ROGERS. I think we are informing them as we become aware of it. But one of my concerns is we're only going to see one slice of this picture. I'm also interested in it from the private sector's perspective. Tell us what you are seeing. If we can bring these two together, we'll have such a broader perspective and much more in-depth knowledge of what's happening. I think that's part of this. It's not just, hey, one side needs to do a better job. I'm not trying to say it's two-sided, but I think it's our ability to bring this together as a team.

Chairman BURR. Given that you've seen the difficulty especially this Committee and the intelligence community has had communicating with the tech companies about a way forward that is in commonality, are you concerned at how this is going to become an increasingly challenging landscape for both Congress and for the intelligence community working as we see new tech firms emerge every day?

Admiral ROGERS. Yes, I am, because, quite frankly, I wonder, how bad does it have to get before we realize we have to do some things fundamentally differently? I would argue if you look at the Internet of Things, you look at the security levels within those components, folks, this is going to orders of magnitude. If we think the problem is a challenge now, if we just wait it's going to get much, much worse, exponentially, from a security perspective.

Chairman BURR. Director Pompeo, the IC assesses that North Korea is likely to press ahead with more tests in 2018, missile tests, noting that North Korea's foreign minister indicated an atmospheric nuclear test over the Pacific may be under consideration

by Pyongyang. What's the IC assess the regional reaction to this kind of test would be?

Director POMPEO. Senator, thanks for the question. If I may just take one minute to say, I've been doing this for a year now and I want to express my appreciation to this Committee for helping the CIA do the things it needs to do, providing us the resources and the authorities we need. We have put a lot of effort against this very problem. You have been incredibly supportive of that. So my team thanks you for that.

We think a test like that would certainly further unite the region. Having said that, our sense is that we have built a global coalition pushing back against Kim Jong Un and his terror regime. With respect to what each particular country might do, I'd prefer to keep that conversation to closed session this afternoon.

Chairman BURR. Great.

What's the IC's assessment of North Korea's willingness to employ its expansive conventional military capabilities?

Director POMPEO. Senator, one of the things that Director Coats referred to in his opening remarks is that Kim Jong Un remains not only intent on staying in power, the thing all dictators prefer to do, die in their sleep fully at the peak of their power; but he has this mission that is a longstanding North Korean idea of reunification. Their capacity to use a nuclear umbrella combined with their conventional forces to exert coercive behavior, certainly inside their country, certainly against South Korea, but more broadly, is something that our analysts are continuing to look at.

We can see as they ratchet up their nuclear capability, making a response more different, their capacity to do harm in the region as a result of their incredible conventional capabilities alone increases.

Chairman BURR. Probably for General Ashley and Admiral Rogers: According to the statement for the record, the widespread proliferation of artificial intelligence is likely to prompt new national security concerns. How is the IC accounting for the possibility of these new national security concerns? Are we seeing indications now that our adversaries are working to harness emerging technologies, like artificial intelligence, and is the IC looking to maximize the potential of emerging technologies in our own processes and analysis of data and intelligence?

General ASHLEY. Sir, if I could take a first shot at that one. You look at DIA—and thanks for all the support the Committee provides to the Defense Intelligence Agency. If you look at our coordination, if you look at foreign militaries and the operational environment, this is central to looking at doctrine and what they're developing. When you think about artificial intelligence, our near-peer competitors are pursuing this. It's a lot of commercial technology that's available. But when you look at the volume, big data and what's available, the ability to digest and pull all that information in, artificial intelligence is going to be integral to that.

An example of one of the projects we're working on—and this is at the open source level—Project Maven. You look at full motion video, for example, or social media. In full motion video, you're never going to be able to have the work force that's going to be able to go through all of the material, whether it's video, whether it's

what Admiral Rogers works in the way of signals intelligence, or what's available in social media. So artificial intelligence, machine learning, which is really kind of where we are right now. It's more machine learning than it is artificial intelligence. We're seeing all of our near-peer competitors invest in these kinds of technologies because it's going to get them to decision cycles faster, allow them to digest information in greater volumes, and have a better situational understanding of what's happening in the battle space, and in some cases just what's happening in the strategic environment.

Admiral ROGERS. Sir, I would agree with General Ashley. I would also highlight, every organization on this table is faced with the challenge of victims of our own success in some ways. The ability to access data at increased levels brings its own set of challenges. So we are collectively all attempting to deal with this.

When I look at potential adversaries, I see them going through the same set of challenges. I would argue when I look at the PRC in particular, there clearly is a national strategy designed to harness the power of artificial intelligence to generate strategic outcomes, along the lines that General Ashley highlighted, to generate positive outcomes.

You look at their research, you look at how it is affecting the amount of data they are going after. I can remember five, ten years ago looking at some data concentrations and thinking to myself: This is so large and has such a disparate amount of information in it, boy, it would be really different for an opponent potentially to generate insight and knowledge from it. I don't have those kinds of conversation any more.

With the power of machine learning, artificial intelligence, and big data analytics, data concentrations now increasingly are targets of attraction to a whole host of actors. We have watched the PRC and others engage in activities designed to access these massive data concentrations.

General ASHLEY. If I could follow up on that also, because this is one of those areas that's debatable in the commercial industry, so you see a lot of investment, academia and others, that are pursuing this. So there's a key piece of this I think is worth addressing as well, which is how do you operationalize it? If I could just use a World War II example, the fact that there were planes, radios, and tanks was not unique to the Germans in World War II. What they did is they came up with an operational concept that allowed them to leverage that.

Peter Singer, if anyone's ever read "Wired for War" or "Ghost Fleet," is a futurist. We sat on a panel with him a couple years ago, and it was interesting when I asked him: As you look at the things that are emerging from the technology and things that are coming out, what do you see in the way of breakthroughs to give somebody a really marked advantage? Peter's comment wasn't that I see something that gives someone such a marked advantage. It's who's able to harness it, who's able to operationalize it and put it to effect. So that's really a key difference, because a lot of that technology is going to be available globally.

Chairman BURR. Thank you.

Director COATS. If I could just ask your permission here, Robert Cardillo's agency NGA has probably taken some very significant

lead on this, given the enormous volume of collection that they take and the inability to process that through the use of humans. I've asked Robert to be prepared to answer that question for you because I think they're taking some leading efforts that might be helpful.

Director CARDILLO. I think it's important to note at the front what hasn't changed. Quite frankly, the mission, the responsibility, this whole table has is to provide you with decision advantage. What's changed is the world around us and now within us. So what we used to hold exclusively because we had capabilities that others didn't, is now more shared. So as Admiral Rogers has said, this is something that we all lock arms on, because it isn't the access that is exclusive anymore; it's the use. It's the concept of operations, as General Ashley said.

I have the same concerns you do about getting the cooperation we need from these companies. I'm rather optimistic about it because I think at the end of the day we can advance the American economy, we can advance American entrepreneurship, and we can advance our understanding of the world in a way that gets back to that first step, which is decision advantage.

Chairman BURR. Rest assured, the processing of data will come up in our closed session with you. I've got you targeted.

Vice Chair.

Vice Chairman WARNER. Thank you, Mr. Chairman.

I think I take with some note the fact that the ODNI Director started his discussion with cyber. I think it's very telling in terms of how we view worldwide threats.

Let me get one question out on the record. We all know it's been over a year since the Russian intervention in our 2016 elections. We've also seen Russia intervene in a number of other Western democracies. I'd like each of you to briefly reconfirm to the American public that our intelligence community understands this threat.

Last year those of you who were on the panel each expressed confidence in the January 2017 IC assessment that Russia interfered in the 2016 elections. I'd like each of you today to, one, reaffirm that; and also, with a simple yes or no, do you agree with Director Pompeo that we haven't seen a significant decrease in the Russian activity and we have every expectation—and, Director Coats, you've already alluded to this—that they'll try to continue to intervene in our elections in 2018 and 2020. We'll start with you, Director Cardillo. A simple yes or no will do.

Director CARDILLO. No change in my view of the 2017 assessment. I support that. And I agree with Director Pompeo's assessment about the likelihood of the 2018 occurrence as well.

Vice Chairman WARNER. Admiral.

Admiral ROGERS. I participated in that 2017 work. I stood by it then and I stand by it now, and I agree with Director Pompeo: This is not going to change or stop.

Vice Chairman WARNER. General Ashley.

General ASHLEY. Yes, it is not going to change, nor is it going to stop.

Director COATS. Throughout the entire community, we have not seen any evidence of any significant change from last year.

Director POMPEO. I agree with Director Pompeo.

[Laughter.]

Vice Chairman WARNER. You've been waiting for that answer.

Director POMPEO. I have. I've had that one in the pocket for a while, yes, sir.

Director WRAY. As do I.

Vice Chairman WARNER. One area that I think we were all a little all caught off guard on, and to a degree understandably, was how the Russians use social media. I realize this is a new area for all of us and there are legitimate issues around American civil rights that have to be balanced. But the fact is I think we have to have an organized plan going forward.

This question will be directed at DNI Coats and Director Wray, but if others want to weigh in. Because of the notion that these companies, while maybe located here, operate in cyber space and when we've got somebody masquerading as Mike Pompeo but is actually Boris Badenov in St. Petersburg, it doesn't fit neatly into a particular flow chart.

Director Coats and Director Wray, who is in charge of addressing the threat posed by foreign nationals or foreign nations in terms of their use and misuse of social media?

Director COATS. There's no single agency, quote, "in charge." There are several agencies throughout the Federal Government that have equities in this, and we are working together to try to integrate that process. It clearly is something that needs to be addressed and addressed as quickly as possible.

You and I have had a number of discussions about that. So we are keen on moving forward in terms of not only identification, but relative response and things that we can do to prevent this from happening. We are gaining more, I think, support from the private sector, who are beginning to recognize ever more the issues that are faced with the material that comes through their processes. We cannot as a government direct them what to do, but we certainly are spending every effort we can to work with them to provide some answers to this question.

Vice Chairman WARNER. Great.

Director WRAY. I would agree with Director Coats. I think it's a team effort, and one of the things that's really jumped out at me since being back in government is how much more of a team the intelligence community is than the last time I was in this space. I have one of Mike's people who sits right in my inner team, and vice versa, and we're dealing with each other every day. So it's teamwork within the intelligence community and then partnership with the private sector, which is I think the other big change I've noticed. There's a lot more forward-leaning engagement with the private sector in terms of trying to share information and raise awareness on their end, because at the end of the day we can't fully police social media, so we have to work with them so that they can police themselves a little bit better as well.

Vice Chairman WARNER. Well, let me say I think the companies themselves are slow to recognize this threat. I think they've still got more work to do. But the fact that we don't have clarity in terms of who's in charge means I believe we don't have a full plan.

Let me just get one last question in quickly on the rise—and the Chairman has alluded to this as well—the rise of Chinese tech



companies. I know Senator Cornyn and Senator Feinstein have got legislation on CFIUS. But my fear is that some of these Chinese tech companies may not even have to acquire an American company before they become pervasive in our market.

Again, I'll start with Director Coats and Director Wray: How do we make sure that we send a signal to the private sector before some of these companies in effect totally invade our market, particularly because so many of them are tied back to the Chinese government?

Director COATS. Well, I think it's not only sending a signal and working together, sharing information with the private sector and the public sector. It also I think involves almost a whole of government issue, in particular legislative, with the legislation that is being looked at in terms of the CFIUS process. I think we need to go beyond what the current process is in terms of evaluating. We as a community will coordinate our intelligence to provide policy-makers and those that are making these decisions with the best intelligence we can relative to what the situation is.

So we view this as a top priority, and it's ongoing because, as I mentioned in my earlier remarks here, the Chinese are pervasive on this and we've seen it happen throughout both the public and the private sector.

Director WRAY. We've tried very hard to be more out and about in the private sector in terms of providing what are almost like defensive briefings, so that some of the U.S. telecommunications companies, among other technology industry members, kind of can recognize the threats that are coming their way. I think I've been pretty gratified by the response that we've gotten by most companies once we're able to try to educate them.

I think one of the bigger challenges we face is that, because America is the land of innovation, there's a lot of very exciting stuff that's happening in terms of smaller startup companies. A lot of them are a lot less sophisticated about some of this stuff, and trying to make sure we're touching those and educating them as well is a continuing challenge. The reality is that the Chinese have turned more and more to creative avenues, using nontraditional collectors, which I think we in the intelligence community recognize, but I think the private sector is not used to spotting. So a lot of it is trying to educate them about what to be on the lookout for and to have it be more of a dialogue.

Vice Chairman WARNER. Thank you.

Chairman BURR. Senator Risch.

Senator RISCH. Thank you very much.

First of all, I want to associate myself with the remarks of the Vice Chairman when he said that this Committee will always have your backs. For those of you who've been associated with this Committee—Dan, since you used to sit here; and Director Pompeo, you ran the same operation across the way; Mr. Cardillo, Mr. Rogers—you guys seem like part of the committee, we see you so much up there. You know that's the case, and we sincerely appreciate that.

Every one of us here knows what a tough job each of your agencies has. Speaking for myself and I suspect for most, if not all, of the committee, we have absolute 100 percent confidence in your

ability to, in a very neutral, dispassionate fashion, deliver to us the facts that we need in order to make the policy decisions.

One of the things that does rear its ugly head occasionally and causes issues and that winds up in the media a lot more than it should is when your jobs intersect with domestic political affairs. Mr. Wray, probably you will wind up with this more than anybody else. It gets messy. It gets difficult. I think we've all got to recommit ourselves to what we're actually doing here to reach the right facts.

I would respectfully disagree with my good friend from Virginia that we are no better prepared to handle the Russians' onslaught in 2018 than we were in 2016. When this happened in 2016, those of us on this Committee, those of you at the panel, and most of you, most everyone who works in the IC, were not surprised to find out that the Russians were attempting to meddle in our affairs.

I think probably one of the best hearings we've had this year was the open hearing we had on how they use social media. We saw how disjointed it was, how ineffective it was, how cheap it was for them to do that. But I think after that, with all due respect to my friend from Virginia, I think the American people are ready for this. I think that now they're going to look askance a lot more at the information that is attempted to be passed out through social media.

The American people are smart people. They realize that there's people attempting to manipulate them, both domestic and foreign. I agree with everybody on the panel that this is going to go on. This is the way the Russians have done business. This is no surprise to us. We saw it even more so than we got it in France and Germany in the past year.

So I think the American people are much more prepared than they were before.

Dan, thank you for that analysis of Syria. I doubt it made it any clearer for me or for the American people. It's a Rubik's Cube that is very difficult and, after this weekend, I think it got even more complicated. I think that we're going to have to keep an eye on that.

I agree with you, cyber is certainly something that's right at the top. The financial condition of this country is of critical importance to us.

I want to close and I want to ask a specific question to four of you regarding Korea. I think that's the most existential threat that we face. I think it's something that's at our doorstep. A year ago when we talked about this, it was then. This is now. The movement of North Korea has not slowed down. In fact, if anything I think all of us would agree that it's probably picked up. And it's at our doorstep.

This is going to have to be dealt with in the very, very near future. We've talked about trying to engage in conversations and what conditions would be, etcetera. I think we're still in the process of refining that. But that's moving.

We've all watched over the last week the smile campaign that North Korea has inflicted on the South Korean people. The South Korean people seem to be charmed by it to some degree. Some of them seem to be captivated by it. From my point of view, I think

it's nothing more than a stall by the North Koreans to further develop what they're trying to do; and I suspect in my judgment I think we need to be very, very cautious of this.

Director Coats, Pompeo, Rogers, and Ashley, I'd like to hear your view of this supposed turn in the last couple of weeks by the North Koreans?

Director COATS. Well, this is an existential threat, potentially to the United States, but also to North Korea. Kim Jung Un views any kind of kinetic attack or effort to force him to give up his nuclear weapons as an existential threat to his nation and to his leadership in particular.

As you know, it's a very hard collection nation, given their secrecy and so forth. But we do know that it's a one-man decision. We have processes in place here in the United States to have multiple engagements with various agencies in terms of our policy-making and relative to the decision that ultimately the President makes. That does not appear to be the case in North Korea.

The provocative nature and the instability that Kim has demonstrated potentially is a significant threat to the United States. I agree with you that the decision time is becoming ever closer in terms of how we respond to this. Our goal is a peaceful settlement. We are using maximum pressure on North Korea in various ways, which can be described by my colleagues here, most of that in closed session. But we have to face the fact that this is a potentially existential problem for the United States.

Senator RISCH. Wise words.

Director Pompeo.

Director POMPEO. The last part of your question, about this past now almost week at the Olympics: We should all, the American people should all remember that Kim Jung Un is the head of the propaganda and agitation department. There is no indication there's any strategic change in the outlook for Kim Jung Un and his desire to retain his nuclear capacity to threaten the United States of America. No change there.

Senator RISCH. Admiral Rogers.

Admiral ROGERS. I would just say if KJU thinks he can split the relationship between ourselves and the South Koreans he is sadly mistaken.

Senator RISCH. And finally, Lieutenant General Ashley.

General ASHLEY. No change to his strategic calculus. As a matter of fact, under the KJU regime you've seen a much more deliberate effort in terms of readiness, very different from his father. So you've got a million man army, 70 percent of it is south of Pyongyang, and they train in a very deliberate fashion. The strategic calculus has not changed and we should not be misled by the events that are taking place around the Olympics.

Senator RISCH. Thank you so much.

My time is up, Mr. Chairman. Thank you.

Chairman BURR. Senator Feinstein.

Senator FEINSTEIN. Thanks very much.

I want to associate myself with some of the comments of Senator Risch. We just had a secure briefing last week and I think it was difficult and harsh. I harken back to the words of the Secretary of State on the three nos: one, that we do not seek regime change;

two, we do not—we are not seeking the accelerated reunion of the peninsula; and finally, that we will not bring U.S. forces north of the Demilitarized Zone if the Korean Peninsula is reunified.

Let me ask you, Mr. Pompeo, because you just spoke with some certainty: Does Kim Jung Un really understand and believe that our goals are not regime change or regime collapse?

Director POMPEO. Senator Feinstein, I can't give you any certainty about what Kim Jung Un actually subjectively believes. A very difficult intelligence problem anywhere in the world, most especially difficult there. I have expressed this before: We do remain concerned, our analysts remain concerned, that Kim Jung Un is not hearing the full story. That is, that those around him aren't providing nuance, aren't suggesting to him the tenuous nature of his position both internationally and domestically, the breach with China, and the deep connections between the United States and the Republic of Korea.

We are not at all certain that the leaders around him are sharing that information in a way that is accurate, complete, and full.

Senator FEINSTEIN. In a recent Washington Post op-ed, Victor Cha, who was recently under consideration to be United States Ambassador to South Korea, warned of the dangers of a preventive United States military strike against North Korea. He cautioned that such a strike would not halt North Korea's nuclear weapons program and could spark an uncontrolled conflict in the region that could kill hundreds of thousands of Americans.

He is not the only one. A number of experts on the area have said that. He argued to continue to press for multilateral sanctions at the UN, to provide Japan and South Korea advanced weapons training and intel, and some other things.

Has the intelligence community assessed how the North Korean regime would react to a preventive United States attack?

Director POMPEO. We have. I would prefer to share that with you in closed session this afternoon.

Senator FEINSTEIN. Would you do that this afternoon?

Director POMPEO. Yes, absolutely, Senator, yes. We have written about various forms of actions. We analyze the certainty and uncertainty we have around that analysis, as well as what we think happens in the event that the United States decides not to do that and continues to allow Kim Jung Un to develop his nuclear weapons arsenal.

Senator FEINSTEIN. Have you explored what it would take to bring them to the table?

Director POMPEO. We have. I prefer to share that with you in closed session, yes, ma'am.

Senator FEINSTEIN. Would you bring that to our attention this afternoon as well?

Director POMPEO. Yes, ma'am.

Senator FEINSTEIN. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Thank you, Senator Feinstein.

Senator Rubio.

Senator RUBIO. Thank you.

Thank you all for being here. I also echo the same words everyone else has shared with you about the esteem we have for all of our agencies and the important work they do.

I—and I think this has already been touched upon. I do believe that Russia, Vladimir Putin in particular, efforts around the world are very important. But the biggest issue of our time in my view, and I think in the view of most of the Members of this Committee and I would venture to guess most of the members of this panel, is China and the risks they pose.

I'm not sure, in the 240-some odd year history of this Nation, we have ever faced a competitor and potential adversary of this scale, scope, and capacity. It is my personal view, and it's shared by many people, that they are carrying out a well-orchestrated, well-executed, very patient, long-term strategy to replace the United States as the most powerful and influential nation on Earth.

You see that reflected in this repeated use of this term "community of common destiny," which basically means a retreat from Western values of democracy and freedom and openness towards some other model that benefits them. Their pursuit of this appears to be every element of their national power—military, commercial, trade, economic, information, and media.

The tools they use are everything from hacking into companies and critical infrastructure and defense contractors, everybody you can imagine, to using our immigration system against us, to even our universities.

That's where I wanted to begin. This week I—well, let me just ask this, and I'd start this with Director Coats: Is it your view that the United States today as a government is prepared for the scale, scope, and magnitude of the challenge presented by this plan that China's carrying out?

Director COATS. We have full awareness of what the Chinese are, attempting to have full awareness of what the Chinese are attempting to do on a global basis. There's no question that what you have just articulated is what's happening with China. They're doing it in a very smart way. They're doing it in a very effective way. They are looking beyond their own region. I think they have—it's clear that they have a long-term strategic objective to become a world power and they are executing throughout the whole of government ways in which they can accomplish that.

We have intensive studies going on throughout the intelligence community relative to A to Z on what China is doing. General Mattis has asked us for that. Others have asked us to provide that. Senator Warner called me last week. We had a discussion on that. I assured him that we are pulling all of our elements of intelligence-gathering together to provide a very, very deep dive into what China is doing now and what their plans are for the future and how it would impact on the United States.

Senator RUBIO. Just to highlight the different ways and untraditional ways in which they're pursuing this plan, Director Wray, let me ask you, what in your view could you say in this setting is the counterintelligence risk posed to U.S. national security from Chinese students, particularly those in advanced programs in the sciences and mathematics?



Director WRAY. I think in this setting I would just say that the use of nontraditional collectors, especially in the academic setting, whether it's professors, scientists, students, we see in almost every field office that the FBI has around the country. It's not just in major cities. It's in small ones as well. It's across basically every discipline.

I think the level of naivete on the part of the academic sector about this creates its own issues. They're exploiting the very open research and development environment that we have, which we all revere, but they're taking advantage of it.

So one of the things we're trying to do is view the China threat as not just a whole of government threat, but a whole of society threat on their end. I think it's going to take a whole of society response by us. So it's not just the intelligence community, but it's raising awareness within our academic sector, within our private sector, as part of the defense.

Senator RUBIO. In that vein, last week I wrote a letter to five higher education institutions in Florida about the Confucius Institutes, which are funded by Chinese government dollars, at U.S. schools. It is my view that they're complicit in these efforts to covertly influence public opinion and to teach half-truths designed to present Chinese history, government, or official policy in the most favorable light.

Do you share concerns about Confucius Institutes as a tool of that whole of society effort and as a way to exploit the sort of naive view among some in the academic circles about what the purpose of these institutes could be?

Director WRAY. We do share concerns about the Confucius Institutes. We've been watching that development for a while. It's just one of many tools that they take advantage of. We have seen some decrease recently in their own enthusiasm and commitment to that particular program, but it is something that we are watching warily and in certain instances have developed appropriate investigative steps.

Senator RUBIO. Thank you.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Vice Chairman Warner highlighted in his opening statement the importance of an effective security clearance process. So I've got a question for you, Director Wray. Was the FBI aware of allegations related to Rob Porter and domestic abuse? And if so, was the White House informed this could affect his security clearance? When were they informed? And, who at the White House was informed?

Director WRAY. Well, Senator, there's a limit to what I can say about the content of any particular background investigation, for a variety of reasons that I'm sure you can appreciate. I would say that the background investigation process involves a fairly elaborate set of standards, guidelines, protocols, agreements, etcetera, that have been in place for 20-plus years, and I'm quite confident that in this particular instance the FBI followed the established protocols.

Senator WYDEN. So was the White House informed that this could affect his security clearance? That's a yes or no.

Director WRAY. I can't get into the content of what was briefed to the——

Senator WYDEN. What were they informed?

Director WRAY. What I can tell you is that the FBI submitted a partial report on the investigation in question in March and then a completed background investigation in late July; that soon thereafter we received request for follow-up inquiry; and we did the follow-up and provided that information in November; and that we administratively closed the file in January; and then earlier this month we received some additional information and we passed that on as well.

Senator WYDEN. Okay. Let me turn now to the two recent arbitrary and inconsistent decisions that affect the politicizing of the classification system. The first was the public release of the Nunes memo. The second involved the report that the Congress required on Russian oligarchs, their relationship with President Putin, and indications of corruption. In that case the Secretary of the Treasury released nothing other than a list of rich Russians taken from public sources.

My question—and any of you can respond—Did any of you take a position on either of these two arbitrary classification decisions, and did any of you have any communications with the White House about either of those classification matters?

Director COATS. I'll start, and the answer is no.

General ASHLEY. No.

Admiral ROGERS. I raised concerns on this issue with the DNI.

Director CARDILLO. No.

Director POMPEO. The CIA was not asked to review the classification of the document.

Director WRAY. Not on the second, the oligarch Treasury document. We did have interaction about the memo from Chairman Nunes.

Senator WYDEN. Is there anything you can say that protects sources and methods in an open session with respect to that matter?

Director WRAY. Well, I would just say, as we said publicly, that we had grave concerns about that memo's release.

Senator WYDEN. Okay.

On encryption: Director Wray, as you know—this isn't a surprise because I indicated I would ask you about this—you have essentially indicated that companies should be making their products with back doors in order to allow you to do your job. And we all want you to protect Americans. At the same time, sometimes there's these policies that make us less safe and give up our liberties. That's what I think we get with what you are advocating, which is weak encryption.

Now, this is a pretty technical area, as you and I have talked about, and there's a field known as cryptography. I don't pretend to be an expert on it. But I think there is a clear consensus among experts in the field against your position to weaken strong encryption. So I have asked you for a list of the experts that you have consulted. I haven't been able to get it. Can you give me a date this afternoon when you will give me—this morning—a sense of when we will be told who these people are and who is advising

you to pursue this route? Because I don't know of anybody respected in the field who is advising that it is a good idea to adopt your position to weaken strong encryption. So can I get that list?

Director WRAY. I would be happy to talk more about this topic this afternoon. My position is not that we should weaken encryption. My position is that we should be working together, government and the private sector, to try to find a solution that balances both concerns.

Senator WYDEN. I'm on the program for working together. I just think we need to be driven by objective facts, and the position you all are taking is out of sync with what all the experts in the field are saying. I would just like to know who you are consulting with, and we'll talk some more about it this afternoon.

Thank you, Mr. Chairman.

Chairman BURR. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Director Pompeo, last week the New York Times published a report that alleged that U.S. intelligence officials had paid \$100,000 to a Russian source for phony secrets, including potentially compromising information about the President and information on certain tools allegedly stolen from the NSA.

First, is it accurate that the CIA has categorically denied the assertions in this story? And second, if so, what would be the motivations of a Russian who peddled this story to the New York Times and other Western media outlets? Is this part of the Russian campaign to undermine faith in Western democracies?

Director POMPEO. Senator Collins, first let me say thanks for the question. Reporting on this matter has been atrocious. It's been ridiculous, totally inaccurate. In our view, the suggestion the CIA was swindled is false. The people who were swindled were James Risen and Matt Rosenberg, the authors of those two pieces. Indeed, it's our view that the same two people who were proffering phony information to the United States Government proffered that same phony information to these two reporters.

The Central Intelligence Agency did not provide any resources, no money, to these two individuals who proffered U.S. Government information directly or indirectly at any time. And the information that we were working to try and retrieve was information that we believed might well have been stolen from the U.S. Government. It was unrelated to this idea of kompromat that appears in each of those two articles.

Senator COLLINS. Thank you.

Director Wray, the President has repeatedly raised concerns about current and former FBI leaders and has alleged corruption and political bias in the performance of the FBI's law enforcement and national security missions. I want to give you the opportunity today to respond to those criticisms. What is your reaction?

Director WRAY. Well, Senator, I would say that my experience, now six months in with the FBI, has validated all my prior experiences with the FBI, which is that it is the finest group of professionals and public servants I could hope to work for. Every day, many, many, many times a day, I'm confronted with unbelievable examples of integrity, professionalism and grit.

There are 37,000 people in the FBI, who do unbelievable things all around the world. Although you would never know it from watching the news, we actually have more than two investigations. And most of them do a lot to keep Americans safe.

Senator COLLINS. Thank you. That's one of the reasons I wanted to give you an opportunity to respond.

Director Coats, we've had a lot of discussion this morning about Russian attempts, which are ongoing, to influence elections in Western democracies, to undermine NATO, and to try to destroy institutions in our country and elsewhere. This is an election year in our country and it's, frankly, frustrating to me that we haven't passed legislation to help states strengthen their security of their voting systems.

Putting that issue aside, there is also going to be an election this year in Latvia, one of our NATO allies. What is your assessment of whether or not the Russians are actively engaged in trying to influence that election, and how concerned is the intelligence community that they might be successful in producing a government that is very sympathetic to Russia's foreign policy objectives?

Director COATS. Not only are we concerned, the 29 nations of NATO are concerned. I returned not that long ago from a meeting in Brussels with the intelligence arm of NATO, all 29 nations. The topic was addressed primarily on Russian meddling in elections and trying to undermine democratic values. At the end of that, the new director of that organization asked for a show of hands or any verbal response from any representatives of the 29 nations if they thought that Russia had not interfered with their processes, and particularly their elections, or had the potential to do so. Not one person raised their hand.

He said: So do I understand that we are unanimous in assessing what the Russians are trying to do to undermine our elections, to undermine our coordination with the United States and relationships with each other, to undermine the very basic principles of sharing with other European countries, everything that is accomplished through NATO? Do I understand that no one has an objection to—you all see this for what it is?

Dead silence. He said: I take silence to be consent. So I think that says that this is pervasive, that the Russians have a strategy that goes well beyond what's happening here in the United States, even though—while they have historically tried to do these kinds of things, clearly in 2016 they upped their game. They took advantage, sophisticated advantage of social media. They're doing that not only in the United States, they're doing that throughout Europe and perhaps elsewhere.

So I think that sends a very strong signal that any elections that are coming up need to be—we need to assume that there might be interference with that, particularly from the Russians and maybe from some other malign actors, and steps need to be taken to work with State and local officials, because many of these elections in the off year will be State and local—governorships, even members of certain houses of representation within the states themselves.

So it clearly is an issue that is whole of government and whole of—I would say this: The more—and we also agreed with this at Brussels and I tried to make that point while I was there. The

more transparency we can provide to the American people, to people of nations that see this threat coming, the better off we will be.

Obviously, we have to take other measures. But we need to inform the American public that this is real, that it's going to be happening, and the resilience needed for us to stand up and say we're not going to allow some Russian to tell us how to vote, how we ought to run our country. I think there needs to be a national cry for that.

Senator COLLINS. Thank you. Very valuable.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Thank you, Chairman.

Director Wray, the FBI has been accused of political bias recently against the President, by the President himself. In fact, he said the FBI's reputation is, quote, "in tatters." Do you think the FBI's reputation is in any way in tatters, and are you confident in the independence of your agents?

Director WRAY. Senator, there's no shortage of opinions about our agency, just like every other agency up here and just like the Congress. I can only speak from my experience.

Senator HEINRICH. I think you're doing better than the Congress.

Director WRAY. And my experience has been that every office I go to, every division I go to, has patriots, people who could do anything else with their careers, but have chosen to work for the FBI because they believe in serving others. The feedback I get from our State and local law enforcement partners, from our foreign partners, from the folks we work with in the private sector and the community, office after office after office, has been very, very gratifying and reassuring to me.

I'm a big believer in the idea that the FBI speaks through its work, through its cases, through the victims it protects. I encourage our folks not to get too hung up on what I consider to be the noise on TV and in social media.

Senator HEINRICH. So you haven't seen any evidence of some sort of inherent political bias in the agency?

Director WRAY. No.

Senator HEINRICH. How do statements like that impact the morale of rank and file agents, or are they able to shake that off?

Director WRAY. Well, we have 37,000 people. They're all individuals. They all think in their own way. But I guess I would say that our people are very mission-focused. They're accustomed to the fact that we do some of the hardest things there are to do for a living. And I like to think that our folks are pretty sturdy.

I think of a woman I met just the other day, an agent in the Miami office, who had a bad accident, 12 stitches in her face, and the next day, boom, right back at work. I think about the folks in the San Juan office that I visited recently. You want to talk about people going through a real storm. They do it, and they're out in the community. I can tell you, the community values what they do on the island.

Senator HEINRICH. Thank you.

An op-ed by a number of former intelligence analysts called the Nunes memo and its release, quote, "one of the worst cases of politicization of intelligence in modern American history," end quote. You said you had concerns about that memo. I know you



can't get into the gritty details of that, but can you say in your view whether or not one of those concerns is that it may have selectively cherry-picked information without presenting the entire fact pattern that led up to that FISA warrant application?

Director WRAY. Well, Senator, I would just repeat what we said at the time, which is that we had then and continue to have now grave concerns about the accuracy of the memorandum because of omissions. We provided thousands of documents that were very sensitive and lots and lots of briefings, and it's very hard for anybody to distill all that down to three and a half pages.

Senator HEINRICH. Director Pompeo, have you seen Russian activity in the lead-up to the 2018 election cycle?

[Pause.]

Director POMPEO. Yes. I paused only I'm trying to make sure I stay on the unclassified side. Yes, we have seen Russian activity and intentions to have an impact on the next election cycle here.

Senator HEINRICH. Director Coats.

Director COATS. Yes, we have.

Senator HEINRICH. Anyone else? Admiral Rogers.

Admiral ROGERS. Yes, and I think this would be a good topic to get into greater detail this afternoon.

Senator HEINRICH. This afternoon, right.

According to news reports, there are dozens of White House staff with only interim security clearances still, to include Jared Kushner, until last week to include White House Staff Secretary Rob Porter, what I would assume would have regularly reviewed classified documents as part of his job.

Director Coats, if someone is flagged by the FBI with areas of concern in their background investigations into White House staff with interim clearances, should those staff continue to have access to classified materials?

Director COATS. Let me first just speak in general relative to temporary classifications. Clearly, with a new administration in particular, we're trying to fill a lot of new slots. And the classification process and security clearance process, as has been mentioned—

Senator HEINRICH. I'm only speaking with regard to folks who may have had issues raised, as opposed to just being in the matter of course of going through the long process.

Director COATS. Well, I'm not in a position—and we can talk about this in the classified session. But I'm not in a position to discuss what individual situations are for specified individuals. I might just say that I think sometimes it is necessary to have some type of preliminary clearance in order to fill a slot. But I have publicly stated if that is the case the access has to be limited in terms of the kind of information they can be in a position to receive or not receive.

So I think that's something that we have to do as a part of our security clearance review. The process is broken. It needs to be reformed. As Senator Warner has previously said, it's not evolution; it's revolution. We have 700,000 backups. So we have situations where we need people in places, but they don't yet have that.

Your specific question I think I'd like to take up in the classified session.

Senator HEINRICH. Chairman, I'm over my time.

Thank you, Director Coats.

Chairman BURR. Senator Blunt.

Senator BLUNT. Thank you, Mr. Chairman.

Director Coats, Director Pompeo, Admiral Rogers, I think you all talked about evidence that the Russians would intend to do things to be active in our elections. There really seems to me two divisions of that activity. One is information that's put on the record, misleading, false, trying to develop that level. The other, even more sinister, might be the level of dealing with the election system itself, the voting day system, the registration system. Of those two, clearly the voting day system, the one we need to have the most concerns about that critical infrastructure.

This Committee has been working toward both of those goals, of trying to shore up critical infrastructure on Election Day as well as alert people to and decide what might be done about misinformation on the other side of the ledger.

Voting begins in March. That's next month. If we're going to have any impact on securing that voting system itself, it would seem to me that we need to be acting quickly. I think a great part of the strength of the system is the diversity of the system, different not only from State to State, but from election jurisdictions within those states. That's a strength, not a weakness, in my view.

But what are some of the things we can do to be more helpful to local election officials in encouraging them to share information when they think their systems are being attacked, getting more information to them than we have. There was a lot of criticism in the last cycle that we knew that some election systems were being attacked and didn't tell them they were being attacked.

So the three of you in any order. Let's just do the order that I started with: Director Coats, Director Pompeo, and Admiral Rogers. Any thoughts you have on what we can do to protect the critical infrastructure of the election system and how quickly we need to act if we intend to do that this year?

Director COATS. Well, the intelligence community, all elements of it are aware, and we want to provide, collect and provide, as much information as we can, so that we can give those warnings and alerts, so that we can share information back and forth with local and State on election processes.

With the Federal Government, the Department of Homeland Security, the FBI, obviously are more involved, given these are domestic issues. But we do look to every piece of intelligence we can gather, so that we can provide these warnings. It is an effort that I think the government needs to put together at the State and local level and work with those individuals who are engaged in the election process.

In terms of the security of their machines, cyber plays a major role here. So I think it is clearly an area where the Federal Government, foreign collection on potential threats of interference, warnings, and then processes in terms of how to put in place security and secure that to ensure the American people that their vote is sanctioned and well and not manipulated in any way whatsoever.

Senator BLUNT. Director Pompeo.

Director POMPEO. Senator Blunt, when I answered Senator Heinrich's question earlier I was referring to the former, the first part of your question, not truly to the latter. The things we've seen Russia doing to date are mostly focused on information types of warfare, the things that Senator Warner was speaking on most directly earlier.

With respect to the CIA's role—and I think Admiral Rogers will say his, too—we have two missions. One is to identify, identify the source of this information, make those here domestically aware of it so that they can do the things they need to do, whether that's FBI or DHS, so that they have that information. We are working diligently along many threat vectors to do that.

Then the second thing—and we can talk more about this this afternoon—is we do have some capabilities offensively to raise the cost for those who would dare challenge the United States' elections.

Senator BLUNT. After Admiral Rogers, Director Wray, I may want to come to you and see on that same, sharing information, any impediments to sharing that information with local officials or any reason we wouldn't want to do that.

Admiral Rogers.

Admiral ROGERS. Sir, the only other thing I would add—and this is also shaped by my experience at Cyber Command, where I defend networks—is one of the things that we generally find in that role, many network and system operators do not truly understand their own structures and systems. So one of the things that I think is part of this is how do we help those local, federal, State entities truly understand their network structure and what its potential vulnerabilities, and to harness this information that the intelligence structure and other elements are providing them. It's not necessarily an intel function, but I think it's part of how we work our way through this process.

Senator BLUNT. Director Wray.

Director WRAY. Senator, I think that's just one of the areas that—there's been a lot of discussion about whether we're doing better and this is one of the areas I think we are doing better. We together, at the FBI, together with DHS, recently, for example, scheduled meetings with various election, State election officials. Normally the barrier there would be classification concerns, whether somebody had clearances. We were able to put together briefings, appropriately tailored and with nondisclosure agreements, with those officials. So there are ways, if people are a little bit creative and forward-leaning, to educate the State election officials, which is of course where elections are run in this country.

Senator BLUNT. Well, hopefully we'll be creative and forward-leaning and we'll want to keep track of what we're doing there.

Thank you, Mr. Chairman.

Chairman BURR. Senator King.

Senator KING. Thank you, Mr. Chairman.

The first statement I want to make is more in sorrow than in anger. I'll get to the anger part in a minute. The sorrow part is that, Director Coats, in response to a question from Senator Collins, you gave an eloquent factual statement of the activities of the Russians and the fact that they're continuing around the world and

that they're a continuing threat to this country. All of you have agreed to that.

If only the President would say that. I understand the President's sensitivity about whether his campaign was in connection with the Russians. That's a separate question. But there is no question—we've got before us the entire intelligence community—that the Russians interfered in the election in 2016, they're continuing to do it, and they're a real imminent threat to our elections in a matter of eight or nine months.

My problem is I talk to people in Maine who say: The whole thing is a witch hunt and it's a hoax because the President told me. I just wish you all could persuade the President as a matter of national security to separate these two issues. The collusion issue is over here, unresolved; we'll get to the bottom of that. But there's no doubt, as you all have testified today. We cannot confront this threat, which is a serious one, with a whole of government response when the leader of the government continues to deny that it exists.

Now let me get to the anger part. The anger part involves cyber-attacks. You have all testified that we're subject to repeated cyber-attacks. Cyber-attacks are occurring right now in our infrastructure all over this country. I am sick and tired of going to these hearings, which I've been going to for five years, where everybody talks about cyber-attacks, and our country still does not have a policy or a doctrine or a strategy for dealing with them.

This is not a criticism of the current Administration. I'm an equal opportunity critic here. The prior Administration didn't do it either.

Admiral Rogers, until we have some deterrent capacity we are going to continue to be attacked. Isn't that true?

Admiral ROGERS. Yes, sir. We have to change this current dynamic, because we're on the wrong end of the cost equation.

Senator KING. And we are trying to fight a global battle with our hands tied behind our back.

Director Coats, you have a stunning statement in your report: "They will work to use cyber operations to achieve strategic objectives, unless they face clear repercussions for their cyber operations." Right now there are none. Is that not the case? There are no repercussions. We have no—we have no doctrine of deterrence. How are we ever going to get them to stop doing this if all we do is patch our software and try to defend ourselves?

Director COATS. Those are very relevant questions and I think everyone, not only at this table but in every agency of government, understands the threat that we have here and the impact already being made through these cyber threats. Our role as the intelligence community is to provide all the information we possibly can as to what is happening, so our policymakers can take that, including the Congress, and shape policy as to how we are going to respond to this and deal with this in a whole of government way.

Senator KING. It just never seems to happen. Director Pompeo, you understand this issue, do you not? We are not going to be able to defend ourselves from cyber-attacks by simply being defensive. We have to have a doctrine of deterrence. If they strike us in cyber, they are going to be struck back in some way. It may not be cyber.

Director POMPEO. I would agree with you. I would also argue that—and while I can't say much in this setting, I would argue that your statement that we have done nothing does not reflect the responses that, frankly, some of us at this table have engaged in and the United States Government has engaged in, both before and after this—excuse me—both during and before this Administration.

Senator KING. But deterrence doesn't work unless the other side knows it. The doomsday machine in Dr. Strangelove didn't work because the Russians hadn't told us about it.

Director POMPEO. It's true that it's important that the adversary know it. It is not a requirement that the whole world know it.

Senator KING. And the adversary does know it in your view?

Director POMPEO. I'd prefer to save that for another forum.

Senator KING. Well, I believe that this country needs a clear doctrine: What is a cyber-attack, what is an act of war, what will be the response, what will be the consequences? Right now I haven't seen it.

Director POMPEO. Senator, I agree with you, we collectively. It is a complicated problem, given the nature of—

Senator KING. I include us, by the way.

Director POMPEO. Yes, I would too. I sat as a member of the House of Representatives for six years. I take responsibility for not having been part of solving that, too.

There is a lot of work here to do. We do need a U.S. Government strategy and clear authorities to go achieve that strategy.

Senator KING. I appreciate it. I just don't want to go home to Maine when there's a serious cyber-attack and say: Well, we never really got to it; we knew it was a problem, but we had four different committees of jurisdiction and we just couldn't work it out.

Director POMPEO. Yes, sir.

Senator KING. That's not going to fly.

Director POMPEO. Yes, sir.

Senator KING. Thank you, gentlemen, for your service.

Director COATS. Senator, I might just add that we don't want to learn this lesson the hard way. 9/11 took place because we were not coordinating our efforts. We are now coordinating our efforts, but we didn't have the right defenses in place because the right information was not there. Our job is to get that right information to the policymakers and get on with it, because it's just common sense. If someone is attacking you and there's no retribution or response, it's just going to incentivize more attacks. Right now there are a lot of blank checks. There's a lot of things that we need to do.

Senator KING. Director Coats, thank you. I appreciate that.

Thank you, Mr. Chairman.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Thank you.

Director Coats, you and I talked last year about this same issue that Senator King was just bringing up as well about cyber doctrine and a point person, on who that would be, and a defined person that would give options to the President and the Congress to say, if a response is needed and is warranted, this is the person, this is the entity, that would make those recommendations and



allow the President to be able to make the decisions on what the proper response is.

Has that been completed? Is there a point person to be able to give recommendations on an appropriate response to a cyber-attack to the President?

Director COATS. That has not yet been completed. Of course, your understanding of the standup of Cyber Command and the new director that will be replacing Admiral Rogers—the decision relative to whether there would be a separation between the functions that are currently now NSA and Cyber has yet to be made. General Mattis is contemplating what the next best step is. They've involved the intelligence community in terms of making decisions on that role. But we at this particular point cannot point to one sort of cyber czar, but various agencies throughout the Federal Government are taking this very, very seriously and there are individuals that continue to meet on a regular basis.

The ODNI has something called CTIIC and that is a coordination effort for all the cyber that comes in, so that we don't stovepipe like what we did before 9/11. So things are under way. But in terms of putting a finalized, this is how we're going to do it, together, it's still in process.

Director POMPEO. Senator Lankford, with respect to responses to that, these are Title 10 DOD activities unless they are granted to some other authority, a Title 50 authority. So there is a person responsible. Secretary Mattis has that responsibility to advise the President on the appropriateness of responses in all theaters of conflict with our adversaries.

Senator LANKFORD. Thank you.

I want to bring up the issue of the rising threat of what's happening just south of our border in Mexico. In Mexico the homicide rate went up 27 percent last year. We had 64,000 Americans that died from overdose of drugs. The preponderance of those came through or from Mexico. We have a very rapidly rising threat, it appears to me.

What I'd be interested in from you all is, on a national security level and what you're seeing, what are we facing? What's changing right now in Mexico versus ten years ago in Mexico in our relationship and the threats that are coming from there?

Director COATS. I would defer to Director Wray relative to what his agency is doing. Clearly, we have a continuing problem and the Mexican government has a continuing problem relative to the gangs and the organizations. There have been some high-profile arrests lately. We've taken down some labs. Mexico is cooperating, but they themselves will admit that it's almost overwhelming—their army's been participating—it's almost overwhelming for them to control the situation south of the border. We have our own issues then on border protection and as well as consumption here in the United States.

Senator LANKFORD. Director Wray.

Director WRAY. In many ways what we're seeing is just more of the same. But one of the things that's changed, because I think that was at the heart of your question, I think we're seeing—one of the things we're watching in particular is more black market fentanyl being shipped to transnational criminal organizations in

Mexico, and then their taking advantage of the pricing advantages, and that's being then delivered in large quantities to our streets.

Certainly the Mexico relationship is from a law enforcement perspective and from a domestic security perspective one of our most important. I think the FBI LEGAT office in Mexico is our largest in the world. I'm pretty sure about that, or pretty close to it if not. That's a reflection of how much activity there is.

Senator LANKFORD. Let me ask you a specific Oklahoma question. It's also a national question. There was an individual named Alfallaj that was picked up in Weatherford, Oklahoma, just a couple of weeks ago by the FBI. His fingerprints were identified from a terror training camp in Afghanistan. He'd been in the country for multiple years.

What I'm trying to be able to determine is the coordination of information, the local law enforcement and from data that's gathered from some of the work that's happening overseas in Afghanistan and such. How are those two being married together that we can identify individuals that are a threat to our Nation based on their participation in a terror training camp overseas, now coming to the American shores?

Director WRAY. Well, certainly we've become better at looking at biometric information from overseas and marrying it up with potential threat subjects here in the U.S. as well as in some of our allies. The individual in question, of course, turned out to have his fingerprints on information from the Al-Farooq Camp. It's just a reminder to us that an awful lot of people went through those camps. And while the civilized world, the intelligence community, law enforcement, military, our allies around the world, made a major dent on those people, we're kidding ourselves if we think that an awful lot of them aren't still out there, and it's just a reminder that we need to stay on the balls of our feet.

Senator LANKFORD. Thank you.

General ASHLEY. Senator Lankford, if I could. One additional point. You asked what has changed in Mexico. What has also transpired over the last couple years is you had five principal cartels. We alluded to a number of captures that have taken place, over 100. Those five cartels have kind of devolved into 20, and part of that outgrowth, you see an increase in the level of violence.

Chairman BURR. Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

Thank all of you. First let me just tell you, on behalf of the people of West Virginia, I want to thank you for the job you do in keeping us safe, the professionalism. And we have all the utmost confidence in what you're doing and hope to be able to support even further. But thank you. The people really do appreciate it and we appreciate the service you're giving.

Director Coats, I think you and I both were in the Senate at the same time when Mike Mullen, then-Admiral Mullen, said that the greatest threat we face—I was on Armed Services; you were on Intelligence at that time. We were trying to find out what the greatest threat the United States faces. I was thinking of another country, whether it be Russia, China, or whatever. He didn't hesitate when he said that the threat of our Nation, the greatest threat is

the debt of our Nation. I think you just reiterated that in your opening remarks.

Director, I was a little bit mystified by the report, the worldwide threat assessment. You didn't mention the debt in here. It wasn't in the report as a threat to the Nation, and I didn't know if there was a thought process behind that, because you made a tremendous effort to put that in your opening statement. I appreciate that. But tell me what your thought process here was?

Director COATS. Well, my thought process was that I'm getting a little bit out of my lane in terms of what I'm supposed to do, but I felt that—

Senator MANCHIN. I mean, you do think it's a threat? It's not in this assessment.

Director COATS. It's just something that Congress needs to deal with, and I didn't want to come back and preach at you.

Senator MANCHIN. I got you.

Director COATS. But I thought at the very end—in fact, just yesterday—look, I think I have a responsibility to raise this issue because it does affect the military significantly, it affects the intelligence community, which is tied to the military in terms of intelligence. It's going to have a serious effect on us if we can't control it.

Senator MANCHIN. Well, you've sat on both sides of the aisle. The only thing that seems to be bipartisan here today is spending money. Both sides seem to agree on spending more money, without any accountability. So I'm glad to hear your remarks on that.

If I could, to all the witnesses: I share what Senator Lankford has said about concerns about what's killing more Americans than any of the threats discussed that we have today. It's with drugs. My State of West Virginia's been hit harder than any State. I've got more deaths per capita than any State. It's been ravaging as far as my communities, my homes, my schools, the families. It's just unbelievable what we're going through.

I think in a nutshell what I would be asking—all of you are responsible to do everything you can to keep us safe and you've done a tremendous job as far as from the foreign attack and things of that sort. Director Wray, I appreciate what the FBI does and they have a strong presence in West Virginia and we're very, very appreciative of that. What type of efforts from each one of your agencies have you spent as far as—Is drugs and fighting the drug infestation highest on your priority list, one of your greatest dangers, or is it just part of the overall scheme of things?

Director COATS. Just speaking for the intelligence community, it is a high priority for us. We mentioned it in our threat assessment here. So we are the collectors of foreign sources, transnational organizations, etcetera, whether it's coming from overseas, whether it's coming from Afghanistan, whether it's coming from Colombia, what it is, how it's going.

Then of course it is a whole of government, because once it penetrates the United States we then use our domestic agencies to address that.

Senator MANCHIN. Director Wray, as far as the FBI, because you're on the front line—you're here on the homeland—what do you think? What can we do to help?

Director WRAY. Well, I think on the good news side, in a country that's often very divided this is one issue as far as I can tell where everybody agrees about what a major, major threat it is. It covers communities from North to South, from red to blue, from rich to poor, from urban to rural. I think that's the good news.

The bad news is that it's grown to a point where there's no one agency or one approach that's going to solve the problem. So we're doing our part. Some of the things that we're able to do, we're focusing particularly on gatekeepers, because a lot of this is coming through medical professionals and pharmacies. So we're using intelligence-driven operations there, various initiatives. We have a prescription drug initiative that's focused on that part of it.

We're partnering with our foreign counterparts. We're working with DEA, State and local law enforcement, etcetera. We're also trying to do things to raise awareness. We did a video with DEA called "Chasing the Dragon," which has been shown in schools around the country.

But this is a multi-disciplinary problem.

Senator MANCHIN. My time is short. If I can just ask this question, maybe. Whoever wants to answer this one. Based on what we know and the way we distribute money for foreign aid to different countries, knowing that a lot of the countries we distribute to is basically allowing, permitting, this type of scourge coming to our country as far as in the form of drugs, have you all thought and considered and make recommendations that we hold them hostage, if you will, or liable, basically, to the money they're receiving from the United States with the best of intentions? But that best of intentions is their fight against drugs coming to our country, when we know it's coming, from whether it be a China, Afghanistan, or Iraq, wherever it may be coming from, Mexico and all the South American countries?

We should hold that. I've never seen—we're going to lose a whole generation in West Virginia. I have 10,000 jobs they can't fill. The United States has 3 million jobs we can't fill. And most of it is around drugs.

So this is what we're asking for. This has got to be all hands on deck. I don't know if anybody wants to—do you have that as a high priority? Does anyone believe we should withhold foreign aid to countries that basically we know have illicit drugs coming to our country?

Director POMPEO. Senator, I'll answer this. I think the United States should use every tool, whether that's foreign aid or other tools—

Senator MANCHIN. Money talks.

Director POMPEO [continuing]. To get these—that's exactly right—to get these nations that this is coming from to put it as a priority for their country. Some don't have the capacity to fix it. That is, it's a problem that's bigger than their nation. But we ought to—we should be unafraid to use the leverage that comes with our generosity from the American taxpayer to ensure that these countries are doing everything they can to prevent drugs from coming from their country to ours.

Senator MANCHIN. Thank you. I appreciate that.

Director COATS. As you do know, we do provide efforts within countries to help them eradicate. It hasn't been totally successful, but that is one way in which we use some of that aid if it's directly contributed to the eradication of drugs.

Senator MANCHIN. Thank you.

Chairman BURR. Senator Cotton.

Senator COTTON. Thank you, gentlemen, for your appearance, and thanks to all the men and women who you represent and for the work they do for our country.

Mr. Wray, are you aware of a gentleman by the name of Oleg Deripaska?

Director WRAY. I've heard the name.

Senator COTTON. Is it fair to call him a Putin-linked Russian oligarch?

Director WRAY. Well, I'll leave that characterization to others, and certainly not in this setting.

Senator COTTON. Chuck Grassley, the Chairman of the Judiciary Committee, last week sent a letter to a London-based lawyer who represents Mr. Deripaska and asked if Christopher Steele was employed, either directly or indirectly, by Oleg Deripaska at the time he was writing the so-called "Steele dossier." Do you know if Christopher Steele worked for Oleg Deripaska?

Director WRAY. That's not something I can answer.

Senator COTTON. Could we discuss it in the classified setting?

Director WRAY. There might be more we could say there.

Senator COTTON. Thank you. And maybe we'll hear back from the lawyer in London as well to give us a straight answer.

Jim Comey testified before this Committee in an open setting last summer and he referred to the Steele dossier as "salacious and unverified." Does that remain the FBI's position?

Director WRAY. I think maybe there's more we can talk about this afternoon on that.

Senator COTTON. Okay, thank you.

I'd like to turn my attention to the threat posed by China and specifically Chinese telecom companies. Senator Rubio spoke earlier, and I agree with what he said, about the threat of a rising China, and also the threat of Confucius Centers. There's also the threat the telecom companies, specifically Huawei and ZTE, but also Unicom and Telecom, pose to our country. That's why I've introduced legislation with Senator Cornyn and Senator Rubio to say the U.S. Government can't use Huawei or ZTE and that the U.S. Government can't use companies that use them. I'm glad that some companies, like Verizon and AT&T, among others, have taken this threat seriously.

Could you explain what the risk is that we face from ZTE and Huawei being used in the United States, especially here in this public setting, the risks that companies, State governments, local governments might face if they use Huawei or ZTE products and services?

Director WRAY. I think probably the simplest way to put it in this setting would be that we're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks that provides the capacity to



exert pressure or control over our telecommunications infrastructure. It provides the capacity to maliciously modify or steal information, and it provides the capacity to conduct undetected espionage.

So at a 100,000-foot level, at least in this setting, those are the kinds of things that worry us. I will say, like you, Senator, we've been gratified I think to date by the response of the large U.S. telecommunications providers trying to raise awareness on this issue. But I also recognize that the competitive pressures are building. So it's something that I think we have to be very vigilant about and continue, as you are doing, to raise awareness about.

Senator COTTON. Admiral Rogers, would you care to add anything about the threat posed by Huawei?

Admiral ROGERS. I would agree with Director Wray's characterization here. This is a challenge I think that's only going to increase, not lessen, over time for us.

Senator COTTON. So you would suggest to mayors, county judges, university presidents, and State legislatures, to look warily if Huawei or ZTE comes bearing gifts to them?

Admiral ROGERS. I would say you need to look long and hard at companies like this.

Senator COTTON. All the witnesses, I'd like to address this question to you. Will you please raise your hand if you would use products or services from Huawei or ZTE?

[No response.]

None of you would. You obviously lead intelligence services, so that's something of a biased question.

Raise your hand if you would recommend that private American citizens use Huawei or ZTE products or services?

[No response.]

None of you again are raising your hand. Thank you for that.

Finally, I'd like to turn to a question, Director Pompeo, that's been in the news in the last few hours. There are reports that over 200 Russian mercenaries were killed in eastern Syria. Can you confirm or deny those reports?

Director POMPEO. Senator Cotton, I'll leave to the Department of Defense to talk about what transpired there. I can say this. From an intelligence perspective, we have seen in multiple instances foreign forces using mercenaries in battles that will begin to approach the United States.

Senator COTTON. General Ashley, since you represent the Department of Defense, would you like to confirm or deny?

General ASHLEY. If we could take that to a closed session, Senator, I think we can lay out a rather interesting fabric of what is Syria and what transpired over the last few days.

Senator COTTON. We can address that in the afternoon.

Director Pompeo, to come back, as a general matter can I ask, is massing and maneuvering forces against a location where U.S. personnel are present in Syria a good way to get yourself killed?

Director POMPEO. I think I'll defer that to the Department of Defense as well.

Senator COTTON. General Ashley, would you like to answer that question?

General ASHLEY. Sir, that does make you more susceptible. I would leave that also to the operational commander. But you are at greater risk when you start to mass in that situation.

Senator COTTON. Not a good idea if you want to have a long and fruitful life.

Thank you.

Chairman BURR. Senator Harris.

Senator HARRIS. Thank you.

I want to echo the comments of my colleagues in thanking the men and women who serve in your agencies. I am concerned that the political attacks against the men and women of your agencies may have had an effect on your ability to recruit, retain, and also the morale of your agencies. So I would like to emphasize the point that we all I think share in making, which is we thank the men and women of your agencies for their selfless work. They do it on behalf of the American people, without any expectation of award or reward, and we cannot thank them enough for keeping us safe.

Director WRAY, Chairman Nunes's memo included sensitive FISA information regarding a person who worked on the President's campaign. According to the White House statement, the President was the one who authorized the memo's declassification. Do you believe there is an actual or at least the appearance of a conflict of interest when the President is put in charge of declassifying information that could complicate an ongoing investigation into his own campaign?

Director WRAY. Well, Senator, we've been very clear what our view was about the disclosure and accuracy of the memo in question. But I do think it's the President's role as Commander-in-Chief under the rule that was invoked to object or not to the declassification. So I think that is the President's responsibility.

Senator HARRIS. Regardless of whether there is an appearance or actual conflict of interest?

Director WRAY. Well, I leave it to others to characterize whether there's an appearance or actual conflict of interest. But I think the President was fulfilling his responsibility in that situation.

Senator HARRIS. If the President asked you tomorrow to hand over to him additional sensitive FBI information on the investigations into his campaign, would you give it to him?

Director WRAY. I'm not going to discuss the investigation in question with the President, much less provide information from that investigation to him.

Senator HARRIS. And if he wanted—if he received that information and wanted to declassify it, would he have the ability to do that, from your perspective?

Director WRAY. Information from the——

Senator HARRIS. However he received it, perhaps from members of the United States Congress.

Director WRAY. I think legally he would have that ability.

Senator HARRIS. Do you believe the President should recuse himself from reviewing and declassifying sensitive FBI material related to this investigation?

Director WRAY. I think recusal questions are something I would encourage the President to talk to the White House counsel about.

Senator HARRIS. Has the FBI done any kind of legal analysis on these questions?

Director WRAY. Well, happily, I'm no longer in the business of doing legal analysis. I now get to be a client and blame lawyers for things, instead of being the lawyer who gets blamed. So we have not done a legal analysis.

Senator HARRIS. Have you blamed any lawyers for their analysis of this issue?

Director WRAY. What's that?

Senator HARRIS. Have you blamed any lawyers for their analysis of this issue?

Director WRAY. I have not yet, no.

Senator HARRIS. Okay.

Is the FBI getting the cooperation it needs from social media companies to counter foreign adversaries' influence on our elections?

Director WRAY. I think the cooperation has been improving. I think we're continuing to work with the social media companies to try to see how we can raise their awareness, so that they can share information with us and vice versa. So I think things are moving in the right direction, but I think there's a lot of progress to be made.

Senator HARRIS. What more do you need from social media companies to improve the partnership that you'd like to have with them to counter these attacks?

Director WRAY. Well, I think we always like to have more information shared more quickly from their end. But I think from their perspective it's a dialogue. They're looking to get information from us about what it is we see, so that they can give responsive information. So I think we're working through those issues.

Senator HARRIS. Do you believe that the social media companies have enough employees that have the appropriate security clearance to make these partnerships real?

Director WRAY. That's not an issue I've evaluated, but I'm happy to take a look at it.

Senator HARRIS. Please do, and follow up with the Committee.

Director Coats, one of the things that makes guarding against foreign intelligence threats on social media so complex is that the threat originates overseas and so that would be within the jurisdiction of the CIA and the NSA, and then it comes to our shores and then it passes on to the FBI and also the social media companies themselves.

I'm not aware of any written IC strategy on how we would confront the threat to social media. Does such a strategy exist in writing?

Director COATS. I would have to get back with you on that. I'd be happy to look into it. From my perspective right now, a written strategy, specific strategy, is not in place, but I want to check on that.

Senator HARRIS. Please do follow up.

Also, last year Congress passed a bipartisan Russia sanctions bill. However, the Administration has not imposed those sanctions. From an intelligence perspective, what is your assessment of how Russia interprets the Administration's inaction?

Director COATS. I don't have information relative to what the Russian thinking is in terms of that particular specific reaction. There are other sanctions, as you know, that are being imposed on Russian oligarchs and others through the United Nations and through other things that have been done in reference to the JCPoA. But specifically on your question, I don't have an answer for that.

Director POMPEO. Senator Harris.

Senator HARRIS. Yes?

Director POMPEO. May I comment? I think we ought to look at that in a broader context. That is, how the Russians view all of the actions of this Administration, not just a particular set of sanctions or the absence thereof. So as we've watched the Russians respond to this Administration's decision to provide defensive weapons in Ukraine, to push back against Russian efforts in Syria, sanctions placed on Venezuela were directly in conflict with Russian interests, the list of places that the Russians are feeling the pain from this Administration's actions are long.

Senator HARRIS. But, Director Pompeo, I'm sure you would agree that in order to understand the full scope of effect it is also important that we analyze each discrete component, including what is the interpretation of this Administration's failure to enact the sanctions as has been passed and directed by the United States Congress in a bipartisan manner. Have you done that assessment?

Director POMPEO. Senator, in closed session I'll tell you what we know and don't know about that discrete issue.

Senator HARRIS. Right.

Director POMPEO. Yes, and I agree with you it is important to look at each one in its own place. But I think what we most often see in terms of Russian response, it's to the cumulative activities in response to Russian activities. That is how the United States responds to those, in a cumulative way.

Senator HARRIS. Thank you. I look forward to our conversation. Thank you.

Director POMPEO. Yes, ma'am.

Chairman BURR. Senator Cornyn.

Senator CORNYN. Director Coats, you alluded to the activities of transnational criminal organizations, and I'm thinking particularly as regards our neighbors down south of our border. Recently I heard somebody refer to the cartels, these transnational criminal organizations, as "commodity agnostic." In other words, they'll traffic in people, they'll traffic in drugs and other contraband, all in pursuit of money.

Director COATS. Whatever brings in the most dollars.

Senator CORNYN. Senator Manchin I know and others have alluded to their concern about—and certainly we all share the concern about the deaths and overdoses caused by drugs in America, much of which comes across our southern borders through our ports of entry. This week we're going to be considering border security measures as part of a larger package that the President has proposed while addressing the so-called "DACA recipients."

But, do you believe that modernizing our ports of entry and providing enhanced technology and other means to surveil, follow and

identify illegal drugs coming across our ports of entry would be a good thing for us to do?

Director COATS. I do. I do think that a layered approach is necessary to—it's clear that just one specific defense put in place is not going to solve the problem. It needs to be a layered interest of not only physical facilities, but also Border Patrol, also how those who arrive and perhaps dissipate in waiting for their court appearance, tracking them—a whole range of things that I think are going to be needed to stop that flow from coming in.

Senator CORNYN. I know it's been alluded to, but just to emphasize my concern with the demand side. Maybe we've given up—I hope not—in addressing the demand side, which of course provides the money and the incentive for these cartels to operate, and it's something I think deserves full attention and focus of the United States Government. I've heard General Kelly in his previous job at DHS talk about that, and I hope we will return to that focus as part of this layered approach, the demand side, because it's something I think that is maybe the hardest thing to deal with, but perhaps might have the greatest impact.

Director COATS. The supply depends on the demand and the demand drives the supply and provides the capital, with which to take extraordinary methods that bypass our defenses in order to get those drugs into the United States.

On the demand side, this is a whole of the American people process. It's PTA's. We growing up got these videos of driving in driver's training and the horrendous look at crashes and so forth and so on. We need to let every student know what the consequences of these drugs are to their lives and to their future. We need to get parents involved, parent-teacher associations involved, so whether they pick up their values from church or from the neighborhood or whatever.

This is a national crisis and we all of us here represent or are from states which are staggering through the process here of watching young people and others die from drugs that are more potent than they've ever been.

Senator CORNYN. Let me just lay down a couple of markers here in my comments, but then I want to end on CFIUS, the Committee on Foreign Investment in the United States.

I will join Senator Rubio and Senator King, Senator Lankford, and others concerned about the failure of the U.S. Government again to have an all-of-government strategy to deal with the cyber threat. I have no doubt in my mind that we have superior capabilities, but they're stovepiped. I don't think we, the policymakers, are doing a good enough job, and I think it's incumbent upon us to try to provide some policy guidance so that you and others in the intelligence community and the national security apparatus can address this threat in the way that it needs to be addressed.

Our adversaries don't suffer from a lack of an all-of-government policy. They are all over that. China, I agree with Senator Rubio about their strategy, and some of you have responded to that.

But one of the strategies that China and other countries have adopted is to avoid some of the review measures in the Committee on Foreign Investment in the United States when it comes to direct investment, buying those dual-use technologies, startup companies



and the like, and then using that to gain strategic advantage against the United States.

I wonder if maybe, Director Wray, could you address that; and then anybody else in the time permitted, I'd be glad to hear what you have to say about that.

Director WRAY. Senator, I think you're exactly right that CFIUS reform is particularly relevant to the China threat, although not exclusively China threat. And there is a degree to which CFIUS as it currently stands is susceptible too much to the kind of "round pegs only go in round holes" kind of thing. It's not hard to come up with other-shaped pegs to get around that process, the obvious example being joint ventures, but there are other ways as well. So that's one of the significant problems.

Another problem is the amount of time that's built into the process to do a thorough review, which is too short. Another problem is the inability to share information, since other countries, our allies, are going through the same thing, to be able to share information, so when they go through their own versions of the CFIUS process they have the benefit of what was attempted in our country, and vice versa.

I think in general we need to take a more strategic perspective on China's efforts to use acquisitions and other types of business ventures, as opposed to just a tactical, looking only within the four corners of one particular transaction.

General ASHLEY. If I could, the Director laid out really kind of the bigger issue at the strategic level and for us at DIA, we're kind of taking on the tactical. So we're the ones that are right about ready to penetrate the line. So if you look at supply chain risk management, we actually run the Threat Analysis Center that is hooked into CFIUS. So we bring the services together and look at supply chain risk management for CI issues associated with whom-ever may get a contract and ties back to China and other nations.

But you allude to the fact that every case for CFIUS comes back and we take a look at it. We get about three days with it. We could use more time to make a more thorough scrub.

Senator CORNYN. Thank you.

Chairman BURR. Thank you.

Senator REED.

Senator REED. Thank you, Mr. Chairman. I apologize for being late. We had a simultaneous hearing in the Armed Services Committee on SOCOM.

All morning, gentlemen, we've heard the story of Russia influencing our campaigns and indeed in the current campaign for the midterms. So let me begin with Mr. Wray and say: Has the President directed you and your agency to take specific actions to confront and blunt Russian influence activities that are ongoing?

Director WRAY. We're taking a lot of specific efforts to blunt—

Senator REED. Directed by the President?

Director WRAY. Not specifically directed by the President.

Senator REED. Director Pompeo, have you received a specific presidential direction to take steps to disrupt these activities?

Director POMPEO. I'm not sure how specific. The President's made very clear we have an obligation from our perspective, from a foreign intelligence perspective, to do everything we can to make

sure that there's a deep and thorough understanding of every threat, including threats from Russia.

Senator REED. But has he singled out the Russian threat, which appears to be critical to this election coming up? I know there are threats from many different vectors, but have you received a specific threat, i.e., it's very important to him to get this done correctly?

Director WRAY. Yes, I think the President's been very clear that he has asked our agency to cooperate with each of the investigations that's ongoing and do everything we can to ensure that we thoroughly understand this potential threat.

Senator REED. Director Coats, have you received a specific directive to take specific steps to disrupt, understand first and then disrupt, Russian activities directed at our elections on 2018?

Director COATS. I would echo what Director Pompeo just said. We work together on this throughout. The agency has full understanding that we are to provide whatever intelligence is relevant and make sure that that is passed on to our policymakers, including the President.

Senator REED. Passing on relevant intelligence is not actively disrupting the operations of an opponent. Do you agree?

Director COATS. No. We pass it on and they make the decision as to how to implement it.

Senator REED. As the Director of Intelligence, are you aware of or leading an inter-agency, an inter-governmental working group that is tasked with countering Russian activities? Not merely reporting on it, but tasked with countering those activities? Are you aware of any type of inter-agency group, any inter-governmental groups since State elections are critical or State elected officials are critical?

Director COATS. Well, we essentially are relying on the investigations that are under way, both with this Committee and the HPSCI Committee, as well as the Special Counsel.

Senator REED. So you're not taking any specific steps, based on the intelligence, to disrupt Russian activities that are occurring at this moment?

Director COATS. We take all kinds of steps to disrupt Russian activities in terms of what they're trying to do. I think I'll turn it over to Director Pompeo to—

Senator REED. Let me finish with the rest of the gentlemen. Are you finished, Mr. Coats, Director Coats?

Director COATS. Yes.

Senator REED. Thank you. Thank you.

Director POMPEO. Senator Reed, we have a significant effort. I'm happy to talk to you about it in closed session. The CIA—and it is not just our effort. It is a certainly all-of-IC effort—there may be others participating as well—to do our best to push back against this threat. It's not just the Russian threat. It's the Iranians and Chinese. It's a big, broad effort.

Senator REED. I understand, Mr. Director, we have mutual threats, but one threat that has been central. And you've testified to this publicly. The last election there was Russian influence. This election, they seem to be more prepared. They've learned their lessons. The simple question I pose is: Has the President directed the

intelligence community in a coordinated effort, not merely to report, but to actively stop this activity? The answer seems to be that I'm hearing is the reporting's going on, as we're reporting about every threat coming in to the United States.

Let me get back quickly. Do any of the other panelists have anything to add on this point?

Admiral ROGERS. For us, I can't say that I've been explicitly directed to, quote, "blunt" or actively stop. On the other hand, it's very clear, generate knowledge and insight, help us understand this so we can generate better policy. That clearly—that direction has been very explicit, in fairness.

Senator REED. But I think again—you may agree or disagree—collecting intelligence, then acting on it in a coordinated fashion, are two different things.

Admiral ROGERS. Yes, sir. I'd also argue, what's our role as intelligence professionals in all of this?

Senator REED. Let me just end. I've got very few moments remaining. We've talked a lot about China, CFIUS, and their involvement in trying to buy companies in the United States. What I think has to be pointed out, too, is they are undertaking significant national investment in artificial intelligence and quantum computing that is dwarfing anything that the Administration is proposing or suggesting.

If artificial intelligence has even half of the benefits that its promoters claim, it is going to be extraordinarily disruptive. Quantum computing has the capacity to undercut cryptology as we know it, and the experts can correct me if I'm wrong. Some of the mechanisms that quantum computing can generate could, based on infinite measurements of gravity, detect devices underground and under the water, which for anybody who's a submariner, you've got to be wondering.

So where is our national Manhattan program for AI and quantum computing that will match the Chinese? Director Coats, you seem to be anxious to answer that. I'll let you do that.

Director COATS. I think there are some things that we'll talk about in a classified setting here. We're treading a very narrow line here relative to discussing this in an open meeting.

Senator REED. I don't want to tread that line, but we do have to recognize that, again, the Chinese activity to appropriate our intellectual property is obvious. They are generating their own intellectual property at a rate that could be disruptive and we are not matching them. Again, this Manhattan analogy might be a little bit out of date, but when we saw the potential effects of a scientific development back in the forties, we spared no expense so that we would get it first before our opponents.

The Chinese seem to be making that type of commitment very publicly: hundreds of millions, billions of dollars. They've said publicly; they have a plan and they're working the plan.

Director COATS. And we provide that information to the extent that we can collect that information. But just like the Manhattan Project, we don't openly share what steps that we're taking to address it.

Senator REED. I respect that.

Thank you, Mr. Chairman.

Thank you, sir.

Chairman BURR. Thank you, Senator Reed, and I do hope you'll come back to the closed session if you can this afternoon. I think that you'll get some fidelity in that closed session.

I want to turn to—we're about to wrap up. Everybody can look up. There are no more questions, so you don't have to lose eye contact with us hoping you're not the guy that they're going to ask to answer.

[Laughter.]

You can tell who the newbies are. They've stayed focused on the Members the entire time; and the ones that have been here before have been like this (indicating.).

I want to turn to the Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman.

We look forward to seeing you all this afternoon. Robert, we hope to get some overhead questions to you this afternoon.

Echoing what we've all said, appreciate your service. But I think we're hearing again a lot of commonality as we think about cyber, misinformation, and disinformation. It really is asymmetrical.

One of the things that has struck me is that if you do a rough calculation and add up the costs to Russia in terms of their intervention in America, elections, the Dutch elections where they hand-counted all the ballots, the French elections where Facebook acknowledged taking down 30,00 sites. You add that all together, it's less than the cost of one new F-35 airplane. Pretty good bang for the buck.

I remember a year or so ago at Langley looking at some of our fighter technology, stealth technology, and the colonel showing me around bemoaning the fact that the Chinese had gotten this again on the cheap by stealing a lot of the intellectual property that underlies that technology.

Echoing what Senator Reed said—and again, I think this is where we all need to put our heads together—we just made a massive additional investment in DOD. We're at roughly ten times the size on our spend versus our near-peer adversaries like China and Russia. I do feel, not from a criticism standpoint, but more from just where we ought to be thinking about going forward, that we may be buying the best twentieth century military that money can buy, when we see our near-peer adversaries making these massive investments in areas like AI, machine learning, quantum computing. I think we all need to think through this from a general strategic standpoint.

I worry that we've got certain low-hanging fruit as we think about Chinese tech companies and how to get CFIUS right. One of the things some of us discussed with you in the past is, if you look simply at IoT-connected devices, we're going to double the number from about 10 billion to 20 billion in the next three to five years. Yet we have no even de minimis security requirements for the Federal Government purchasing of IoT devices.

I would—I know I've talked with General Ashley on this. I don't believe there is, even across the IC and DOD, prerequisite that before we buy some of these connected refrigerators or sensors or common consumer goods, that there be that patchability or no embedded passcodes.

So I think again there's a lot of work we can do, but we don't have the luxury of short time.

Senator Blunt raised some of the questions around election security. I know the Chairman's going to make this comment in his closing remarks. I think this Committee has done some very good bipartisan work in a series of areas that arose out of the Russia investigation. It's our hope that on election security we can come forward with a set of recommendations very quickly, because we have primaries coming up as early as March. My hope is that there will be able to be bipartisan legislation to try to start addressing this issue.

So thank you, gentlemen. I look forward to our session this afternoon. With that, I'll turn it over to the Chairman.

Chairman BURR. Thank you, Vice Chairman.

Admiral Rogers, I can't remember whether it was you or somebody else at the table said when we had a closed session about investment: It's not how much we spend; it's how we deploy the capital that we've devoted to a particular thing. I think as a general statement we get much better at the way we deploy capital, and I think we deploy it with a measurement tool today on return that's totally different than it was 10 and 20 and 30 years ago. I think that's important.

This Committee has a global mandate, a mandate that I think has been reflected, I think, in the statements and the questions of the Members of this Committee today. It's my hope that the American people got a sense of the breadth of topics this Committee deals with on a daily basis, and so do you.

What was unsaid today? What was unsaid is that the Special Counsel is not the only investigation that's going on in Washington. The scope of the Special Counsel's investigation was clearly stated by the DAG when he hired Bob Mueller. I think the media has spent some portion of every day trying to portray that the scope of that investigation has changed.

The truth is I don't know. I'm not sure that anybody in this room knows. But here's what I do know: I know the Senate Intel investigation continues. We're hopefully wrapping up some important areas that we have focused on. The Vice Chairman just alluded to the fact that it is our hope and our belief that before the primaries begin we intend to have an overview of our findings that will be public. We intend to have an open hearing on election security. And it's the Committee's intent to make recommendations that will enhance the likelihood that the security of our election process is in place.

In addition to that, our review of the ICA, the Intel Community Assessment which was done in December of 2016, we have reviewed in great detail, and we hope to report on what we found, to support the findings where it's appropriate, and to be critical if in fact we saw areas that we found came up short. We intend to make that public. To begin with, none of these would be without a declassification process, but we will have a public version that we air as quickly as we can.

The third piece is the review of when we learned of Russia's intrusions into our system, what we did or what we didn't do, and again with the intent of sharing as much of that with the American



public as we can find through open hearings and through an overview.

Lastly, we will continue to work towards conclusions related to any cooperation or collusion by any individual, campaign, or company with efforts to influence the outcome of elections or to create societal chaos in the United States.

I want to thank each of you at the table for an unprecedented access to intelligence products, legal documents, and other materials that were needed for us to do our job.

We have a very talented group of individuals who have conducted this investigation. The remarks of every individual who has come in before us has commented on their professionalism and the fact that at the end of eight hours they couldn't tell who was a Democrat and who was a Republican. So the effort to be bipartisan has not just been public; it is private as well, and permeates all the way down through our staff.

They couldn't do this in a timely fashion without the access that each of you have provided us and your agencies. Let me just reiterate again: We understand that this is an unprecedented access to this information.

I promised you when we started a year ago that the sensitive nature of that material would in fact be protected. The Vice Chairman and I have done everything in our power to do that. We think we have maintained that promise. There have been times where information has found its way out, some of recent, where it didn't come from us, but certainly have portrayed it did. And that's okay, because you know and we know the security measures we've got in place to protect the sensitivity of that material.

We have also protected the sensitivity of the individuals that have been interviewed, voluntarily. The individuals who have come in, what they've shared with us; to date we have not released any interview notes, because that's not for public consumption. We ask people to come in and share with us things that help us understand what happened. It's our responsibility to take that information and to put it into some form that furthers the American people's understanding and assurance that we have thoroughly reviewed this.

We will continue the promise that we made to each of you until the conclusion of this investigation and on. There are no expectations that everything you have shared with us is now a precedent that you have to continue. I hope it's not. I have said publicly, and criticized for it, that our Committee was created to operate in secrecy, I believe that's where we perform our best work, and we're given the opportunity and the need for the American people to have a better understanding, that we should provide that for them in as controlled an atmosphere as we do.

Today is an example of that, and we can now move from a public setting to a more private and closed setting to continue to get some clarity on some of the issues that our Members need.

I want you to understand the take-away here. The take-away is this Committee has and will continue to focus on answering the question that was given to this Committee from an investigation standpoint: What Russia did to influence the 2016 elections? There are efforts to expand our efforts. They are not internal. We realize

we have to answer for the American people: What did Russia do to mess with the 2016 elections?

Like many of you, on some of the questions when we've asked that were specific about it in public and in private, we find it's multi-jurisdictional. We've got to begin to sort that out for us, us the American people.

So I thank you for your willingness to be here today. I thank you for the performance of your employees, who have worked tirelessly with very little thanks, and of late with a lot of criticism, to keep this country safe, and I might say to keep other countries safe, because we are very generous when we know that bad things are going to happen.

The Committee is appreciative of the relationship that we have. We will continue to work to earn your trust, because that's the only way we can perform the type of oversight that we believe the Committee is mandated to do. And for the cooperation that each one of you provides us, we're grateful for that.

With this, this hearing's adjourned until a closed session at 2:30. [Whereupon, at 12:10 p.m., the hearing was adjourned.]

## **Supplemental Material**

**UNCLASSIFIED RESPONSES TO QUESTIONS FOR THE RECORD  
SENATE SELECT COMMITTEE ON INTELLIGENCE  
HEARING FEBRUARY 13, 2018**

Hearing Date: February 13, 2018  
 Committee: SSCI  
 Member: Sen. Rubio  
 Witnesses: Director Coats  
 Info Current as of: April 2, 2018

**Question:** The National Security Strategy of the United States emphasizes, “The United States also remains committed to supporting and advancing religious freedom.”

**What kind of violations and threats to religious freedom do you assess are threats to our national security? Which countries are the greatest offenders?**

**Answer:**

Most foreign government violations of religious freedom—from the persecution of small communities of Baha’is and Jehovah’s Witnesses in many countries to North Korean prohibitions against all faiths—can be categorized as human rights concerns that might create conditions for future harm to U.S. national security interests. More direct threats to U.S. interests primarily arise when religious repression fuels either the growth of anti-Western violent extremism or instability in a country, such as majority-Buddhist Burma’s crackdown on its population of 2 million Muslim Rohingya, which the United Nations and others have described as ethnic cleansing. Violations by governments against Muslims, for example, can bolster Islam-under-attack narratives that jihadist groups use to attract recruits and advance their agendas against the West and its partners. Government violations of religious freedom also can fuel societal intolerance against the targeted faiths, which in turn can lead to societal tensions, protests, political turmoil, or other forms of instability in a wide variety of places around the globe, including China and Western Europe.

- Among the governments that violate religious freedoms—Burma, China, Eritrea, Iran, North Korea, Saudi Arabia, Sudan, Tajikistan, Turkmenistan, and Uzbekistan—are designated by the Department of State as Countries of Particular Concern (CPC) for engaging in or tolerating “systematic, ongoing, and egregious” violations. In 2017, the U.S. Commission on International Religious Freedom (USCIRF) recommended designating Russia and Syria as CPCs and placed Egypt, Indonesia, and Malaysia on the second-highest tier of concern.
- Of the non-CPC countries, Egypt, Indonesia, Malaysia, Russia, and Syria ranked highest on the Pew Research Center’s most recent index of government violators compiled in December 2015. Sunni terrorist groups are internationally notorious for being among the more egregious violators of religious freedom globally.



Hearing Date: February 13, 2018  
Committee: SSCI  
Member: Sen. Rubio  
Witnesses: Director Coats  
Info Current as of: April 2, 2018

**Question:** The National Security Strategy of the United States emphasizes, “The United States also remains committed to supporting and advancing religious freedom.”

**What trends do you see regarding religious freedom violations, especially from governments justifying violations in the name of security or countering extremism?**

**Answer:**

The depth and breadth of religious freedom violations around the world varies from country to country but is historically elevated, according to diplomatic, UN, and other open-source reporting. The level of violations in the early and mid-1990s that spurred passage of the 1998 International Religious Freedom Act has since worsened, according to the USCIRF and other open-source reporting. Government restrictions on religious practice increased in all major regions of the world between 2007 and 2015, according to the Pew Research Center, while social hostilities and violations by nonstate actors also steadily increased in most regions. Department of State and USCIRF reporting highlights the growth in recent years of government violations of religious freedom tied to laws intended to counter terrorism or extremism.

Hearing Date: February 13, 2018  
Committee: SSCI  
Member: Sen. Wyden  
Witnesses: Director Coats  
Info Current as of: April 23, 2018

**Question:** Recent news reports indicate that the same Russian hackers who infiltrated the Democratic National Committee in 2016 and the German Bundestag in 2014 repeatedly targeted senior US government officials, defense contractors, and scientists through their personal email accounts. (AP, “‘Fancy Bear’ hackers took aim at US defense contractors,” February 7, 2018.)

**Do you believe there is a legitimate government interest in protecting the personal accounts and devices of government officials?**

**Answer:**

The personal accounts and devices of government officials can contain information that is useful for our adversaries to target, either directly or indirectly, these officials and the organizations with which they are affiliated.

Hearing Date: February 13, 2018  
Committee: SSCI  
Member: Sen. Wyden  
Witnesses: Director Coats  
Info Current as of: April 23, 2018

**Question:** Recent news reports indicate that the same Russian hackers who infiltrated the Democratic National Committee in 2016 and the German Bundestag in 2014 repeatedly targeted senior U.S. government officials, defense contractors, and scientists through their personal email accounts. (AP, “‘Fancy Bear’ hackers took aim at U.S. defense contractors,” February 7, 2018.)

**What resources do you need in order to ensure that these personal accounts and devices are not a vulnerable target for foreign intelligence services?**

**Answer:**

We have the resources we need to continue our respective education and awareness programs, which are the most important weapons in the cyber-battlefield when it comes to personal devices and accounts. We also need to continue to harden our government systems, both classified and unclassified, to prevent the potential compromise of a Government-issued personal device or account from becoming a major cyber-intrusion or cyber-success against our government networks or programs; I have made this a priority for the IC. If these programs require additional resources, I will inform this committee.

Hearing Date: February 13, 2018  
Committee: SSCI  
Member: Sen. Cotton  
Witnesses: Director Coats  
Info Current as of: March 29, 2018

**Question:** In 2017, the Director of the Central Intelligence Agency referred to WikiLeaks as a "non-state hostile intelligence service" that often aids U.S. adversaries like Russia and China. At my request, Chairman Burr and Vice-Chairman Warner included language to that effect in the FY17 Intelligence Authorization Act.

**Do you agree with Director Pompeo and this Committee that WikiLeaks is a non-state hostile intelligence service that often aids U.S. adversaries like Russia?**

**Answer:**

Yes, WikiLeaks should be viewed as a non-state hostile foreign intelligence entity whose actions, both individually and in collaboration with others, have caused harm to U.S. national security and interests.

84

Hearing Date: February 13, 2018  
Committee: SSCI  
Member: Sen. Heinrich  
Witnesses: Director Coats  
Info Current as of: April 23, 2018

**Question:** How long can personnel from the Executive Office of the President (EOP) hold an interim clearance before the clearance process is terminated and access suspended?

**Answer:**

Under Executive Order 12968 (EO 12968), where official functions must be performed prior to the completion of the investigation and adjudication process, temporary eligibility for access to classified information may be granted. EO 12968 imposes no time limit on temporary access.



85

Hearing Date: February 13, 2018  
Committee: SSCI  
Member: Sen. Heinrich  
Witnesses: Director Coats  
Info Current as of: April 23, 2018

**Question:** What accountability is there to the DNI, as the government's security executive agent, for the granting of interim security clearances generally, and the interim SCI clearances, specifically?

**Answer:**

While the DNI has policy and oversight responsibilities for Government personnel security programs and access to SCI, under authorities set forth in statute and Executive Order, Agency Heads are responsible for establishing and maintaining an effective program to ensure that temporary access to classified information by personnel is clearly consistent with the interest of national security. Agency Heads are responsible for following the DNI's policy guidance when granting such clearances.

86

Hearing Date: February 13, 2018  
Committee: SSCI  
Member: Sen. Heinrich  
Witnesses: Director Coats  
Info Current as of: April 23, 2018

**Question:** Has the DNI reviewed all the cases of interim access to SCI, both in the EOP and across the government?

**Answer:**

The DNI does not routinely review cases of interim access to SCI in the government. The DNI does not recommend temporary accesses be granted or denied in specific cases unless an Agency Head specifically requests guidance.

87

Hearing Date: February 13, 2018  
Committee: SSCI  
Member: Sen. Heinrich  
Witnesses: Director Coats  
Info Current as of: April 23, 2018

**Question:** Are personnel with interim access to SCI under a Continuous Evaluation protocol, and if so, who manages that?

**Answer:**

Personnel with interim access may be under Continuous Evaluation. Identification of the population covered by Continuous Evaluation is the responsibility of the Agency Head.

88

Hearing Date: February 13, 2018  
Committee: SSCI  
Member: Sen. Heinrich  
Witnesses: Director Coats  
Info Current as of: April 23, 2018

**Question:** Are there executive branch and EOP personnel who have held interim access to SCI for longer than one year, and if so, how many such personnel and in what agencies do they work?

**Answer:**

In terms of EOP interim SCI access, the best source of information would be EOP, and I would defer to them to address questions regarding EOP personnel with interim access to SCI.

89

Hearing Date: February 13, 2018  
 Committee: SSCI  
 Member: Sen. Harris  
 Witnesses: Director Coats  
 Info Current as of: April 16, 2018

**Question:** You have the authority to issue Intelligence Community Directives that establish policy across the IC. Your predecessor used that authority to establish specific duties to warn victims?

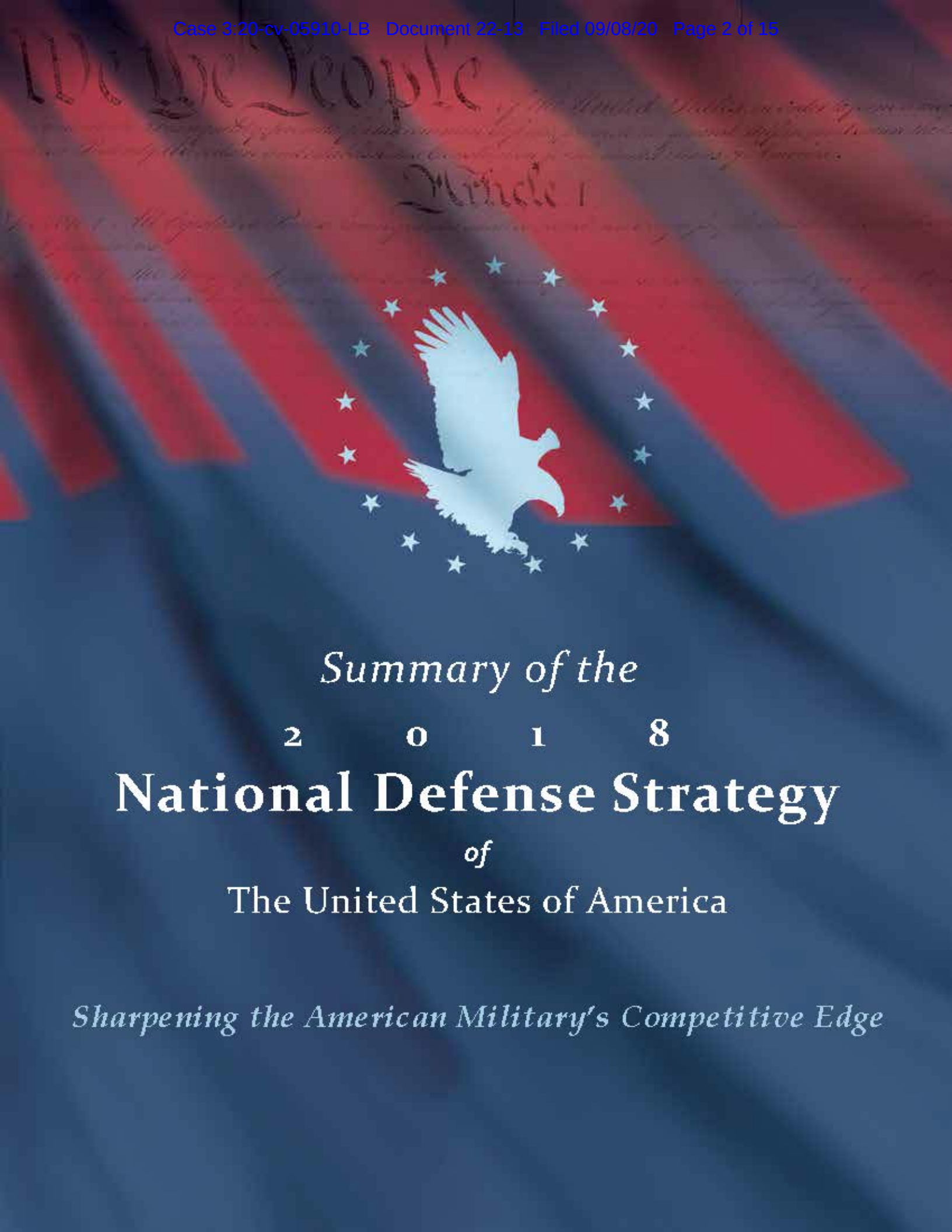
Will you commit to using that same authority to establish a specific duty to warn states about election related cybersecurity threats? If not, why not?

**Answer:**

We appreciate the importance of this issue, and the IC remains committed to warning our intelligence consumers about the wide range of serious threats facing the United States that are prioritized and disseminated commensurate with oversight by select committees for intelligence. We do not intend to issue a policy specifically establishing a duty to warn states about election-related cybersecurity threats. The referenced policy, ICD 191, *Duty to Warn*, was issued in 2015 directing IC elements to warn U.S. and non-U.S. persons of impending threats of intentional killing, serious bodily injury, or kidnapping. The Duty to Warn Directive was established to account for intelligence that, when encountered, would be acted upon in a time-sensitive manner directly by IC elements. We do have policies in place that were established to ensure the IC is providing intelligence information, at an appropriate clearance level, to support the Department of Homeland Security (DHS) and other Executive Branch agencies, as appropriate, in their ability to provide useful information to state, local, and tribal governments in a timely manner. The first of these policies, ICD 209, *Tearline Production and Dissemination*, was issued at the request of DHS to expand the utility of intelligence to a broad range of customers. The second Directive, ICD 208, *Write for Maximum Utility*, was issued to ensure intelligence products were written and disseminated in a manner that provides the greatest use for our customers. The IC will continue to support our customers by providing useful and timely intelligence information as appropriate.



# EXHIBIT 13



*Summary of the*  
**2 0 1 8**  
**National Defense Strategy**  
*of*  
**The United States of America**

*Sharpening the American Military's Competitive Edge*

**Table of Contents**

Introduction ..... 1

Strategic Environment ..... 2

Department of Defense Objectives ..... 4

Strategic Approach ..... 4

    Build a More Lethal Force ..... 5

    Strengthen Alliances and Attract New Partners ..... 8

    Reform the Department for Greater Performance and Affordability ..... 10

Conclusion ..... 11

NATIONAL DEFENSE STRATEGY

---

**INTRODUCTION**

The Department of Defense's enduring mission is to provide combat-credible military forces needed to deter war and protect the security of our nation. Should deterrence fail, the Joint Force is prepared to win. Reinforcing America's traditional tools of diplomacy, the Department provides military options to ensure the President and our diplomats negotiate from a position of strength.

Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding. We are facing increased global disorder, characterized by decline in the long-standing rules-based international order—creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security.

China is a strategic competitor using predatory economics to intimidate its neighbors while militarizing features in the South China Sea. Russia has violated the borders of nearby nations and pursues veto power over the economic, diplomatic, and security decisions of its neighbors. As well, North Korea's outlaw actions and reckless rhetoric continue despite United Nation's censure and sanctions. Iran continues to sow violence and remains the most significant challenge to Middle East stability. Despite the defeat of ISIS's physical caliphate, threats to stability remain as terrorist groups with long reach continue to murder the innocent and threaten peace more broadly.

This increasingly complex security environment is defined by rapid technological change, challenges from adversaries in every operating domain, and the impact on current readiness from the longest continuous stretch of armed conflict in our Nation's history. In this environment, there can be no complacency—we must make difficult choices and prioritize what is most important to field a lethal, resilient, and rapidly adapting Joint Force. America's military has no preordained right to victory on the battlefield.

This unclassified synopsis of the classified *2018 National Defense Strategy* articulates our strategy to compete, deter, and win in this environment. The reemergence of long-term strategic competition, rapid dispersion of technologies, and new concepts of warfare and competition that span the entire spectrum of conflict require a Joint Force structured to match this reality.

A more lethal, resilient, and rapidly innovating Joint Force, combined with a robust constellation of allies and partners, will sustain American influence and ensure favorable balances of power that safeguard the free and open international order. Collectively, our force posture, alliance and partnership architecture, and Department modernization will provide the capabilities and agility required to prevail in conflict and preserve peace through strength.

The costs of not implementing this strategy are clear. Failure to meet our defense objectives will result in decreasing U.S. global influence, eroding cohesion among allies and partners, and reduced access to markets that will contribute to a decline in our prosperity and standard of living. Without sustained and predictable investment to restore readiness and modernize our military to make it fit for our time, we will rapidly lose our military advantage, resulting in a Joint Force that has legacy systems irrelevant to the defense of our people.

---



NATIONAL DEFENSE STRATEGY

---

**STRATEGIC ENVIRONMENT**

The *National Defense Strategy* acknowledges an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations. These changes require a clear-eyed appraisal of the threats we face, acknowledgement of the changing character of warfare, and a transformation of how the Department conducts business.

The central challenge to U.S. prosperity and security is the *reemergence of long-term, strategic competition* by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations’ economic, diplomatic, and security decisions.

China is leveraging military modernization, influence operations, and predatory economics to coerce neighboring countries to reorder the Indo-Pacific region to their advantage. As China continues its economic and military ascendance, asserting power through an all-of-nation long-term strategy, it will continue to pursue a military modernization program that seeks Indo-Pacific regional hegemony in the near-term and displacement of the United States to achieve global preeminence in the future. The most far-reaching objective of this defense strategy is to set the military relationship between our two countries on a path of transparency and non-aggression.

Concurrently, Russia seeks veto authority over nations on its periphery in terms of their governmental, economic, and diplomatic decisions, to shatter the North Atlantic Treaty Organization and change European and Middle East security and economic structures to its favor. The use of emerging technologies to discredit and subvert democratic processes in Georgia, Crimea, and eastern Ukraine is concern enough, but when coupled with its expanding and modernizing nuclear arsenal the challenge is clear.

Another change to the strategic environment is a *resilient, but weakening, post-WWII international order*. In the decades after fascism’s defeat in World War II, the United States and its allies and partners constructed a free and open international order to better safeguard their liberty and people from aggression and coercion. Although this system has evolved since the end of the Cold War, our network of alliances and partnerships remain the backbone of global security. China and Russia are now undermining the international order from within the system by exploiting its benefits while simultaneously undercutting its principles and “rules of the road.”

Rogue regimes such as North Korea and Iran are destabilizing regions through their pursuit of nuclear weapons or sponsorship of terrorism. North Korea seeks to guarantee regime survival and increased leverage by seeking a mixture of nuclear, biological, chemical, conventional, and unconventional weapons and a growing ballistic missile capability to gain coercive influence over South Korea, Japan, and the United States. In the Middle East, Iran is competing with its neighbors, asserting an arc of influence and instability while vying for regional hegemony, using state-sponsored terrorist activities, a growing network of proxies, and its missile program to achieve its objectives.

Both revisionist powers and rogue regimes are competing across all dimensions of power. They have increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals.

---



NATIONAL DEFENSE STRATEGY

---

*Challenges to the U.S. military advantage* represent another shift in the global security environment. For decades the United States has enjoyed uncontested or dominant superiority in every operating domain. We could generally deploy our forces when we wanted, assemble them where we wanted, and operate how we wanted. Today, every domain is contested—air, land, sea, space, and cyberspace.

We face an ever more lethal and disruptive battlefield, combined across domains, and conducted at increasing speed and reach—from close combat, throughout overseas theaters, and reaching to our homeland. Some competitors and adversaries seek to optimize their targeting of our battle networks and operational concepts, while also using other areas of competition short of open warfare to achieve their ends (e.g., information warfare, ambiguous or denied proxy operations, and subversion). These trends, if unaddressed, will challenge our ability to deter aggression.

The security environment is also affected by *rapid technological advancements and the changing character of war*. The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed. New technologies include advanced computing, “big data” analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future.

New commercial technology will change society and, ultimately, the character of war. The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed. Maintaining the Department’s technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base.

States are the principal actors on the global stage, but *non-state actors* also threaten the security environment with increasingly sophisticated capabilities. Terrorists, trans-national criminal organizations, cyber hackers and other malicious non-state actors have transformed global affairs with increased capabilities of mass disruption. There is a positive side to this as well, as our partners in sustaining security are also more than just nation-states: multilateral organizations, non-governmental organizations, corporations, and strategic influencers provide opportunities for collaboration and partnership. Terrorism remains a persistent condition driven by ideology and unstable political and economic structures, despite the defeat of ISIS’s physical caliphate.

It is now undeniable that the *homeland is no longer a sanctuary*. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. New threats to commercial and military uses of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated.

Rogue regimes, such as North Korea, continue to seek out or develop *weapons of mass destruction* (WMD) – nuclear, chemical, and biological – as well as long range missile capabilities and, in some cases, proliferate these capabilities to malign actors as demonstrated by Iranian ballistic missile exports. Terrorists likewise continue to pursue WMD, while the spread of nuclear weapon technology and advanced manufacturing technology remains a persistent problem. Recent advances in bioengineering raise another concern, increasing the potential, variety, and ease of access to biological weapons.

---

NATIONAL DEFENSE STRATEGY

---

**DEPARTMENT OF DEFENSE OBJECTIVES**

In support of the *National Security Strategy*, the Department of Defense will be prepared to defend the homeland, remain the preeminent military power in the world, ensure the balances of power remain in our favor, and advance an international order that is most conducive to our security and prosperity.

Long-term strategic competitions with China and Russia are the principal priorities for the Department, and require both increased and sustained investment, because of the magnitude of the threats they pose to U.S. security and prosperity today, and the potential for those threats to increase in the future. Concurrently, the Department will sustain its efforts to deter and counter rogue regimes such as North Korea and Iran, defeat terrorist threats to the United States, and consolidate our gains in Iraq and Afghanistan while moving to a more resource-sustainable approach.

Defense objectives include:

- Defending the homeland from attack;
- Sustaining Joint Force military advantages, both globally and in key regions;
- Deterring adversaries from aggression against our vital interests;
- Enabling U.S. interagency counterparts to advance U.S. influence and interests;
- Maintaining favorable regional balances of power in the Indo-Pacific, Europe, the Middle East, and the Western Hemisphere;
- Defending allies from military aggression and bolstering partners against coercion, and fairly sharing responsibilities for common defense;
- Dissuading, preventing, or deterring state adversaries and non-state actors from acquiring, proliferating, or using weapons of mass destruction;
- Preventing terrorists from directing or supporting external operations against the United States homeland and our citizens, allies, and partners overseas;
- Ensuring common domains remain open and free;
- Continuously delivering performance with affordability and speed as we change Departmental mindset, culture, and management systems; and
- Establishing an unmatched twenty-first century National Security Innovation Base that effectively supports Department operations and sustains security and solvency.

**STRATEGIC APPROACH**

A long-term strategic competition requires the seamless integration of multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement, and military. More than any other nation, America can expand the competitive space, seizing the initiative to challenge our competitors where we possess advantages and they lack strength. A more lethal force, strong alliances and partnerships, American technological innovation, and a culture of performance will generate decisive and sustained U.S. military advantages.

---



NATIONAL DEFENSE STRATEGY

---

As we expand the competitive space, we continue to offer competitors and adversaries an outstretched hand, open to opportunities for cooperation but from a position of strength and based on our national interests. Should cooperation fail, we will be ready to defend the American people, our values, and interests. The willingness of rivals to abandon aggression will depend on their perception of U.S. strength and the vitality of our alliances and partnerships.

*Be strategically predictable, but operationally unpredictable.* Deterring or defeating long-term strategic competitors is a fundamentally different challenge than the regional adversaries that were the focus of previous strategies. Our strength and integrated actions with allies will demonstrate our commitment to deterring aggression, but our dynamic force employment, military posture, and operations must introduce unpredictability to adversary decision-makers. With our allies and partners, we will challenge competitors by maneuvering them into unfavorable positions, frustrating their efforts, precluding their options while expanding our own, and forcing them to confront conflict under adverse conditions.

*Integrate with U.S. interagency.* Effectively expanding the competitive space requires combined actions with the U.S. interagency to employ all dimensions of national power. We will assist the efforts of the Departments of State, Treasury, Justice, Energy, Homeland Security, Commerce, USAID, as well as the Intelligence Community, law enforcement, and others to identify and build partnerships to address areas of economic, technological, and informational vulnerabilities.

*Counter coercion and subversion.* In competition short of armed conflict, revisionist powers and rogue regimes are using corruption, predatory economic practices, propaganda, political subversion, proxies, and the threat or use of military force to change facts on the ground. Some are particularly adept at exploiting their economic relationships with many of our security partners. We will support U.S. interagency approaches and work by, with, and through our allies and partners to secure our interests and counteract this coercion.

*Foster a competitive mindset.* To succeed in the emerging security environment, our Department and Joint Force will have to out-think, out-maneuver, out-partner, and out-innovate revisionist powers, rogue regimes, terrorists, and other threat actors.

We will expand the competitive space while pursuing three distinct lines of effort:

- First, rebuilding military readiness as we build a more lethal Joint Force;
- Second, strengthening alliances as we attract new partners; and
- Third, reforming the Department's business practices for greater performance and affordability.

**Build a More Lethal Force**

The surest way to prevent war is to be prepared to win one. Doing so requires a competitive approach to force development and a consistent, multiyear investment to restore warfighting readiness and field a lethal force. The size of our force matters. The Nation must field sufficient, capable forces to defeat enemies and achieve sustainable outcomes that protect the American people and our vital interests. Our aim is a Joint Force that possesses decisive advantages for any likely conflict, while remaining proficient across the entire spectrum of conflict.

---

## NATIONAL DEFENSE STRATEGY

---

*Prioritize preparedness for war.* Achieving peace through strength requires the Joint Force to deter conflict through preparedness for war. During normal day-to-day operations, the Joint Force will sustainably compete to: deter aggression in three key regions—the Indo-Pacific, Europe, and Middle East; degrade terrorist and WMD threats; and defend U.S. interests from challenges below the level of armed conflict. In wartime, the fully mobilized Joint Force will be capable of: defeating aggression by a major power; deterring opportunistic aggression elsewhere; and disrupting imminent terrorist and WMD threats. During peace or in war, the Joint Force will deter nuclear and non-nuclear strategic attacks and defend the homeland. To support these missions, the Joint Force must gain and maintain information superiority; and develop, strengthen, and sustain U.S. security relationships.

*Modernize key capabilities.* We cannot expect success fighting tomorrow's conflicts with yesterday's weapons or equipment. To address the scope and pace of our competitors' and adversaries' ambitions and capabilities, we must invest in modernization of key capabilities through sustained, predictable budgets. Our backlog of deferred readiness, procurement, and modernization requirements has grown in the last decade and a half and can no longer be ignored. We will make targeted, disciplined increases in personnel and platforms to meet key capability and capacity needs. The *2018 National Defense Strategy* underpins our planned fiscal year 2019-2023 budgets, accelerating our modernization programs and devoting additional resources in a sustained effort to solidify our competitive advantage.

- *Nuclear forces.* The Department will modernize the nuclear triad—including nuclear command, control, and communications, and supporting infrastructure. Modernization of the nuclear force includes developing options to counter competitors' coercive strategies, predicated on the threatened use of nuclear or strategic non-nuclear attacks.
  - *Space and cyberspace as warfighting domains.* The Department will prioritize investments in resilience, reconstitution, and operations to assure our space capabilities. We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations.
  - *Command, control, communications, computers and intelligence, surveillance, and reconnaissance (C4ISR).* Investments will prioritize developing resilient, survivable, federated networks and information ecosystems from the tactical level up to strategic planning. Investments will also prioritize capabilities to gain and exploit information, deny competitors those same advantages, and enable us to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks.
  - *Missile defense.* Investments will focus on layered missile defenses and disruptive capabilities for both theater missile threats and North Korean ballistic missile threats.
  - *Joint lethality in contested environments.* The Joint Force must be able to strike diverse targets inside adversary air and missile defense networks to destroy mobile power-projection platforms. This will include capabilities to enhance close combat lethality in complex terrain.
  - *Forward force maneuver and posture resilience.* Investments will prioritize ground, air, sea, and space forces that can deploy, survive, operate, maneuver, and regenerate in all domains while under attack. Transitioning from large, centralized, unhardened infrastructure to smaller, dispersed, resilient, adaptive basing that include active and passive defenses will also be prioritized.
-



NATIONAL DEFENSE STRATEGY

---

- *Advanced autonomous systems.* The Department will invest broadly in military application of autonomy, artificial intelligence, and machine learning, including rapid application of commercial breakthroughs, to gain competitive military advantages.
- *Resilient and agile logistics.* Investments will prioritize prepositioned forward stocks and munitions, strategic mobility assets, partner and allied support, as well as non-commercially dependent distributed logistics and maintenance to ensure logistics sustainment while under persistent multi-domain attack.

*Evolve innovative operational concepts.* Modernization is not defined solely by hardware; it requires change in the ways we organize and employ forces. We must anticipate the implications of new technologies on the battlefield, rigorously define the military problems anticipated in future conflict, and foster a culture of experimentation and calculated risk-taking. We must anticipate how competitors and adversaries will employ new operational concepts and technologies to attempt to defeat us, while developing operational concepts to sharpen our competitive advantages and enhance our lethality.

*Develop a lethal, agile, and resilient force posture and employment.* Force posture and employment must be adaptable to account for the uncertainty that exists in the changing global strategic environment. Much of our force employment models and posture date to the immediate post-Cold War era, when our military advantage was unchallenged and the primary threats were rogue regimes.

- *Dynamic Force Employment.* Dynamic Force Employment will prioritize maintaining the capacity and capabilities for major combat, while providing options for proactive and scalable employment of the Joint Force. A modernized Global Operating Model of combat-credible, flexible theater postures will enhance our ability to compete and provide freedom of maneuver during conflict, providing national decision-makers with better military options.

The global strategic environment demands increased strategic flexibility and freedom of action. The Dynamic Force Employment concept will change the way the Department uses the Joint Force to provide proactive and scalable options for priority missions. Dynamic Force Employment will more flexibly use ready forces to shape proactively the strategic environment while maintaining readiness to respond to contingencies and ensure long-term warfighting readiness.

- *Global Operating Model.* The Global Operating Model describes how the Joint Force will be postured and employed to achieve its competition and wartime missions. Foundational capabilities include: nuclear; cyber; space; C4ISR; strategic mobility, and counter WMD proliferation. It comprises four layers: contact, blunt, surge, and homeland. These are, respectively, designed to help us compete more effectively below the level of armed conflict; delay, degrade, or deny adversary aggression; surge war-winning forces and manage conflict escalation; and defend the U.S. homeland.

*Cultivate workforce talent.* Recruiting, developing, and retaining a high-quality military and civilian workforce is essential for warfighting success. Cultivating a lethal, agile force requires more than just new technologies and posture changes; it depends on the ability of our warfighters and the Department workforce to integrate new capabilities, adapt warfighting approaches, and change

---



NATIONAL DEFENSE STRATEGY

---

business practices to achieve mission success. The creativity and talent of the American warfighter is our greatest enduring strength, and one we do not take for granted.

- *Professional Military Education (PME).* PME has stagnated, focused more on the accomplishment of mandatory credit at the expense of lethality and ingenuity. We will emphasize intellectual leadership and military professionalism in the art and science of warfighting, deepening our knowledge of history while embracing new technology and techniques to counter competitors. PME will emphasize independence of action in warfighting concepts to lessen the impact of degraded/lost communications in combat. PME is to be used as a strategic asset to build trust and interoperability across the Joint Forces and with allied and partner forces.
- *Talent management.* Developing leaders who are competent in national-level decision-making requires broad revision of talent management among the Armed Services, including fellowships, civilian education, and assignments that increase understanding of interagency decision-making processes, as well as alliances and coalitions.
- *Civilian workforce expertise.* A modern, agile, information-advantaged Department requires a motivated, diverse, and highly skilled civilian workforce. We will emphasize new skills and complement our current workforce with information experts, data scientists, computer programmers, and basic science researchers and engineers—to use information, not simply manage it. The Department will also continue to explore streamlined, non-traditional pathways to bring critical skills into service, expanding access to outside expertise, and devising new public-private partnerships to work with small companies, start-ups, and universities.

**Strengthen Alliances and Attract New Partners**

Mutually beneficial alliances and partnerships are crucial to our strategy, providing a durable, asymmetric strategic advantage that no competitor or rival can match. This approach has served the United States well, in peace and war, for the past 75 years. Our allies and partners came to our aid after the terrorist attacks on 9/11, and have contributed to every major U.S.-led military engagement since. Every day, our allies and partners join us in defending freedom, deterring war, and maintaining the rules which underwrite a free and open international order.

By working together with allies and partners we amass the greatest possible strength for the long-term advancement of our interests, maintaining favorable balances of power that deter aggression and support the stability that generates economic growth. When we pool resources and share responsibility for our common defense, our security burden becomes lighter. Our allies and partners provide complementary capabilities and forces along with unique perspectives, regional relationships, and information that improve our understanding of the environment and expand our options. Allies and partners also provide access to critical regions, supporting a widespread basing and logistics system that underpins the Department's global reach.

We will strengthen and evolve our alliances and partnerships into an extended network capable of deterring or decisively acting to meet the shared challenges of our time. We will focus on three elements for achieving a capable alliance and partnership network:

## NATIONAL DEFENSE STRATEGY

- 
- *Uphold a foundation of mutual respect, responsibility, priorities, and accountability.* Our alliances and coalitions are built on free will and shared responsibilities. While we will unapologetically represent America's values and belief in democracy, we will not seek to impose our way of life by force. We will uphold our commitments and we expect allies and partners to contribute an equitable share to our mutually beneficial collective security, including effective investment in modernizing their defense capabilities. We have shared responsibilities for resisting authoritarian trends, contesting radical ideologies, and serving as bulwarks against instability.
  - *Expand regional consultative mechanisms and collaborative planning.* We will develop new partnerships around shared interests to reinforce regional coalitions and security cooperation. We will provide allies and partners with a clear and consistent message to encourage alliance and coalition commitment, greater defense cooperation, and military investment.
  - *Deepen interoperability.* Each ally and partner is unique. Combined forces able to act together coherently and effectively to achieve military objectives requires interoperability. Interoperability is a priority for operational concepts, modular force elements, communications, information sharing, and equipment. In consultation with Congress and the Department of State, the Department of Defense will prioritize requests for U.S. military equipment sales, accelerating foreign partner modernization and ability to integrate with U.S. forces. We will train to high-end combat missions in our alliance, bilateral, and multinational exercises.

Enduring coalitions and long-term security partnerships, underpinned by our bedrock alliances and reinforced by our allies' own webs of security relationships, remain a priority:

- *Expand Indo-Pacific alliances and partnerships.* A free and open Indo-Pacific region provides prosperity and security for all. We will strengthen our alliances and partnerships in the Indo-Pacific to a networked security architecture capable of deterring aggression, maintaining stability, and ensuring free access to common domains. With key countries in the region, we will bring together bilateral and multilateral security relationships to preserve the free and open international system.
  - *Fortify the Trans-Atlantic NATO Alliance.* A strong and free Europe, bound by shared principles of democracy, national sovereignty, and commitment to Article 5 of the North Atlantic Treaty is vital to our security. The alliance will deter Russian adventurism, defeat terrorists who seek to murder innocents, and address the arc of instability building on NATO's periphery. At the same time, NATO must adapt to remain relevant and fit for our time—in purpose, capability, and responsive decision-making. We expect European allies to fulfill their commitments to increase defense and modernization spending to bolster the alliance in the face of our shared security concerns.
  - *Form enduring coalitions in the Middle East.* We will foster a stable and secure Middle East that denies safe havens for terrorists, is not dominated by any power hostile to the United States, and that contributes to stable global energy markets and secure trade routes. We will develop enduring coalitions to consolidate gains we have made in Afghanistan, Iraq, Syria, and elsewhere, to support the lasting defeat of terrorists as we sever their sources of strength and counterbalance Iran.
  - *Sustain advantages in the Western Hemisphere.* The U.S. derives immense benefit from a stable, peaceful hemisphere that reduces security threats to the homeland. Supporting the U.S. interagency lead,
-



## NATIONAL DEFENSE STRATEGY

---

the Department will deepen its relations with regional countries that contribute military capabilities to shared regional and global security challenges.

- *Support relationships to address significant terrorist threats in Africa.* We will bolster existing bilateral and multilateral partnerships and develop new relationships to address significant terrorist threats that threaten U.S. interests and contribute to challenges in Europe and the Middle East. We will focus on working by, with, and through local partners and the European Union to degrade terrorists; build the capability required to counter violent extremism, human trafficking, trans-national criminal activity, and illegal arms trade with limited outside assistance; and limit the malign influence of non-African powers.

### **Reform the Department for Greater Performance and Affordability**

The current bureaucratic approach, centered on exacting thoroughness and minimizing risk above all else, is proving to be increasingly unresponsive. We must transition to a culture of performance where results and accountability matter. We will put in place a management system where leadership can harness opportunities and ensure effective stewardship of taxpayer resources. We have a responsibility to gain full value from every taxpayer dollar spent on defense, thereby earning the trust of Congress and the American people.

*Deliver performance at the speed of relevance.* Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting. Current processes are not responsive to need; the Department is over-optimized for exceptional performance at the expense of providing timely decisions, policies, and capabilities to the warfighter. Our response will be to prioritize speed of delivery, continuous adaptation, and frequent modular upgrades. We must not accept cumbersome approval chains, wasteful applications of resources in uncompetitive space, or overly risk-averse thinking that impedes change. Delivering performance means we will shed outdated management practices and structures while integrating insights from business innovation.

*Organize for innovation.* The Department's management structure and processes are not written in stone, they are a means to an end—empowering the warfighter with the knowledge, equipment and support systems to fight and win. Department leaders will adapt their organizational structures to best support the Joint Force. If current structures hinder substantial increases in lethality or performance, it is expected that Service Secretaries and Agency heads will consolidate, eliminate, or restructure as needed. The Department's leadership is committed to changes in authorities, granting of waivers, and securing external support for streamlining processes and organizations.

*Drive budget discipline and affordability to achieve solvency.* Better management begins with effective financial stewardship. The Department will continue its plan to achieve full auditability of all its operations, improving its financial processes, systems, and tools to understand, manage, and improve cost. We will continue to leverage the scale of our operations to drive greater efficiency in procurement of materiel and services while pursuing opportunities to consolidate and streamline contracts in areas such as logistics, information technology, and support services. We will also continue efforts to reduce management overhead and the size of headquarters staff. We will reduce or eliminate duplicative organizations and systems for managing human resources, finance, health services, travel, and supplies. The Department will also work to reduce excess property and infrastructure, providing Congress with options for a Base Realignment and Closure.

---

NATIONAL DEFENSE STRATEGY

---

*Streamline rapid, iterative approaches from development to fielding.* A rapid, iterative approach to capability development will reduce costs, technological obsolescence, and acquisition risk. The Department will realign incentive and reporting structures to increase speed of delivery, enable design tradeoffs in the requirements process, expand the role of warfighters and intelligence analysis throughout the acquisitions process, and utilize non-traditional suppliers. Prototyping and experimentation should be used prior to defining requirements and commercial-off-the-shelf systems. Platform electronics and software must be designed for routine replacement instead of static configurations that last more than a decade. This approach, a major departure from previous practices and culture, will allow the Department to more quickly respond to changes in the security environment and make it harder for competitors to offset our systems.

*Harness and protect the National Security Innovation Base.* The Department's technological advantage depends on a healthy and secure national security innovation base that includes both traditional and non-traditional defense partners. The Department, with the support of Congress, will provide the defense industry with sufficient predictability to inform their long-term investments in critical skills, infrastructure, and research and development. We will continue to streamline processes so that new entrants and small-scale vendors can provide cutting-edge technologies. We will also cultivate international partnerships to leverage and protect partner investments in military capabilities.

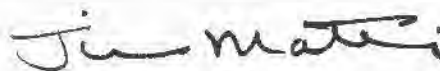
## CONCLUSION

This strategy establishes my intent to pursue urgent change at significant scale.

We must use creative approaches, make sustained investment, and be disciplined in execution to field a Joint Force fit for our time, one that can compete, deter, and win in this increasingly complex security environment. A dominant Joint Force will protect the security of our nation, increase U.S. influence, preserve access to markets that will improve our standard of living, and strengthen cohesion among allies and partners.

While any strategy must be adaptive in execution, this summary outlines what we must do to pass intact to the younger generation the freedoms we currently enjoy. But there is nothing new under the sun: while this strategy will require sustained investment by the American people, we recall past generations who made harsher sacrifices so that we might enjoy our way of life today.

As it has for generations, free men and women in America's military will fight with skill and valor to protect us. To carry out any strategy, history teaches us that wisdom and resources must be sufficient. I am confident this defense strategy is appropriate and worthy of the support of the American people.



Jim Mattis



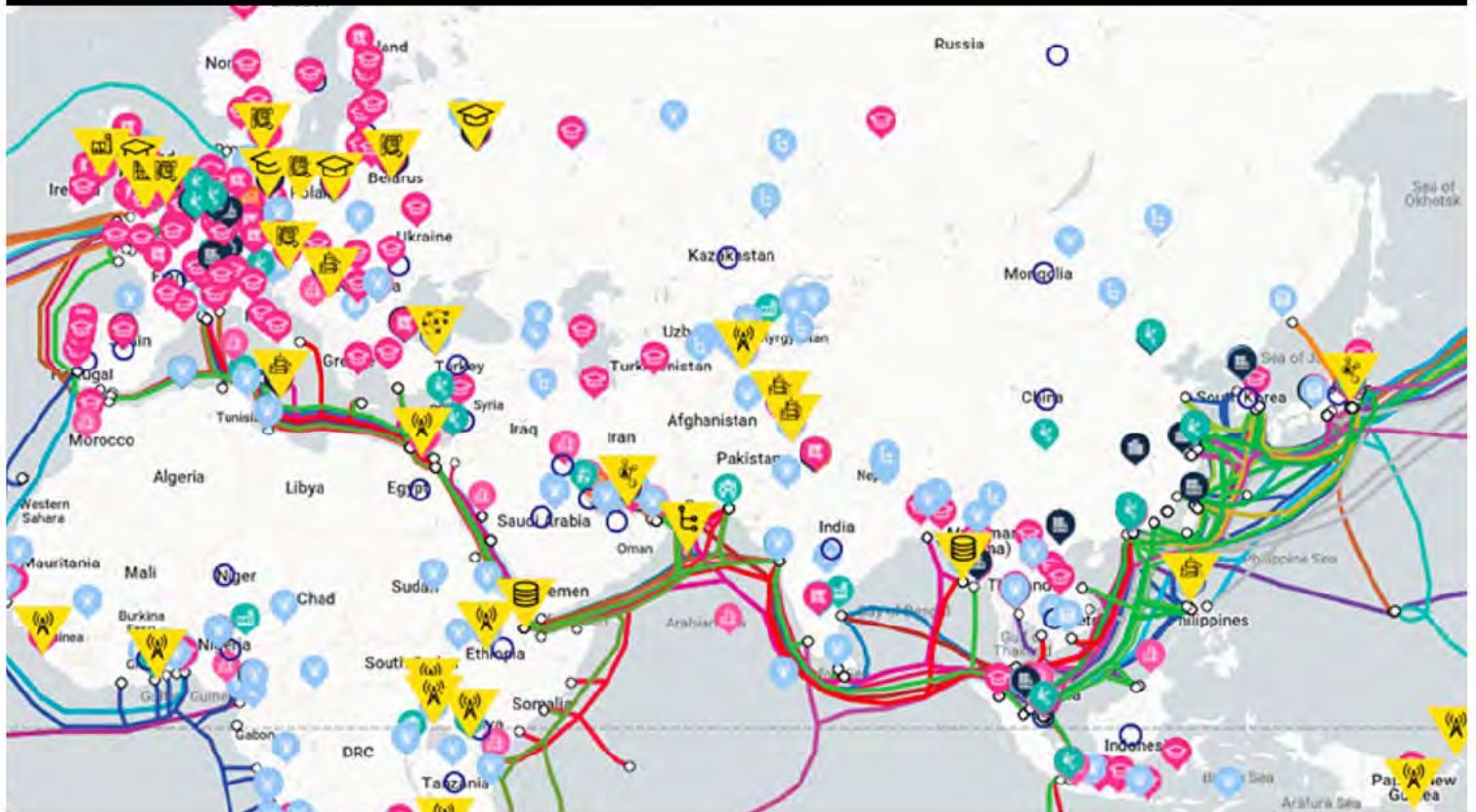




# EXHIBIT 14

# Mapping China's technology giants

Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan and Elise Thomas



## About the authors

**Danielle Cave** is Deputy Head of ASPI's International Cyber Policy Centre.

**Dr Samantha Hoffman** is a Fellow at the International Cyber Policy Centre.

**Alex Joske** is a Researcher working with the International Cyber Policy Centre.

**Fergus Ryan** is an Analyst working with International Cyber Policy Centre.

**Elise Thomas** is a Researcher working with the International Cyber Policy Centre.

## What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

## ASPI International Cyber Policy Centre

The ASPI International Cyber Policy Centre's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia-Pacific.

The work of ICPC would be impossible without the financial support of our partners and sponsors across government, industry and civil society. ASPI is grateful to the US State Department for providing funding for this research project.

## Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

## ASPI

Tel +61 2 6270 5100

Fax + 61 2 6273 9566

Email [enquiries@aspi.org.au](mailto:enquiries@aspi.org.au)

[www.aspi.org.au](http://www.aspi.org.au)

[www.aspistrategist.org.au](http://www.aspistrategist.org.au)

[www.aspi.org.au/icpc/home](http://www.aspi.org.au/icpc/home)

[facebook.com/ASPI.org](https://www.facebook.com/ASPI.org)

[@ASPI\\_ICPC](https://twitter.com/ASPI_ICPC)

© The Australian Strategic Policy Institute Limited 2019

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers. Notwithstanding the above, educational institutions (including schools, independent colleges, universities and IAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from ASPI and free of charge.

First published April 2019

**Cover image:** This image is from ASPI's China's tech giants website: <https://chinatechmap.aspi.org.au/>. ASPI's International Cyber Policy Centre allows this image to be republished under the Creative Commons License Attribution-Share Alike. The site can also be embedded into other websites via the menu tab.

# Mapping China's technology giants

Danielle Cave, Samantha Hoffman, Alex Joske,  
Fergus Ryan and Elise Thomas



# Contents

<b>Executive summary</b>	<b>03</b>
<b>Introduction</b>	<b>04</b>
<b>The database</b>	<b>05</b>
<b>Methodology</b>	<b>06</b>
<b>China's tech firms &amp; the CCP</b>	<b>07</b>
<b>Enabling &amp; exporting digital authoritarianism</b>	<b>08</b>
Surveillance cities: Huawei's 'smart cities' projects	10
Censorship and suppression: aiding authoritarianism in Zimbabwe	11
National ID programs: Venezuela's 'Fatherland Card'	12
Shaping politics and policy in Belarus	13
Controlling information flows—WeChat and the future of social messaging	14
<b>Enabling human rights abuses in China: Uyghurs in Xinjiang</b>	<b>16</b>
<b>Future strategic implications</b>	<b>17</b>
<b>Conclusion</b>	<b>19</b>
<b>Notes</b>	<b>20</b>
<b>Acronyms and abbreviations</b>	<b>23</b>



## Executive summary

Chinese technology companies are becoming increasingly important and dynamic actors on the world stage. They're making important contributions in a range of areas, from cutting-edge research to connectivity for developing countries, but their growing influence also brings a range of strategic considerations. The close relationship between these companies and the Chinese Communist Party (CCP) raises concerns about whether they may be being used to further the CCP's strategic and geopolitical interests.

The CCP has made no secret about its intentions to export its vision for the global internet. Officials from the Cyber Administration of China have written about the need to develop controls so that 'the party's ideas always become the strongest voice in cyberspace.'<sup>1</sup> This includes enhancing the 'global influence of internet companies like Alibaba, Tencent, Baidu [and] Huawei' and striving 'to push China's proposition of internet governance toward becoming an international consensus'.

Given the explicitly stated goals of the CCP, and given that China's internet and technology companies have been reported to have the highest proportion of internal CCP party committees within the business sector,<sup>2</sup> it's clear these companies are not purely commercial actors.

ASPI's International Cyber Policy Centre has created a public database to map the global expansion of 12 key Chinese technology companies. The aim is to promote a more informed debate about the growth of China's tech giants and to highlight areas where this expansion is leading to political and geostrategic dilemmas. It's a tool for journalists, researchers, policymakers and others to use to understand the enormous scale and complexity of China's tech companies' global reach. The dataset is inevitably incomplete, and we invite interested users to help make it more comprehensive by submitting new data through the online platform.

Our research maps and tracks:

- 17,000+ data points that have helped to geo-locate 1700+ points of overseas presence for these 12 companies;
- 404 University and research partnerships including 195+ Huawei Seeds for the Future university partnerships;
- 75 'Smart City' or 'Public Security Solution' projects, most of which are in Europe, South America and Africa;
- 52 5G initiatives, across 34 countries;
- 119 R&D labs, the greatest concentration of which are in Europe;
- 56 undersea cables, 31 leased cable and 17 terrestrial cables;
- 202 data centres and 305 telecommunications & ICT projects spread across the world.



## Introduction

China's technology, internet and telecommunications companies are among the world's largest and most innovative. They're highly competitive, and many are leaders in research and development. They've played a central role in bringing the benefits of modern technology to hundreds of millions of people, particularly in the developing world.

As a function of their increasingly global scale and scope, China's tech giants can exert increasing levels of influence over industries and governments around the world. The close relationship between Chinese companies and the Chinese Communist Party (CCP) means that the expansion of China's tech giants is about more than commerce.

A key research question includes: What are the geostrategic, political and human rights implications of this expansion? By mapping the global expansion of 12 of China's largest and most influential technology companies, across a range of sectors, this project contributes new data and analysis to help answer such questions.

All Chinese companies are subject to China's increasingly stringent security, intelligence, counter-espionage and cybersecurity laws.<sup>3</sup> That includes, for example, requirements in the CCP constitution<sup>4</sup> for any enterprise with three or more full party members to host internal party committees, a clause in the Company Law<sup>5</sup> that requires companies to provide for party activity to take place, and a requirement in the National Intelligence Law to cooperate in and conceal involvement in intelligence work.<sup>6</sup>

Several of the companies included in this research are also directly complicit in human rights abuses in China, including the reported detention of up to 1.5 million Uyghur Muslims in Xinjiang.<sup>7</sup> From communications monitoring to facial recognition that enables precise and pervasive surveillance, advanced technology—from these and other companies—is crucial to the increasingly inescapable surveillance net that the CCP has created for some Chinese citizens.

Every year since 2015, China has ranked last in the annual Freedom on the Net Index.<sup>8</sup> The CCP has made no secret of its desire to export its concepts of internet and information 'sovereignty',<sup>9</sup> as well as cyber censorship,<sup>10</sup> around the world.<sup>11</sup> Consistent with that directive, this research shows that Chinese companies are playing a role in aiding surveillance and providing sophisticated public security technologies and expertise to authoritarian regimes and developing countries that face challenges to their political stability, governance and rule of law.

In conducting this research, ASPI's International Cyber Policy Centre (ICPC) has used open-source information in English and Chinese to track the international operations and investments of 12 major Chinese technology companies: Huawei, ZTE, Tencent, Baidu, China Electronics Technology Group Corporation (CETC), Alibaba, China Mobile, China Telecom, China Unicom, Wuxi, Hikvision and BGI.

This research has been compiled in an online database that ICPC is making freely accessible to the public. While it contains more than 1,700 projects and more than 17,000 data points, it's not exhaustive. We welcome and encourage members of the public to help us make this dataset more complete by [submitting data via the website](#).

## The database

Throughout 2018, ICPC received frequent questions from media and stakeholders about the international activities of Chinese technology companies; for example, about Huawei's operations in particular regions or how widespread the use of Baidu or WeChat is outside of China.

These were always difficult questions to answer, as there's a lack of publicly available quantitative and qualitative data, and some of these companies disclose little in the way of policies that affect data, security, privacy, freedom of expression and censorship. What information is available is spread across a wide range of sources and hasn't been compiled. In-depth analysis of the available sources also requires Chinese-language capabilities, an understanding of Chinese state financing structures, and the use of internet archiving services as web pages are moved, altered or even deleted.

A further impediment to transparency is that Chinese media are under increasing control from the CCP and publish few investigative reports, which severely limits the available pool of media sources. The global expansion and influence of US internet companies, particularly Facebook, for example, has rightly received substantial attention and scrutiny over the past few years. Much of that scrutiny has come from, and will continue to come from, independent media, academia and civil society. However, the same scrutiny is often lacking when it comes to Chinese tech and social media companies.

The sheer capacity of China's giant tech companies, their reach and influence, and the unique party-state environment that shapes, limits and drives their global behaviour set them apart from other large technology companies expanding around the world.

This project seeks to:

1. Analyse the global expansion of a key sample of China's tech giants by mapping their major points of overseas presence.
2. Provide the public with an analysis of the governance structures and party-state politics from which those companies have emerged and with which they're deeply entwined.

## Methodology

To fill this research gap, ICPC sought to create an interactive global database to provide policymakers, academics, journalists, government officials and other interested readers with a more holistic picture of the increasingly global reach of China's tech giants.

A complete mapping of all Chinese technology companies globally would be impossible within the confines of our research. ICPC has therefore selected 12 companies from across China's telecommunications, technology, internet and biotech sectors:

- Alibaba
- Baidu
- BGI
- China Electronics Technology Group (CETC)
- China Mobile
- China Telecom
- China Unicom
- Hikvision (a subsidiary of CETC)
- Huawei
- Tencent
- Wuxi
- ZTE.

This dataset will continue to be updated during 2019. This research relied on open-source information in English and Chinese. This has included company websites, corporate information, tenders, media reporting, databases and other public sources.

The size and complexity of these companies, and the speed at which they're expanding, means this dataset will inevitably be incomplete. For that reason, we encourage researchers, journalists, experts and members of the public to contribute and submit data via the online platform in order to help make the dataset more complete over time.



## China's tech firms & the CCP

The CCP's influence and reach into private companies has increased sharply over the past decade. In 2006, 178,000 party committees had been established in private firms.<sup>12</sup> By 2016, that number had increased sevenfold to approximately 1.3 million.<sup>13</sup> Today, whether the companies, their leadership, and their employees like it or not, the CCP is present in private and public enterprise. Often the activity of party committees and party-building activity is linked to the CCP's version of the concept of 'corporate social responsibility'<sup>14</sup>—a concept that the party has explicitly politicised. For instance, in the publishing industry, corporate social responsibility includes political responsibility<sup>15</sup> and protecting state security.<sup>16</sup> Internet and technology companies are believed to have the highest proportion of CCP party committees in the private sector.<sup>17</sup>

This expanding influence and reach also extends to foreign companies. For example, by the end of 2016, the CCP's Organisation Department claimed that 70% of China's 100,000 foreign enterprises possessed party organisations.<sup>18</sup> Expanding the party's reach and role inside private enterprises appears to have been a priority since party chief Jiang Zemin's 'Three Represents' policy, which opened party membership to businesspeople, became CCP doctrine in 2002.

All the companies mapped as a part of this project have party committees, party branches and party secretaries. For example, Alibaba has around 200 party branches;<sup>19</sup> in 2017 it was reported that Tencent had 89 party branches;<sup>20</sup> and Huawei has more than 300.<sup>21</sup>

Sometimes, the relevance and significance of the CCP's presence within technology companies is dismissed or trivialised as merely equivalent to the presence of government relations or human resources departments in Western corporations. However, the CCP's expectations of these committees is clear.<sup>22</sup> The CCP's constitution states that a party organisation 'shall be formed in any enterprise ... and any other primary-level work unit where there are three or more full party members';<sup>23</sup> Article 32 outlines their responsibilities, which include encouraging everyone in the company to 'consciously resist unacceptable practices and resolutely fight against all violations of party discipline or state law'. Article 33 states that party committees inside state-owned enterprises are expected to 'play a leadership role, set the right direction, keep in mind the big picture, ensure the implementation of party policies and principles, and discuss and decide on major issues of their enterprise in accordance with regulations'.<sup>24</sup>

The establishment and expansion of party committees in private enterprises appears to be one of the ways in which Beijing is trying to reduce financial risks and exercise control over the economy. Because entities 'cannot be without the party's voice' and 'must safeguard the state-owned assets and interests from damage',<sup>25</sup> the party committees are expected to weigh in on major decisions and policies, including the appointment and dismissal of important cadres, major project investment decisions and large-scale capital expenditures.<sup>26</sup> Although this guidance is longstanding practice in state-owned enterprises, it also appears to be taking root in private enterprises. Conducting a review of corporate disclosures in 2017, the *Nikkei Asian Review* identified 288 companies listed in China that 'changed their articles of association to ensure management policy that reflects the party's will'.<sup>27</sup> In 2018,



26 publicly listed Chinese banks revised their articles of association to support party committees and the establishment of subordinate discipline inspection committees. Many of the revised articles reportedly include language requiring party consultation before major decisions are made.<sup>28</sup>

This control mechanism is explicit in the party's vetting of business leaders. For example, although he's not a party member, Baidu CEO Robin Li is a member of the Chinese People's Political Consultative Conference, the country's primary 'united front' body.<sup>29</sup> The party conducts a comprehensive assessment of any of the business executives brought into official advisory bodies managed by the United Front Work Department, the Chinese People's Political Consultative Conference and the National People's Congress. Two of the four criteria – which relates to a business person's political inclinations – include, their 'ideological status and political performance', as well as their fulfillment of social responsibilities. And second, their personal compliance with laws and regulations.<sup>30</sup>

## Enabling & exporting digital authoritarianism

The crown jewel of Chinese foreign policy under Xi Jinping is the Belt and Road Initiative (BRI), which is to be a vast global network of infrastructure intended to enable the flow of trade, people and ideas between China and the rest of the world.<sup>31</sup> Technology, under the banner of the Digital Silk Road, is a key component of this project.

China's ambitions to influence the international development of technological norms and standards are openly acknowledged.<sup>32</sup> The CCP recognises the threat posed by an open internet to its grip on power—and, conversely, the opportunities that dominance over global cyberspace could offer by extending that control.<sup>33</sup>

In a 2017 article published in one of the most important CCP journals, officials from the Cyber Administration of China (the top Chinese internet regulator) wrote about the need to develop controls so that 'the party's ideas always become the strongest voice in cyberspace.'<sup>34</sup> This includes enhancing the 'global influence of internet companies like Alibaba, Tencent, Baidu [and] Huawei' and striving 'to push China's proposition of internet governance toward becoming an international consensus'.

Officials from the Cyberspace Administration of China have written that 'cyberspace has become a new field of competition for global governance, and we must comprehensively strengthen international exchanges and cooperation in cyberspace, to push China's proposition of Internet governance toward becoming an international consensus.'<sup>35</sup> China's technology companies are specifically referenced as a part of this effort: 'The global influence of Internet companies like Alibaba, Tencent, Baidu, Huawei and others is on the rise.'<sup>36</sup>

Western technology firms have attracted heated criticism for making compromises in order to engage in the Chinese market, which often involves constraining free speech or potentially abetting human rights abuses.<sup>37</sup> This attention is warranted and should continue. However, strangely, global consumers have so far been less critical of the Chinese firms that have developed and deployed sophisticated technologies that now underpin the CCP's ability to control and suppress segments of China's population<sup>38</sup> and which can be exported to enable similar control of other populations.



The 'China model' of digitally enabled authoritarianism is spreading well beyond China's borders. Increasingly, the use of technology for repression, censorship, internet shutdowns and the targeting of bloggers, journalists and human rights activists are becoming standard practices for non-democratic regimes around the world.

In its 2018 *Freedom on the net* report, Freedom House singled out China as the worst abuser of human rights on the internet. The report also found that the Chinese Government is actively seeking to export its moral and ethical norms, expertise and repressive capabilities to other nations. In addition to the Chinese Government's efforts, Freedom House specifically called out the role of the Chinese tech sector in facilitating the spread of digital repression. It found that Chinese companies:

have supplied telecommunications hardware, advanced facial-recognition technology, and data analytics tools to a variety of governments with poor human rights records, which could benefit Chinese intelligence services as well as repressive local authorities. Digital authoritarianism is being promoted as a way for governments to control their citizens through technology, inverting the concept of the internet as an engine of human liberation.<sup>39</sup>

Reporters Without Borders has also sounded the alarm over the involvement of Chinese technology companies in repressing free speech and undermining journalism. As part of an extensive report on the Chinese Government's attempts to reshape the world's media in its own image, it concluded that:

From consumer software apps to surveillance systems for governments, the products that China's hi-tech companies try to export provide the regime with significant censorship and surveillance tools ... In May 2018, the companies were enlisted into the China Federation of Internet Societies (CFIS), which is openly designed to promote the Chinese Communist Party's presence within them. Chinese hi-tech has provided the regime with an exceptional influence and control tool, which it is now trying to extend beyond China's borders.<sup>40</sup>

Pushing back against both the practices of digital authoritarianism and the norms and values that underpin such practices requires a clear-eyed understanding of the way they're being spread. For example, a study of the BRI has found that the ways in which some BRI projects, including digital projects, are structured create serious concerns about the erosion of sovereignty for host nations, such as when a recipient government doesn't have full control of the operations, management, digital infrastructure or data being generated through those projects.<sup>41</sup>

Sovereign governments are, of course, ultimately responsible for their actions. For some, particularly Western governments, this includes being transparent and accountable in their use of technology for surveillance and information control. And, if they aren't, the media, civil society and the public have avenues to hold them to account. However, companies also have responsibilities in this space, which is why many sensitive and dual-use technologies are subject to export controls. The need for companies to be held accountable for how new technologies are used is particularly acute in developing countries, where the state may be less able or less willing to do so because of challenges arising from governance, legislative and regulatory capacity, transparency and corruption.



The following case studies have been selected as illustrations of the ways in which Chinese technology companies, often with funding from the Chinese Government, are aiding authoritarian regimes, undermining human rights and exerting political influence in regions around the world.

### Surveillance cities: Huawei's 'smart cities' projects

An important and understudied part of the global expansion of Chinese tech companies involves the proliferation of sophisticated surveillance technologies and 'public security solutions'.<sup>42</sup> Huawei is particularly dominant in this space, including in developing countries where advanced surveillance technologies are being introduced for the first time.

Through this research and as of April 2019, we have mapped 75 Smart City-Public Security projects, most of which involve Huawei.<sup>43</sup> Those projects—which are often euphemistically referred to as 'safe city' projects—include the provision of surveillance cameras, command and control centres, facial and licence plate recognition technologies, data labs, intelligence fusion capabilities and portable rapid deployment systems for use in emergencies.

The growth of Huawei's 'public security solution' projects has been rapid. For example, the company's 'Hisilicon' chips reportedly make up 60% of chips used in the global security industry.<sup>44</sup> In 2017, Huawei listed 40 countries where its smart-city technologies had been introduced;<sup>45</sup> in 2018, that reach had reportedly more than doubled to 90 countries (including 230 cities). Because of a lack of detail or possible differences in definition, this project currently covers 43 countries.<sup>46</sup>

This research has found that, in many developing countries, exponential growth is being driven by loans provided by China Exim Bank (which is wholly owned by the Chinese Government).<sup>47</sup> The loans, which must be paid back by recipients,<sup>48</sup> are provided to foreign governments, and it's been reported in academia and the media that the contractors used must be Chinese companies.<sup>49</sup> In many of the examples examined, Huawei was awarded the primary contract; in some cases, the contract was managed by a Chinese state-owned enterprise and Huawei played a 'sub-awardee' role as a provider of surveillance equipment and services.<sup>50</sup>

Smart-city technologies can impart substantial benefits to states using them. For example, in Singapore, increased access to digital services and the use of technology that exploits the 'internet of things' (for traffic control, health care and video surveillance) has led to increased citizen mobility and productivity gains.<sup>51</sup>

However, in many cases, Huawei's safe-city solutions focus on the introduction of new public security capabilities, including in countries such as Ecuador, Pakistan, the Philippines, Venezuela, Bolivia and Serbia. Many of those countries rank poorly, some very poorly, on measures of governance and stability, including the World Bank's governance indicators of political stability, the absence of violence, the control of corruption and the rule of law.<sup>52</sup>

Of course, the introduction of new public security technologies may have made cities 'safer' from a crime prevention perspective, but, unsurprisingly, in some countries it's created a range of political and capacity problems, including alleged corruption; missing money and opaque deals;<sup>53</sup> operational and ongoing maintenance problems;<sup>54</sup> and alleged national security concerns.<sup>55</sup>



## Censorship and suppression: aiding authoritarianism in Zimbabwe

The example set by the Chinese state is increasingly being looked to by non-democratic regimes—and even some democratic governments—as proof that a free and open internet is neither necessary nor desirable for development. ‘If China could become a world power without a free Internet, why do African countries need a free internet?’ one unnamed African leader reportedly asked interviewers from the Department of Media Studies at the University of Witwatersrand.<sup>56</sup>

The business dealings of Chinese technology companies in Zimbabwe, for example, are closely entwined with the CCP’s support for the country’s authoritarian regime. China is Zimbabwe’s largest source of foreign investment, partly as a result of sanctions imposed by Western countries over human rights violations by the regime. Zimbabwean President Emmerson Mnangagwa’s first visit outside of Africa after his election was to China, where he thanked President Xi Jinping and China for supporting Zimbabwe against Western sanctions and called for even deeper economic and technical cooperation between the two nations.<sup>57</sup>

Chinese companies play a central role in Zimbabwe’s telecommunications sector. Huawei has won numerous multimillion-dollar contracts with state-owned cellular network NetOne, some of which have been the subject of corruption allegations.<sup>58</sup> Several of Huawei’s Zimbabwe projects have been financed through Chinese Government loans.<sup>59</sup>

ZTE also has a significant footprint in the country (and has also been the subject of corruption allegations).<sup>60</sup> This has included a \$500 million loan, in partnership with China Development Bank, to Zimbabwe’s largest telco, Econet, in 2015.<sup>61</sup> ZTE has previously provided equipment, including radio base stations, for Econet’s 3G network.<sup>62</sup> Zimbabwean telecommunications providers currently owe millions of dollars to Huawei and ZTE, as well as Ericsson, which reportedly led to network disruptions in March 2019.<sup>63</sup>

The CCP and Chinese companies haven’t just helped to cushion Zimbabwe’s leaders against the impact of sanctions. They’re also providing both a model and means for the regime’s authoritarian practices to be brought forward into the digital age, both online and offline.

The Zimbabwean Government has been considering draconian new laws to restrict social media since at least 2016, when the official regulator issued an ominous warning to internet users against ‘generating, passing on or sharing such abusive and subversive materials.’<sup>64</sup> In the same year, a law was passed to allow authorities to seize devices in order to prevent people using social media.<sup>65</sup>

In early 2019, the government blocked social media and imposed internet shutdowns in response to protests against fuel price increases. Information Minister Energy Mutodi stated that ‘social media was used by criminals to organize themselves . . . this is why the government had to . . . block [the] internet,’ as he announced plans for forthcoming cybercrime laws to criminalise the use of social media to spread ‘falsehoods.’<sup>66</sup>

The government has openly been looking to China as a model for controlling social media,<sup>67</sup> including by creating a cybersecurity ministry, which a spokesperson described as ‘like a trap used to catch rats.’<sup>68</sup>



Parts of this 'trap' reportedly come from China. In 2018, it was reported that China, alongside Russia and Iran, had been helping Zimbabwe to set up a facility to house a 'sophisticated surveillance system' sold to the government by 'one of the largest telecommunications companies' in China.<sup>69</sup> Given the description and context, it seems plausible that this company may be Huawei or ZTE.

'We have our means of seeing things these days, we just see things through our system. So no one can hide from us, in this country,' said former Intelligence Minister Didymus Mutasa.<sup>70</sup>

The government is increasingly looking to expand its surveillance from the online space into the real world. It's signed multiple agreements with Chinese companies for physical surveillance systems, including a highly controversial planned national facial recognition system with Chinese company CloudWalk.<sup>71</sup>

It's also interested in developing its own indigenous facial recognition technology, and is working with CETC subsidiary Hikvision to do it.<sup>72</sup> Hikvision is already supplying surveillance cameras for police and traffic control systems.<sup>73</sup> In 2018, Zimbabwean authorities signed a memorandum of understanding with the company to implement a 'smart city' program in Mutare. This included the donation of facial recognition terminals equipped with deep-learning artificial intelligence (AI) systems.

In a media statement, the government stated:

The software is meant to be integrated with the facial recognition hardware which will be made locally by local developers in line with the government's drive to grow the local ICT sector making Zimbabwe to be the number one country in Africa to spearhead the facial recognition surveillance and AI system nationwide in Zimbabwe.<sup>74</sup>

### **National ID programs: Venezuela's 'Fatherland Card'**

Chinese tech companies are involved in national identity programs around the world. One of the most concerning examples is playing out amid the political and humanitarian crisis in Venezuela.

A Reuters investigation in 2018 uncovered the central role played by ZTE in inspiring and implementing the Maduro regime's 'Fatherland Card' program.<sup>75</sup> The Fatherland Card (*Carnet de la Patria*) records the holder's personal data, such as their birthday, family information, employment, income, property owned, medical history, state benefits received, presence on social media, membership of a political party and history of voting.

Although the card is technically voluntary, without it Venezuelans can be denied access to government-subsidised food, medication or gasoline.<sup>76</sup> In the midst of Venezuela's political crisis, registering for a 'voluntary' card is no choice at all for many. In fact, people in Caracas are queuing for hours to get hold of one, despite the risks of handing over personal data to the increasingly unstable and repressive Maduro regime.<sup>77</sup>

According to Reuters, ZTE was contracted by the government to build the underlying database and accompanying mobile payment system. A team of ZTE employees was embedded with Cantv, the Venezuelan state telecommunications company that manages the database, to help secure and monitor the system. ZTE has also helped to build a centralised government video surveillance system.



There are concerns that the card program is being used as a tool to interfere in the democratic process. During the 2018 elections, observers reported kiosks being set up near or even inside voting centres, where voters were encouraged to scan their cards to register for a ‘fatherland prize’.<sup>78</sup> Those who did so later received text messages thanking them for voting for Maduro (although they never did get the promised prize).

Authorities claim that the cards record *whether* a person voted, but not whom they voted for. However, an organiser interviewed by Reuters claimed to have been instructed by government managers to tell voters that their votes could be tracked. Regardless of the truth of the matter, even the rumours that the government may be watching who votes for it—or, perhaps more pertinently, against it—could be expected to influence the way people vote.

In the context of the current crisis, this technologically enabled population control takes on an even sharper edge. Cyberspace has emerged as a key battleground in the struggle between the Maduro regime and the Venezuelan opposition led by Juan Guaidó.

In addition to selective social media blocks<sup>79</sup> and total internet shutdowns,<sup>80</sup> there’s also evidence of more insidious attacks. For example, a website set up by the opposition to coordinate humanitarian aid delivery was subject to a DNS hijacking attack, including the theft of the personal data of potentially thousands of pro-opposition volunteers.<sup>81</sup>

Cantv, Venezuela’s government-run telecommunications company, is reportedly ‘dependent on agreements with ZTE and Huawei to supply equipment and staff and ... Cantv sends its employees to China to receive training.’<sup>82</sup> These deals are financed through the Venezuela China Joint Fund. China is known as something of an international leader in DNS blocking and manipulation, and the Chinese Government is strongly supporting the Maduro regime, including by targeting social media users in China who post or share content critical of Maduro.<sup>83</sup>

## Shaping politics and policy in Belarus

In some parts of the world, Chinese technology companies are helping shape the politics and policy of new technologies through the development of high-level relationships with national governments. This is particularly concerning in the case of non-democratic countries.

Often referred to as ‘Europe’s last dictatorship’, Belarus has been under the control of authoritarian strongman Aleksandr Lukashenko since 1994.<sup>84</sup> In recent years, ties with China have come to play an increasingly significant role not only in Belarus’s delicate diplomatic relations with its powerful neighbours, but also in its very indelicate domestic policies of violent repression. This has included the use of digital technologies for mass surveillance and the targeted persecution of activists, journalists and political opponents.<sup>85</sup>

Huawei has been supplying video surveillance and analysis systems to the Lukashenko regime since 2011 and border monitoring equipment since at least 2014.<sup>86</sup> Also in 2014, Huawei’s local subsidiary, Bel Huawei Technologies, launched two research labs for ‘intellectual remote surveillance systems’. Through the labs, Huawei provides ‘laboratory-based training ... for the specialists of Promsvyaz, Beltelekom, HSCC and other organisations’.<sup>87</sup>

Over the past several years, collaboration between the Belarusian Government and Chinese technology companies has expanded rapidly, in line with Belarus's engagement with the BRI and with deepening diplomatic and economic ties between Lukashenko's regime and the CCP.<sup>88</sup>

In March 2019, Belarus unveiled a draft information security law. 'It is purely our own product. We didn't borrow it from anyone,' State Secretary of the Security Council Stanislav Zas told Belarusian state media.<sup>89</sup>

A day later, China's ambassador to Belarus spoke to the same outlet about how 'Belarusian and Chinese companies [have] managed to establish intensive cooperation in the area of cyber and information security', and about the desire of both countries to 'expand cooperation in the sphere of cybersecurity'.<sup>90</sup>

'Both countries have good practice in this field. We are going to even deeper cooperate [sic] and share experience,' the Chinese ambassador said.

Huawei has played an especially prominent role in this process at multiple levels. It has continued and expanded the training it provides to Belarusians, including sending students to study in China and signing an agreement with the Belarusian State Academy of Communications for a joint training centre.<sup>91</sup>

Huawei is also exerting political and policy influence. In May 2018, the company released its *National ICT priorities for the Republic of Belarus*.<sup>92</sup> The proposal includes recommendations for 'public safety' technologies, such as video surveillance and drones, and a citizen status identification system.

'Belarus has not yet widely deployed integrated police systems, and thus can refer to the solution adopted in Shenzhen,' the document notes. This is likely to be a reference to the facial recognition program implemented by Shenzhen police to 'crack down on jaywalking'.<sup>93</sup>

During a meeting with the chairman of Huawei's board, Guo Ping, for the launch of the plan, then Belarusian Prime Minister Andrei Kobyakov expressed his hope that:

the accumulated experience and prospects of cooperation will play an important role in the development of information and communication technologies in Belarus and in making friendship between our countries stronger. The Belarusian government counts on further effective interaction and professional cooperation.<sup>94</sup>

### **Controlling information flows—WeChat and the future of social messaging**

Launched in 2011, WeChat quickly became China's dominant social network but has largely struggled to build up a significant user base overseas. Still, of the social media super-app's 1.08 billion monthly active users,<sup>95</sup> an estimated 100–200 million are outside China.<sup>96</sup>

Southeast Asia provides the most fertile ground for WeChat outside of China: the app has 20 million users in Malaysia; 17% of the population of Thailand use it;<sup>97</sup> and it's the second most popular messaging app in Bhutan and Mongolia.<sup>98</sup>



The potential for WeChat to substantially grow its user base overseas remains, particularly as it hits a wall in user growth in China<sup>99</sup> and overseas expansion becomes more of an imperative.

To the extent that it's being used outside of mainland China, WeChat poses significant risks as a channel for the dissemination of propaganda and as a tool of influence among the Chinese diaspora.

WeChat is increasingly used by politicians in liberal democracies to communicate with their ethnic Chinese voters, which necessarily means that communication is subject to CCP censorship by default.<sup>100</sup>

In one instance, in September 2017 Canadian parliamentarian Jenny Kwan posted a WeChat message of support for Hong Kong's Umbrella Movement—a series of pro-democracy protests that took place in 2014—only to have it censored by WeChat.<sup>101</sup>

In 2018, Canadian police received complaints about alleged vote buying taking place on WeChat.<sup>102</sup> A group called the Canada Wenzhou Friendship Society was reportedly using the app to offer voters a \$20 'transportation fee' if they went to the polls and encouraging them to vote for specific candidates.

Because WeChat is one of the main conduits for Chinese-language news, censorship controls help Beijing to ensure that news sources using the app for distribution report only news that serves the CCP's strategic objectives.<sup>103</sup>

WeChat is not only a significant influence and censorship tool for the CCP, but also has the potential to facilitate surveillance. An Amnesty International study ranking global instant messaging apps on how well they use encryption to protect online privacy gave WeChat a score of 0 out of 100.<sup>104</sup> Content that passes through WeChat's servers in China is accessible to the Chinese authorities by law.<sup>105</sup>

## Enabling human rights abuses in China: Uyghurs in Xinjiang

Many of the repressive techniques and technologies that Chinese companies are implementing abroad have for a long time been used on Chinese citizens. In particular, the regions of Tibet and Xinjiang are often at the bleeding edge of China's technological innovation.

The complicity of China's tech giants in perpetrating or enabling human rights abuses—including the detention of an estimated 1.5 million Chinese citizens<sup>106</sup> and foreign citizens<sup>107</sup>—foreshadows the values, expertise and capabilities that these companies are taking with them out into global markets. From the phones in people's pockets to the tracking of 2.5 million people using facial recognition technology<sup>108</sup> to the 're-education' detention centres,<sup>109</sup> Chinese technology companies—including several of the companies in our dataset—are deeply implicated in the ongoing surveillance, repression and persecution of Uyghurs and other Muslim ethnic minority communities in Xinjiang.

Many of the companies covered in this report collaborate with foreign universities on the same kinds of technologies they're using to support surveillance and human rights abuses in China. For example, CETC—which has research partnerships with the University of Technology Sydney,<sup>110</sup> the University of Manchester<sup>111</sup> and the Graz Technical University in Austria<sup>112</sup>—and its subsidiary Hikvision are deeply implicated in the crackdown on Uyghurs in Xinjiang. CETC has been providing police in Xinjiang with a centralised policing system that draws in data from a vast array of sources, such as facial recognition cameras and databases of personal information. The data is used to support a 'predictive policing' program, which according to Human Rights Watch is being used as a pretext to arbitrarily detain innocent people.<sup>113</sup> CETC has also reportedly implemented a facial recognition project that alerts authorities when villagers from Muslim-dominated regions move outside of prescribed areas, effectively confining them to their homes and workplaces.<sup>114</sup>

Huawei provides the Xinjiang Public Security Bureau with technical support and training.<sup>115</sup> At the same time, it has funded more than 1,200 university research projects and built close ties to many of the world's top research institutions.<sup>116</sup> The company's work with Xinjiang's public security apparatus also includes providing a modular data centre for the Public Security Bureau of Aksu Prefecture in Xinjiang and a public security cloud solution in Karamay. In early 2018, the company launched an 'intelligent security' innovation lab in collaboration with the Public Security Bureau in Urumqi.<sup>117</sup> According to reporting, Huawei is providing Xinjiang's police with technical expertise, support and digital services to ensure 'Xinjiang's social stability and long-term security'.

Hikvision took on hundreds of millions of dollars worth of security-related contracts in Xinjiang in 2017 alone, including a 'social prevention and control system' and a program implementing facial-recognition surveillance on mosques.<sup>118</sup> Under the contract, the company is providing 35,000 cameras to monitor streets, schools and 967 mosques, including video conferencing systems that are being used to 'ensure that imams stick to a "unified" government script'.<sup>119</sup>

Most concerning of all, Hikvision is also providing equipment and services directly to re-education camps. It has won contracts with at least two counties (Moyu<sup>120</sup> and Pishan<sup>121</sup>) to provide panoramic cameras and surveillance systems within camps.



## Future strategic implications

The degree to which nations and communities around the world are coming to rely on Chinese technology companies for critical services and infrastructure, from laying cables to governing their cities, has significant strategic implications both now and for many years into the future:

- **Undermining democracy:** Perhaps the greatest long-term strategic concern is the role of Chinese technology companies—and technology companies from other countries that aid or engage in similar behaviour—in enabling authoritarianism in the digital age, from supplying surveillance technologies to automating mass censorship and the targeting of political dissidents, journalists, human rights advocates and marginalised minorities. The most challenging issue is the continued export around the world of the model of vicious, ubiquitous surveillance and repression being refined now in Xinjiang.
- **Espionage and intellectual property theft:** The espionage risks associated with Chinese companies are clearly laid out in Chinese law, and the Chinese state has a well-established track record of stealing intellectual property.<sup>122</sup> This risk is only likely to increase as ‘smart’ technology becomes ever more pervasive in private and public spaces. From city-wide surveillance to the phones in the pockets of political leaders (or, in a few years, the microphones in their TVs and refrigerators), governments, the private sector and civil society alike need to seriously consider how to better protect their information from malicious cyber actors.
- **Developing technologies:** Chinese companies are leading the field in research and development into a range of innovative, and strategically sensitive, emerging technologies. Their global expansion provides them with key resources, such as huge and diverse datasets and access to the world’s best research institutions and universities.<sup>123</sup>

Fair competition between leading international companies to develop these crucial technologies is only to be expected, and Chinese tech companies have made enormous positive contributions to the sum total of human knowledge and innovation.

However, the strategic, political and ideological goals of the CCP—which has directed and funded much of this research—can’t be ignored. From AI to quantum computing to biotechnology, the nations that dominate those technologies will exercise significant influence over how the technologies develop, such as by shaping the ethical norms and values that are built into AI systems, or how the field of human genetic modification progresses. Dominance in these fields will give nations a major strategic edge in everything from economic competition to military conflict.

- **Military competition:** In cases of military competition with China, the Chinese Government would of course seek to leverage, to its own advantage, its influence over Chinese companies providing equipment and services to its enemies. This should be a serious strategic consideration for nations when they choose whether to allow Chinese companies to be involved in the build-out of critical infrastructure such as 5G networks, especially given the CCP’s increasing assertiveness and coercion globally.



This issue is particularly acute for countries already experiencing tensions over China's territorial claims in regions such as the South China Sea. For example, in 2016, after a ruling by a UN-backed tribunal dismissed Chinese claims, suspected Chinese hackers attacked announcement and communications systems in two of Vietnam's major airports, including a 'display of profanity and offensive messages in English against Vietnam and the Philippines'.<sup>124</sup> A simultaneous hack on a Vietnamese airline led to the loss of more than 400,000 passengers' data. Vietnam's Information and Communications Minister said that the government was 'reviewing Chinese technology and devices' in the wake of the attack.<sup>125</sup> Cybersecurity firm FireEye says that it's observed persistent targeting of both government and corporate targets in Vietnam that's suspected to be linked to the South China Sea dispute.<sup>126</sup>

5G infrastructure build outs should be an area of particular concern. An article in the China National Defence Report in March 2019<sup>127</sup> discusses the military applications for China of 5G in the move to 'intelligentised' warfare. '[A]s military activities accelerate towards extending into the domain of intelligentization, air combat platforms, precision-guided munitions, etc. will be transformed from 'accurate' to 'intelligentized'. 5G-based AI technology will definitely have important implications for these domains,' write the authors, who appear to be researchers affiliated with Xidian University and the PLA's Army Command Academy.

## Conclusion

Chinese companies have unquestionably made important and valuable contributions to the technology industry globally, from contributing to cutting edge research and pushing the boundaries of developing technologies, to enabling access to affordable, good quality devices and services for people around the world. They are not going anywhere, and they are going to continue to play a vital role in the ways in which governments, companies and citizens around the world connect with one another.

At the same time, however, it is important to recognise that the activities of these companies are not purely commercial, and in some circumstances risk mitigation is needed. The CCP's own policies and official statements make it clear that it perceives the expansion of Chinese technology companies as a crucial component of its wider project of ideological and geopolitical expansion. The CCP committees embedded within the tech companies and the close ties (whether through direct ownership, legal obligations or financing agreements including loans and lucrative contracts) between the companies and the Chinese government make it difficult for them to be politically neutral actors, as much as some of the companies might prefer this. There is also a legitimate question about whether global consumers should demand greater scrutiny of Chinese technology firms that facilitate human rights abuses in China and elsewhere.

Governments around the world are struggling with the political and security implications of working with Chinese corporations, particularly in areas such as critical infrastructure, for example in 5G, and in collaborative research partnerships that might involve sensitive or dual-use technologies. Part of this struggle is due to a lack of in-depth understanding of the unique party-state environment that shapes, limits and drives the global behaviour of Chinese companies. This research project aims to help plug that gap so that policymakers, industry and civil society can make more informed decisions when engaging China's tech giants.



## Notes

- 1 Sarah Cook, 'China's cyber superpower strategy: implementation, internet freedom implications, and US responses', written testimony to House Committee on Oversight and Government Reform, Freedom House, 28 September 2018, [online](#); Kania et al., 'China's strategic thinking on building power in cyberspace: a top party journal's timely explanation translated'.
- 2 Emily Feng, 'Chinese tech groups display closer ties with Communist party', *Financial Times*, 11 October 2017, [online](#); Zhang Lin, 'Chinese Communist Party needs to curtail its presence in private businesses', *South China Morning Post*, 25 November 2018, [online](#); China Organisation personnel, 'China's internet companies are surging with a "party building tide"' [我国互联网企业涌动'党建潮'], *CPCnews.cn*, 26 March 2018, [online](#).
- 3 Samantha Hoffman, Elsa Kania, 'Huawei and the ambiguity of China's intelligence and counter-espionage laws', *The Strategist*, 13 September 2018, [online](#).
- 4 Constitution of the Communist Party of China, revised and adopted on 24 October 2017, [online](#).
- 5 People's Republic of China Company Law, [online](#) (in Chinese).
- 6 Hoffman & Kania, 'Huawei and the ambiguity of China's intelligence and counter-espionage laws'.
- 7 Chris Buckley, Amy Qin, 'Muslim detention camps are like "boarding schools," Chinese official says', *New York Times*, 12 March 2019, [online](#); Fergus Ryan, Danielle Cave, Nathan Ruser, *Mapping Xinjiang's 're-education' camps*, ASPI, Canberra, 1 November 2018, [online](#).
- 8 'China: not free: 88/100', *Freedom on the net 2018*, Freedom House, Washington DC, 2018, [online](#).
- 9 Jun Mai, 'Xi Jinping renews "cyber sovereignty" call at China's top meeting of internet minds', *South China Morning Post*, 3 December 2017, [online](#).
- 10 Josh Rogin, 'White House calls China's threats to airlines "Orwellian nonsense"', *Washington Post*, 5 May 2018, [online](#) (paywall).
- 11 Samantha Hoffman, *Social credit: technology enhanced authoritarian control with global consequences*, ASPI, Canberra, 28 June 2018, [online](#).
- 12 Wu Jiao, 'Party membership up in private firms', *China Daily*, 17 July 2007, [online](#).
- 13 Michael Martina, 'Exclusive: In China, the party's push for influence inside foreign firms stirs fears', *Reuters*, 24 August 2017, [online](#).
- 14 Jun Hong (君虹), 'The Evolution of Corporate Social Responsibility in China' (中国企业社会责任的演变), *Red Flag Manuscript* (红旗文稿), 9 March 2019, [online](#).
- 15 'Social responsibility and party building work of publishing companies', *CCP News Network*, 30 July 2013, [online](#) (in Chinese).
- 16 Samantha Hoffman, 'China's state security strategy: "everyone is responsible"', *The Strategist*, 11 December 2017, [online](#).
- 17 Emily Feng, 'Chinese tech groups display closer ties with Communist Party', *Financial Times*, 11 October 2017, [online](#) (paywall); Zhang Lin, 'Chinese Communist Party needs to curtail its presence in private businesses', *South China Morning Post*, 25 November 2018, [online](#); China Organisation personnel, 'China's internet companies are surging with a "party building tide"'.
- 18 'Foreign businesses admire their party workers as a "symbol of excellence"', *China Daily*, 22 November 2017, [online](#).
- 19 <https://chinatmap.aspi.org.au/#/company/alibaba>.
- 20 <https://chinatmap.aspi.org.au/#/company/tencent>.
- 21 <https://chinatmap.aspi.org.au/#/company/huawei>.
- 22 Chauncey Jun, 'What communists do in China's tech companies', *Inkstone*, 4 December 2018, [online](#).
- 23 Article 30, Constitution of the Communist Party of China, [online](#); Article 19, Company Law: [online](#).
- 24 Article 30, Constitution of the Communist Party of China.
- 25 Wei Mengchu (魏梦楚), 'Party building is also a productive force.' (党建也是生产力), *Qiushi* (求是), 21 December 2015, [online](#).
- 26 This formulation is the 'Three Majors, One Big' (三重一大). [胡荣良, '国企"三重一大"决策实践与理性选择'], *Guangming Daily*, 1 March 2015, [online](#).
- 27 Yu Nakamura, 'More companies are writing China's Communist Party into their charters', *Nikkei Asian Review*, 24 August 2017, [online](#).
- 28 Matthew Miller, 'China's banks embrace Communist Party committees in risk crackdown', *Reuters*, 27 June 2018, [online](#).
- 29 <https://chinatmap.aspi.org.au/#/company/baidu>.
- 30 'Wang Jianlin, Dong Wenbiao and others step down as "vice ministers", Richard Liu and Lei Jun take office.' (王健林、董文标等卸任"副部长"·刘强东·雷军等上任), *Sohu* ((搜狐)), 1 December 2017, [online](#).
- 31 Daniel Kliman, Rush Doshi, Kristine Lee, Zack Cooper, *Grading China's Belt and Road*, Asia-Pacific Program, Center for a new American Security, [online](#).
- 32 Elsa Kania, Samm Sacks, Paul Triolo, Graham Webster, 'China's strategic thinking on building power in cyberspace: a top party journal's timely explanation translated', *New America*, 25 September 2017, [online](#).
- 33 Adam Segal, 'When China rules the web: technology in service of the state', *Foreign Affairs*, September–October 2018, [online](#); Samm Sacks, 'Beijing wants to rewrite the rules of the internet', *The Atlantic*, 18 June 2018, [online](#); Elliott Zaagman, 'Cyber sovereignty and the PRC's vision for global internet governance', *China Brief*, Jamestown Foundation, 5 June 2018, [online](#).
- 34 Sarah Cook, 'China's cyber superpower strategy: implementation, internet freedom implications, and US responses', written testimony to House Committee on Oversight and Government Reform, Freedom House, 28 September 2018, [online](#); Kania et al., 'China's strategic thinking on building power in cyberspace: a top party journal's timely explanation translated'.



- 35 Elsa Kania, Samm Sacks, Paul Triolo, Graham Webster, 'China's strategic thinking on building power in cyberspace: a top party journal's timely explanation translated', *New America*, 25 September 2017, [online](#).
- 36 Elsa Kania, Samm Sacks, Paul Triolo, Graham Webster, 'China's strategic thinking on building power in cyberspace: a top party journal's timely explanation translated', *New America*, 25 September 2017, [online](#).
- 37 David Meyer, 'Biotech giant Thermo Fisher stops selling DNA sequencers in repressive Chinese region', *Fortune*, 21 February 2019, [online](#); Pui-Wang Tam, 'Daily report: Facebook courts China with censoring software', *New York Times*, 23 November 2016, [online](#); Paul Mozur, 'In China, Facebook tests the waters with a stealth app', *New York Times*, 11 August 2017, [online](#); Ryan Gallagher, 'Google is conducting a secret "performance review" of its censored China search project', *The Intercept*, 28 March 2019, [online](#); Arjun Kharpal, 'Microsoft says facial recognition firm that Beijing allegedly uses to track Muslims is lying about a "partnership"', *CNBC*, 15 March 2019, [online](#); Lindsay Gorman, Matt Schrader, 'US firms are helping build China's Orwellian state', *Foreign Policy*, 19 March 2019, [online](#); Andy Greenberg, 'Apple's China-friendly censorship caused an iPhone-crashing bug', *Wired*, 10 July 2018, [online](#).
- 38 'China has turned Xinjiang into a zone of repression—and a frightening window into the future', *Washington Post*, 23 February 2019, [online](#) (paywall); *Financial Times*, [online](#) (paywall); 'Big Data fuels crackdown in minority region', news release, Human Rights Watch, 26 February 2018, [online](#).
- 39 *Freedom on the net 2018: the rise of digital authoritarianism*, Freedom House, Washington DC, 2018, [online](#).
- 40 *China's pursuit of a new world media order*, Reporters Without Borders, no date, [online](#).
- 41 For example, Zimbabwe's strategic partnership with CloudWalk Technology, Kliman et al., *Grading China's Belt and Road*.
- 42 'A better connected world', *BBC Future*, no date, [online](#).
- 43 Huawei refers to these projects or solutions as 'safe cities', 'smart cities', 'public security projects' and 'public safety projects'.
- 44 Zhang Dong, 'Tackling security, does Huawei have a chance?', trans. Jeffrey Ding, 31 August 2016, [online](#).
- 45 Matt Schrader, *Huawei's Smart Cities and CCP influence, at home and abroad*, Jamestown Foundation, 19 June 2018, [online](#).
- 46 'Huawei Safe Cities: Serbian Security Guards Pioneer of Major Event Protection' (华为平安城市: 塞尔维亚安全卫士 重大赛事保障先锋), *Huawei website*, 22 August 2019, [online](#).
- 47 <http://chinattechmap.aspi.org.au/#/map/marker-749>, <http://chinattechmap.aspi.org.au/#/map/marker-371>, <http://chinattechmap.aspi.org.au/#/map/marker-394>, <http://chinattechmap.aspi.org.au/#/map/marker-1667>, <http://chinattechmap.aspi.org.au/#/map/marker-491>, <http://chinattechmap.aspi.org.au/#/map/marker-388>, <http://chinattechmap.aspi.org.au/#/map/marker-436>, <http://chinattechmap.aspi.org.au/#/map/marker-490>.
- 48 Danielle Cave, 'Witnessing an opaque Pacific power shift', *The Interpreter*, 5 September 2016, [online](#).
- 49 Matthew Dorman, Philippa Brant, 'Chinese assistance in the Pacific: agency, effectiveness and the role of Pacific island governments', *Asia and the Pacific Policy Studies*, 11 June 2014, [online](#); Veneranda Langa, 'Sibn China Exim Bank loan conditions too stringent', *Zimbabwe Situation*, 30 December 2016, [online](#); G Smith, G Carter, X.J Mao, A Tararia, E Tupou, WT Xu, *The development needs of Pacific island countries*, UNDP China, Beijing, 2014, [online](#).
- 50 <http://chinattechmap.aspi.org.au/#/map/marker-749>.
- 51 Navin Sregantan, 'Singapore tops global smart city performance ranking in 2017: study', *Business Times*, 13 March 2018, [online](#).
- 52 World Bank, *Worldwide governance indicators*, [online](#).
- 53 <https://chinattechmap.aspi.org.au/#/map/marker-749>; Charles Rollet, 'Ecuador's all-seeing eye is made in China', *Foreign Policy*, 9 August 2018, [online](#).
- 54 <https://chinattechmap.aspi.org.au/#/map/marker-388>.
- 55 <https://chinattechmap.aspi.org.au/#/map/marker-1667>.
- 56 Fmeka Imejei, 'The imitation game: will China's investments reshape Africa's internet?', *Power 3.0*, 6 December 2018, [online](#).
- 57 Justina Crabtree, 'Zimbabwe is intent on "leapfrogging 18 years of isolation" with China's help', *CNBC*, 3 April 2018, [online](#).
- 58 Tawanda Zinyama, *Contracting out: the role of public procurement in Zimbabwe*, University of Zimbabwe, no date, [online](#).
- 59 'NetOne secures Huawei financing; ICT Minister under the spotlight', *TeleGeography*, 3 January 2018, [online](#); Nkechinyere Uwajumogu, 'Foreign direct investment and sub-Saharan Africa's domestic entrepreneurial development: a comparison between China's inflow and United States of America's inflow', *ResearchGate*, August 2017, [online](#).
- 60 'ZTE solar tender "under probe"', *Sunday Mail*, 27 March 2016, [online](#).
- 61 'Econet secures \$500 million loan facility from the Chinese government', *myZOL*, 4 December 2015, [online](#).
- 62 'Ericsson, ZTF resume work with Econet', *Zimbabwe Independent*, 8 August 2008, [online](#).
- 63 Tatira Zwinoira, 'Network disruptions to continue', *NewsDay*, 7 March 2019, [online](#).
- 64 Potraz, 'Warning over social media abuses', *Bulawayo 24News*, 6 July 2016, [online](#).
- 65 Peta Thornycroft, 'New Zimbabwe law allows seizure of smartphones and laptops as Mugabe turns on social media', *The Telegraph*, 7 August 2016, [online](#).
- 66 'Zimbabwe activists push back on social media restrictions', *VOA News*, 7 February 2019, [online](#).
- 67 'Govt to regulate social media', *Sunday News*, 10 April 2019, [online](#).
- 68 Andres Kunambura, 'Mugabe explains functions of cyber security ministry', *Nehanda Radio*, 11 October 2017, [online](#).
- 69 Itai Mushekwe, 'China, Russia and Iran helping Zimbabwe to set-up own NSA', *Bulawayo 24News*, 23 March 2018, [online](#).
- 70 Mushekwe, 'China, Russia and Iran helping Zimbabwe to set-up own NSA'.
- 71 Amy Hawkins, 'Beijing's Big Brother tech needs African faces', *Foreign Policy*, 24 July 2018, [online](#).
- 72 <https://chinattechmap.aspi.org.au/#/map/marker-159>.



- 73 'Chinese company to mount surveillance cameras', *NewsDay*, 31 August 2018, [online](#).
- 74 Farai Mudingwa, 'Government Acknowledges Facial Recognition System In The Works' *Techzim*, 13 June 2018, [online](#).
- 75 Angus Berwick, 'How ZTE helps Venezuela create China-style social control', *Reuters*, 14 November 2018, [online](#).
- 76 Jim Wyss, Cody Weddle, 'Venezuela's Maduro aims to turn empty stomachs into full ballot boxes', *Miami Herald*, 16 May 2018, [online](#); Fabiola Zerpa, Patricia Laya, 'In Venezuela, the only way to cheap gas is through Big Brother', *Bloomberg*, 29 August 2018, [online](#).
- 77 Gaby J Miller, 'Of fear & hope: embracing the Carnet de la Patria', *Caracas Chronicles*, 11 January 2018, [online](#).
- 78 Scott Smith, Joshua Goodman, 'Venezuela keeps voting stations open amid light turnout', *CTV News*, 20 May 2018, [online](#).
- 79 'Social media shutdown in Venezuela is a warning of what is to come as political tensions rise', *AccessNow*, 22 January 2019, [online](#).
- 80 'Evidence of regional internet blackouts across Venezuela', *Netblocks*, 27 January 2019, [online](#).
- 81 'DNS manipulation in Venezuela in regards to the humanitarian aid campaign', *Kaspersky*, 13 February 2019, [online](#).
- 82 Angus Berwick, 'Service? Don't rely on Venezuela's state telecoms firm Cantv', *Reuters*, 23 November 2018, [online](#).
- 83 'China targets Twitter users critical of Venezuela's Maduro', *Radio Free Asia*, 11 February 2019, [online](#).
- 84 Peter Pomerantsev, 'Europe's last dictatorship keeps surprising everyone', *Washington Post*, 25 March 2017, [online](#) (paywall).
- 85 Belarus: 'It's enough for people to feel it exists': civil society, secrecy and surveillance in Belarus, Amnesty International, 7 July 2016, [online](#).
- 86 Paul Sonne, 'Belarus talking to China firm about gear', *Wall Street Journal*, 21 December 2011, [online](#); 'Huawei to help Belarus create security surveillance system', *BellSA*, 25 August 2011, [online](#); 'Belarus - China project on Brest frontier post complete', *Pravda.by*, 23 August 2013, [online](#).
- 87 'Huawei opens two laboratories in Belarus', news release, Belarusian-Chinese Intergovernmental Committee on Cooperation, 8 September 2014, [online](#).
- 88 Elise Thomas, 'China, Belarus and the bear in the room', *The Strategist*, 31 January 2019, [online](#).
- 89 'Draft Belarus information security concept presented to head of state', *Belarus News*, 12 March 2019, [online](#).
- 90 'Belarus, China interested in tighter cooperation in cyber security', *Belarus News*, 13 March 2019, [online](#).
- 91 'Cooperation with Belarusian universities as [sic] important for Huawei', *Belarus News*, 25 September 2018, [online](#); 'Huawei, Belarusian State Academy of Communications to set up joint training center', *Belarus News*, 2 May 2018, [online](#).
- 92 'Huawei releases proposal for Belarus national ICT priorities, helping build an IT Belarus', news release, Huawei, 16 May 2018, [online](#).
- 93 Vicky Xiuzhong Xu, Bang Xiao, 'Chinese authorities use facial recognition, public shaming to crack down on jaywalking, criminals', *ABC News*, 20 March 2018, [online](#).
- 94 'Belarus counts on lasting effective cooperation with Huawei', *Belarus News*, 15 May 2018, [online](#).
- 95 Emma Lee, 'WeChat claims 1.08 billion users in latest "one minute" data report', *TechNode*, 19 November 2018, [online](#).
- 96 Tim Culpan, 'The world's most powerful app is squandering its lead: WeChat is leaving money on the table', *Bloomberg*, 23 July 2018, [online](#).
- 97 Ben Halder, 'WeChat, China's weapon of mass propaganda?', *Ozy*, 12 October 2018, [online](#).
- 98 Halder, 'WeChat, China's weapon of mass propaganda?'
- 99 Rita Liao, 'The next phase of WeChat', *TechCrunch*, 10 January 2019, [online](#).
- 100 Nikhil Sonnad, 'WeCensor: What happens when you try to send politically sensitive messages on WeChat', *Quartz*, 18 April 2018, [online](#).
- 101 Yaqui Wang, 'How China's censorship machine crosses borders—and into Western politics', news release, *Human Rights Watch*, 20 February 2019, [online](#).
- 102 Melanie Green, 'Vancouver elections could lead to erosion of trust, racist backlash, experts say', *The Star Vancouver*, 14 October 2018, [online](#).
- 103 Tom Sear, Michael Jensen, Titus C Chen, 'Opinion: How digital media blur the border between Australia and China', news release, UNSW Sydney, 19 November 2018, [online](#).
- 104 *How private are your favourite messaging apps?*, Amnesty International, 21 October 2016, [online](#).
- 105 Celia Chen, 'Here's what happens with your data when you use a Chinese messaging app', *South China Morning Post*, 4 January 2018, [online](#).
- 106 Buckley & Qin, 'Muslim detention camps are like "boarding schools," Chinese official says'.
- 107 Megha Rajagopalan, 'This Australian baby boy has spent his whole life trapped in China's police state. Now his dad wants him out', *Buzzfeed News*, 19 February 2019, [online](#).
- 108 Erin Handley, 'China's mass surveillance of Uyghur Muslims in Xinjiang Province revealed in data security flaw', *ABC News*, 9 February 2019, [online](#).
- 109 Ryan et al., *Mapping Xinjiang's 're-education' camps*, [online](#).
- 110 <https://chinatechmap.aspi.org.au/#/map/marker-87>.
- 111 <https://chinatechmap.aspi.org.au/#/map/marker-86>.
- 112 <https://chinatechmap.aspi.org.au/#/map/marker-49>.
- 113 Shai Oster, 'China tries its hand at pre-crime: Beijing wants to identify subversives before they strike', *Bloomberg*, 4 March 2016, [online](#); 'China: Big Data fuels crackdown in minority region', news release, Human Rights Watch, 26 February 2018, [online](#).
- 114 'China uses facial recognition to fence in villagers in far west', *Bloomberg*, 18 January 2018, [online](#).
- 115 Nathan Vanderlippe, 'Huawei's partnership with China on surveillance technology raises concerns for foreign users', *The Globe and Mail*, 14 May 2018, [online](#).



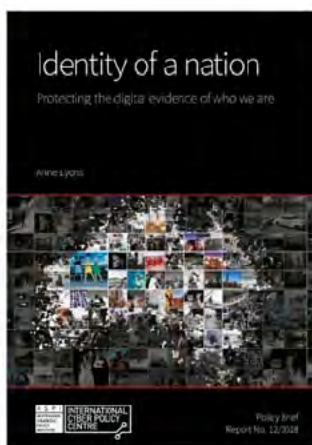
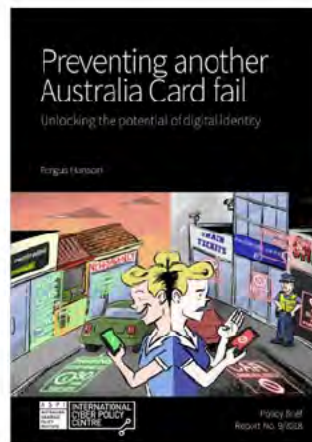
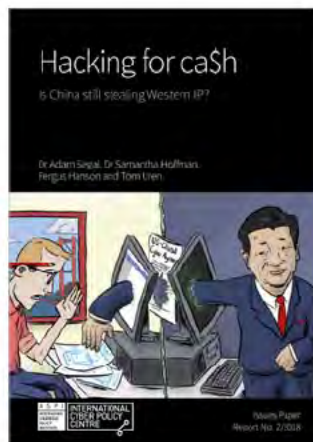
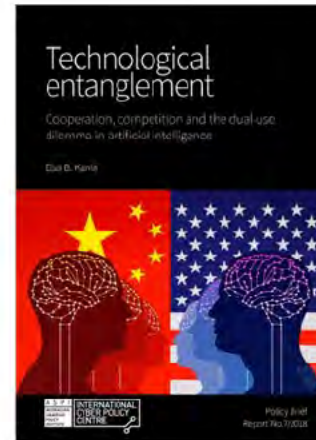
- 116 For example: <https://chinatmap.aspi.org.au/#/map/marker-1042>; Meng Wanzhou, 'Why Huawei values collaboration with universities', *Nikkei Asian Review*, 24, January 2019, online.
- 117 Nathan Vanderklippe, 'Huawei's partnership with China on surveillance technology raises concerns for foreign users', *The Globe and Mail*, 14 May 2018, online.
- 118 AFP, '"No cracks, no blind spots, no gaps": Chinese firms cash in on Xinjiang's growing police state', *Hong Kong Free Press*, 27 June 2018, online.
- 119 Ben Dooley, 'Chinese firms cash in on Xinjiang's growing police state', *AFP*, 27 June 2018, online.
- 120 Emily Feng, 'China steps up surveillance on Xinjiang Muslims', *Financial Times*, 18 July 2018, online.
- 121 Charles Rollet, 'Evidence of Hikvision's involvement with Xinjiang IJOP and re-education camps', *IPVM*, 2 October 2018, online.
- 122 Adam Segal, Samantha Hoffman, Fergus Hanson, Tom Uren, *Hacking for cash: is China stealing Western IP?*, *ASPI*, Canberra, 25 September 2018, online.
- 123 For example: <https://chinatmap.aspi.org.au/#/map/marker-1276>, <https://chinatmap.aspi.org.au/#/map/marker-87>, <https://chinatmap.aspi.org.au/#/map/marker-49>, <https://chinatmap.aspi.org.au/#/map/marker-1174>.
- 124 Charlie Osborne, 'Chinese hackers take down Vietnam airport systems', *ZDNet*, 1 August 2016, online.
- 125 Bloomberg, 'Spyware deluge hits Vietnam sites amid South China Sea spat', *Business Times*, 10 August 2016, online.
- 126 Matthew Tostevin, 'Chinese cyber spies broaden attacks in Vietnam, security firm says', *Reuters*, 31 August 2017, online.
- 127 Elsa Kania, '5G and the Future of AI on the battlefield', *Battlefield Singularity*, 9 April 2019, online.

## Acronyms and abbreviations

AI	artificial intelligence
BAT	Baidu, Alibaba and Tencent
BRI	One Belt, One Road Initiative
CCP	Chinese Communist Party
CETC	China Electronics Technology Group Corporation
ICPC	International Cyber Policy Centre



# Some previous ICPC publications





# EXHIBIT 15



# When the winner takes it all

Big data in China and the battle for privacy

Lotus Ruan



## About the author

**Lotus Ruan** is a researcher at The Citizen Lab, University of Toronto. Her research focuses on the interplay of the state and private companies in terms of internet management and innovation in the digital age with an area focus on China. Prior to joining University of Toronto, Lotus received her master's degree in Asia Pacific Policy Studies at the University of British Columbia and worked as a journalist and news editor in China for two years. She also frequently writes about Chinese politics and social issues for English media outlets including *Foreign Policy*, *The Diplomat*, and *Tech in Asia*.

## What is ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

## ASPI International Cyber Policy Centre

The ASPI International Cyber Policy Centre's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia-Pacific.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various sponsors.

## Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

## ASPI

Tel +61 2 6270 5100

Fax + 61 2 6273 9566

Email [enquiries@aspi.org.au](mailto:enquiries@aspi.org.au)

[www.aspi.org.au](http://www.aspi.org.au)

[www.aspistrategist.org.au](http://www.aspistrategist.org.au)

[facebook.com/ASPI.org](https://www.facebook.com/ASPI.org)

[@ASPI\\_ICPC](https://twitter.com/ASPI_ICPC)

[www.aspi.org.au/icpc/home](http://www.aspi.org.au/icpc/home)

© The Australian Strategic Policy Institute Limited 2018

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers.

First published June 2018.

Cover image: Laptop showing facial recognition technology © Ivan Marc/shutterstock.com.





# When the winner takes it all

Big data in China and the battle for privacy

Lotus Ruan

Issues Paper  
Report No.5/2018



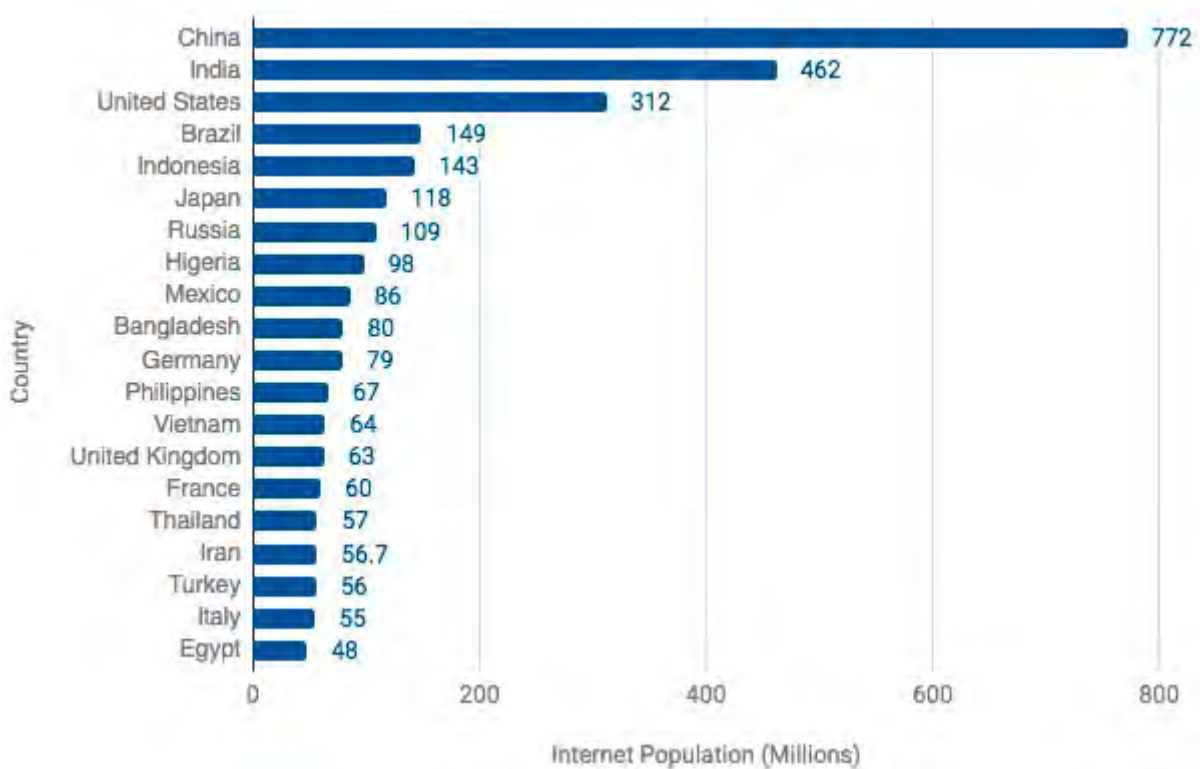
# Contents

<b>Introduction</b>	<b>03</b>
<b>An ambitious big data vision supported by China's internet companies</b>	<b>04</b>
<b>Big data and public security</b>	<b>05</b>
<b>Diminishing rights: China's data laws and regulations</b>	<b>07</b>
<b>Lack of transparency and accountability</b>	<b>10</b>
<b>International implications</b>	<b>12</b>
<b>Conclusion</b>	<b>14</b>
<b>Notes</b>	<b>15</b>
<b>Acronyms and abbreviations</b>	<b>16</b>

## Introduction

If data is the new oil, China is oil super-rich. Data is the essential ingredient for artificial intelligence (AI) and is underpinning a wideranging revolution. China's massive population, lack of privacy protections, controlled tech sector and authoritarian system of governance give it a huge edge in collecting the data needed for that revolution (Figure 1). But the Chinese state and Chinese businesses are also using this wealth of data to pursue state and business goals without the constraints present in other jurisdictions. A lack of privacy protections and rule-of-law protections leaves Chinese citizens at the whim of sophisticated, and often state-controlled, data-driven technologies. Private companies are not only sharing users' personal data with the authorities in compliance with China's regulatory environment such as the most recent Cybersecurity Law but many of those companies—including the industry leaders—are building their business model predominantly around the needs of the state. The success of these technologies in enabling potential mass surveillance and exerting a chilling effect on individuals deserves more attention.

**Figure 1: Top 20 internet populations, by country**



Note: At 31 December 2017, China had 772 million internet users. The proportion of internet users using mobile phones has reached an impressive 97.5%.

This paper examines Chinese state policy on big data industries and analyses the laws and regulations on data collection that companies in China are required to comply with. It also looks at how those rules may affect foreign companies eyeing the China market. Case studies are included to demonstrate the ongoing tensions between big data applications and privacy. The paper concludes by outlining the implications and lessons for other countries.



## An ambitious big data vision supported by China's internet companies

China's State Council has laid out an ambitious [road map](#) outlining its AI vision, which includes creating a US\$150 billion industry and becoming the world leader in AI by 2030.<sup>1</sup> Enormous state financial backing aside, a controlled tech industry,<sup>2</sup> huge data availability and relatively scant privacy protections mean that China is well placed to become a global AI leader; or, to be more accurate, a leader in the development of big-data-driven technologies.

China's online ecosystem is unique compared to Western equivalents. Unlike their Silicon Valley competitors, Chinese technology and internet companies typically design their products to include not just one, but various types of services. Tencent's WeChat, for example, China's most popular mobile chat application, is more than an instant messaging app: it's an all-in-one superapp. A billion active WeChat users now use it to chat with their friends and families, communicate with supervisors and work colleagues, play games, hail taxis, make online purchases and conduct financial investments.<sup>3</sup> WeChat is now even used to handle sensitive government paperwork, such as visa applications, and could soon be used for entry into Hong Kong.<sup>4</sup>

Tencent vowed—openly and ambitiously—to become the fundamental platform for the Chinese internet: a platform 'as vital as the water and electricity resources in daily life'.<sup>5</sup> Alibaba's Alipay, China's Paypal-like e-payment service, has incorporated social functions through which it encourages users to share location data, personal information and purchasing habits with others. Combined with China's real-name registration system,<sup>6</sup> these consolidated functions enable the government and industry to effortlessly profile individual users. In addition, even when an individual's information has been anonymised, their identity can still be re-identified by any interested parties if they have access to two or more sets of data to find the same user in both. In other countries, such identification would attract public concern, but research indicates that there's a lack of awareness and a willingness to trade off privacy for lower cost services among Chinese consumers.<sup>7</sup> For example, research that compared global consumers' views on sharing personal information online found that consumers in China had a more lackadaisical attitude towards privacy protection than consumers in most Western countries.<sup>8</sup>

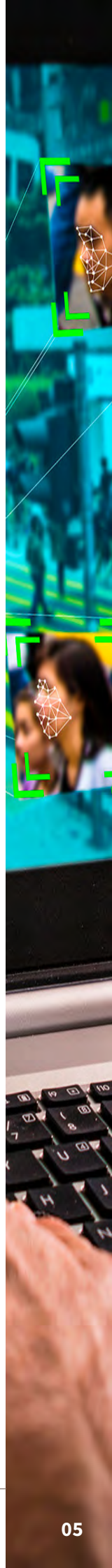
Big data analytics offers invaluable insights to inform the use and delivery of public goods, including increased public safety, law enforcement, resource allocation, urban planning<sup>9</sup> and healthcare systems.<sup>10</sup> But how data is collected and used affects a country's digital ecosystem and its citizens' social and political participation. How China's regulatory environment handles these interactions is analysed in the following section.

## Big data and public security

China is placing huge bets on big data, and a range of policies have been introduced over the past two years to flesh out the government's vision. On October 18 2017, Chinese President Xi Jinping promoted the integration of the internet, big data and AI with the real-world economy in his 19th Party Congress report.<sup>11</sup> But China's interest in big data can be dated to as early as the early 2010s. In July 2012, the State Council specifically mentioned the importance of 'strengthening the development of basic software—especially those that are able to handle large volumes of data'—in a [policy document](#) in its 12th Five-Year Plan . The current administration has beefed up the conceptualisation of China's big data vision. Chinese Premier Li Keqiang, for example, proposed the concept of 'Internet Plus' (互联网+),<sup>12</sup> calling for the integration of mobile internet, cloud computing, big data and the 'internet of things' with modern manufacturing in his March 2015 Government Work Report.<sup>13</sup>

In the months following Li's report, China's central government released a number of top-down designs and guidelines on big data policies (Table 1). By the end of 2016, various government bureaucracies<sup>14</sup> and more than 20 provincial and municipal governments issued their own regulations and development plans for big data industries.<sup>15</sup> Unsurprisingly, most of these government initiatives and policies have a special interest in developing and supporting big data technologies that can be applied to the security sector. Security experts argue that contribution to the emerging social credit system is likely as part of these related initiatives.<sup>16</sup>

Statistics from 2016 show that most of the government's domestic government investment in big data industries has gone to public security projects.<sup>17</sup>



**Table 1: Major big data policies issued by the Chinese Government**

Title	Issuer	Date issued	Main takeaways
Made in China 2025 《中国制造2025》, <a href="#">online</a> .	State Council	May 2015	Lays out a road map for the transformation and upgrade of China's traditional and emerging manufacturing industry, with a focus on big data, cloud computing, the internet of things and related smart technologies. <sup>a</sup>
Action Outline for Promoting the Development of Big Data 《促进大数据发展行动纲要》, <a href="#">online</a> .	State Council	August 2015	Provides a top-down action framework for promoting big data. Details yearly goals such as establishing a platform for sharing data between government departments by the end of 2017, a unified platform for government data before the end of 2018, and nurturing a group of 500 companies in the industry, including 10 leading global enterprises focused on big data application, services and manufacturing by the end of 2020.  It is widely perceived to be a programmatic document guiding the long-term development of China's big data industries.
Outline of the 13th Five-Year Plan for the National Economic and Social Development of the People's Republic of China 《中华人民共和国经济和社会发展第十三个五年规划纲要》, <a href="#">online</a> .	National People's Congress	March 2016	Identifies big data as a 'fundamental strategic resource' (基础性战略资源). Pushes for further sharing of data resources and applications. Lists big data applications as one of the eight major informatisation projects.  It's the first time China incorporated big data into state-centric strategy plans. <sup>b</sup>
The National Scientific and Technological Innovation Planning for the 13th Five Years 《'十三五' 国家创新规划》, <a href="#">online</a> .	State Council	July 2016	Prioritises big-data-driven breakthroughs in AI technologies.
Development Plan for Big Data Industries (2016–2020) 《大数据产业发展规划 (2016-2020年)》, <a href="#">online</a> .	Ministry of Industry and Information Technology	December 2016	Sets an overarching goal for China's big data industries: by 2020, related industry revenue should exceed 1 trillion RMB, with a compound annual growth rate of 30%.

a 徐永华,陈怀宇, 陈亦恺, Anthony Marshall, 何志强, 夏宇飞, 温占鹏, 张龙, 孙春华, '中国制造业走向2025 构建以数据洞察为驱动的新价值网络', IBM商业价值研究院, 中国电子信息产业发展研究院, 13 October 2015 [online](#).

b 林巧婷, '我国首次提出推行国家大数据战略' 中央政府门户网站, 3 November 2015 [online](#).

In the outline of the 13th Five-Year Plan, big data applications were listed as one of the eight major 'informatisation' projects. Informatisation (信息化)—the process by which the political, social and economic interactions in a society have become networked and digitised—cannot be overstated when analysing China's big data vision, especially in the public security sector. Over the past two decades, the Ministry of Public Security has taken an adaptive approach to this trend. It has made continuous efforts<sup>18</sup> to harness the advances of information and communications technologies for security operations—a process called 'public security informatisation' (公安信息化). At its core, public security informatisation relates to shifting police work from reactive to pre-emptive through the use



of data collection and synthesis. “Security” is a broad concept when applied by the Chinese state and is sufficiently broad to enable the control and censoring of public debate in ways that may affect the power or standing of the ruling Chinese Communist Party.

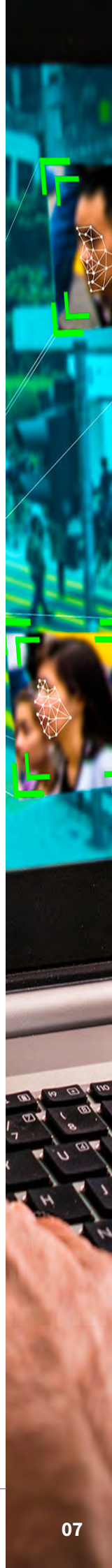
A few statistics help put these concepts and policies in context. Across China, there’s a network of approximately 176 million surveillance cameras—expected to grow to 626 million by 2020<sup>19</sup>—that monitor China’s 1.4 billion citizens. Powered by big-data-driven facial recognition technology, these cameras are able to identify a person’s name, identification card number, gender, clothing and more. Meanwhile, Chinese police have reportedly been collecting DNA samples, fingerprints, iris scans, and blood types of all residents, using questionable methods, in places such as Xinjiang.<sup>20</sup>

Backed by an oceanic amount of data and advanced analytic technologies, Chinese public security forces are emerging as a powerful and dominant intelligence and security sector.<sup>21</sup> The interest from the public security forces in using big data to support government systems for faster and more extensive surveillance and social control largely explains the rapid rise of China’s big data industries.<sup>22</sup> Private companies are not only sharing users’ personal data with the authorities in compliance with China’s Cybersecurity Law,<sup>23</sup> the National Intelligence Law<sup>24</sup> and other relevant [internet management regulations](#), but many of them—including the industry leaders<sup>25</sup>—are building their business model predominantly around the needs of the state.

## Diminishing rights: China’s data laws and regulations

On the other end of the spectrum of the all-encompassing, data-driven analytic technologies are citizens’ *de facto* diminishing rights to privacy and growing challenges of protecting individuals’ data security. In contrast to the wide scope of central- and local-level policy initiatives and government-backed projects on big data collection and use, there’s no uniform law or a national authority to ensure or coordinate data protection in China. Privacy advocates have been striving to have a national privacy protection law passed since 2003.<sup>26</sup> Fifteen years later, the National People’s Congress, China’s highest legislative body, still has not included such uniform law in its agenda.<sup>27</sup>

A number of articles in China’s recent Cybersecurity Law pertain to data collection and privacy protection. However, they take a state-centric approach, expanding the government’s direct involvement in companies’ operations. Missing in this approach is any support for an independent privacy watchdog or support for independent civil society organisations. For now, regulations on data protection remain largely domain-specific, such as those relating to telecommunications and online banking, which are issued by different ministries or local governments (Table 2 summarises the main relevant regulations in China).



**Table 2: Chinese laws, regulations and guidelines on data collection**

Title	Issuer	Date issued	Relevance
Information Security Technology: Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems 《信息安全技术公共及商用服务信息系统个人信息保护指南》, <a href="#">online</a> .	General Administration of Quality Supervision, Inspection and Quarantine & Standardisation Administration of China	November 2012	Establishes basic principles for personal data collection, processing and transfers, including the principles of 'parity of authority and responsibility', 'minimum necessary and not excessive' and 'consent of the individual'. Remains non-compulsory for companies.
Decision on Strengthening Information Protection on Networks 《关于加强网络信息保护的规定》, <a href="#">online</a> .	Standing Committee of the National People's Congress	December 2012	Specifies that the state protects 'electronic information by which individual citizens can be identified and which involves the individual privacy of citizens'.
Provisions on Protecting the Personal Information of Telecommunications and Internet Users 电信和互联网用户个人信息保护规定, <a href="#">online</a> .	Ministry of Industry and Information Technology	July 2013	Regulates how telecommunications and internet service providers may collect and use users' personal data.
Regulation on the Administration of Credit Investigation Industry 征信业管理条例, <a href="#">online</a> .	State Council	January 2013	Encompasses China's grand plan of building a 'social credit system'. Regulates the collection, storage and processing of personal information by credit investigation enterprises. Article 14 points out that 'credit investigation institutions are prohibited from collecting information about the religious belief, genes, fingerprints, blood type, disease or medical history of individuals, as well as other individual information the collection of which is prohibited by laws or administrative regulations.'
Amendment (IX) to the Criminal Law of the People's Republic of China 刑法修正案(九), <a href="#">online</a> .	Standing Committee of the National People's Congress	August 2015	Criminalises the sale or provision of citizens' personal data, with a penalty of up to seven years imprisonment.
Cybersecurity Law 网络安全法, <a href="#">online</a> .	Standing Committee of the National People's Congress	November 2016	Article 76 (5) defines 'personal information' in legal documents for the first time. 'Personal information' refers to all kinds of information, recorded electronically or through other means, that can determine the identity of natural persons independently or in combination with other information, including, but not limited to, a natural person's name, date of birth, identification number, personal biometric information, address and telephone number.
E-commerce Law (draft) 电子商务法 (草案)	Under review by Standing Committee of the National People's Congress	May be passed in 2018	Regulates data collection by e-commerce operators.



Title	Issuer	Date issued	Relevance
Interim Security Review Measures for Network Products and Services 《网络产品和服务安全审查办法(试行)》, <a href="#">online</a> .	Cyberspace Administration of China	May 2017	Specifies that a cybersecurity review will include reviewing risks that product or service suppliers illegally collect, store, process or use user-related information while providing products or services.
Information Security Technology: Personal Information Security Specification 《信息安全技术 个人信息安全规范》, <a href="#">online</a> .	General Administration of Quality Supervision, Inspection and Quarantine & Standardisation Administration of China	December 2017 (took effect in May 2018)	Clarifies the definition of ‘personal sensitive information’, which includes information on one’s wealth, biometrics, personal identity, online identity identifiers and so on.  Remains non-compulsory for companies.

The lack of a legal framework on privacy protection has led to open disputes over who has access to user data. One of the most high-profile cases is the dispute between Tencent, China’s first internet giant to enter the elite US\$500 billion tech club,<sup>28</sup> and Huawei, the Chinese telecom equipment and smartphone maker. Huawei was seeking to collect user data from Tencent’s WeChat, China’s most popular chat app, installed on its Honor Magic phone. The data would help Huawei advance its AI projects. Tencent was quick to object, claiming it would violate user privacy and demanded that the Chinese Government intervene.<sup>29</sup> Huawei argued that users have the right to choose whether and with whom their data is shared. The government suggested the two companies ‘follow relevant laws and regulations’,<sup>30</sup> but existing regulations fail to specify who can collect and process user data.<sup>31</sup> It’s still unclear how the two settled the dispute—or even whether they’ve settled it.<sup>32</sup>

Huawei and Tencent aren’t the first Chinese tech giants to rub shoulders over access to data. In June 2017, Alibaba’s logistics arm, Cainiao, and China’s biggest private courier, SF Express, were in a month-long [stand-off over access to consumer data](#). The fight was eventually resolved with the State Post Bureau’s intervention.<sup>33</sup> Cainiao and SF Express both cited noble-sounding reasons, such as ‘data security’ and ‘user privacy’, for refusing to share data with each other, but the dispute was really about protecting their commercial interests and determining who had access to merchant and shopper data on China’s US\$910 billion online retail market.<sup>34</sup> In the case of Huawei versus Tencent, it’s about who may get to dominate the AI race with the help of massive amounts of data, including users’ chat logs. Due to a void in the current legal framework, it’s likely that disputes between companies over user data access will continue.

## Lack of transparency and accountability

Most of the regulations are aimed at holding companies and individuals—rather than government bodies—accountable for data collection and protection. By contrast, government authorities now have access to more sensitive personal data than ever (through either court orders or surveillance). In addition, law enforcers are requiring companies to ensure a longer period of data retention and zero exemptions from real-name registration policies.

In June 2016, for example, China's Cyberspace Administration issued the Provisions on the Administration of Mobile Internet Applications Information Services (移动互联网应用程序服务管理规定),<sup>35</sup> which require, among other things, that:

- app providers and app stores cooperate with government oversight and inspection
- app providers keep records of users' activities for 60 days
- app providers ensure that new app users register with their real names by verifying users' mobile phone numbers, other identifying information, or both.

In September 2016, Chinese authorities issued new regulations stating explicitly that user logs, messages and comments on social media platforms such as WeChat Moments—a feature that resembles Facebook's timeline feed—can be collected and used as 'electronic data' to investigate legal cases.<sup>36</sup> Cases of WeChat users being arrested for 'insulting police'<sup>37</sup> or 'threatening to blow up a government building'<sup>38</sup> on Moments indicate that the feature may be subject to monitoring by the authorities or the company.

Observers have raised concerns over authorities' use of big-data-driven and AI-enabled technologies such as facial recognition and voice recognition, which may lead to an all-seeing police state. iFlytek, a Chinese information technology company designated by the Ministry of Science and Technology to lead the country's speech recognition development, has partnered with the Ministry of Public Security to develop [a joint research lab](#). According to a report by the company, it has also partnered with local telecommunication companies in eastern Anhui Province to establish a surveillance system that 'notifies public security departments as soon as a suspicious voice is detected'.<sup>39</sup> In the highly restricted Xinjiang region, local authorities are reportedly collecting highly sensitive personal information, including DNA samples, fingerprints and iris scans.<sup>40</sup>

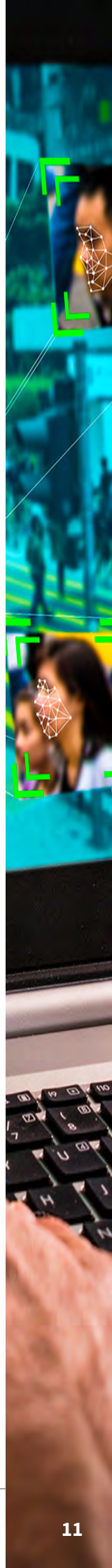
A case that demonstrates ongoing tensions between big data applications and privacy concerns in China is the building of a national social credit system 社会信用体系 (SCS), which is the subject of a forthcoming ICPC policy brief by Samantha Hoffman. The SCS, currently planned for a full launch by 2020, aims to aggregate data on the country's 1.4 billion citizens and assign each person a credit rating based on their socioeconomic status and online behaviour.<sup>41</sup> So far, there's little detail on exactly how the system will unfold. Some companies and local governments have created their own systems (such as Tencent's Tencent Credit,<sup>42</sup> Alibaba's Sesame Credit<sup>43</sup> and many other social credit products developed by smaller players).<sup>44</sup> While a final reward and punishment mechanism remains uncertain, existing reports show some consistent themes. For example, based on their social credit score and

behaviours that affect one's credit, a citizen's access to aeroplane or express train travel will be denied and their privileges, such as faster visa approval and easier access to apartment rentals, will be restricted if the person has a bad social credit score.

The justifications for this scheme include the idea that it's a remedy for the deficit of trust in society.<sup>45</sup> *Southern Metropolis Daily*, a Guangzhou-based liberal-leaning newspaper, surveyed 700 people on their attitudes towards China's social credit system in 2014.<sup>46</sup> It found that even though 40% of the respondents expressed privacy concerns, 80% were in support of this national program because 'it helps build a society of trust' and 'provides a safer and more reliable environment for business'. Yet, the complete lack of transparency and clarity on data protection [raise](#) the alarming prospect of big-data-enabled mass surveillance in China and other authoritarian states.

Both Alibaba<sup>47</sup> and Tencent<sup>48</sup> have rolled out their own versions of social credit systems, which offer a holistic assessment of character based on vaguely defined categories and non-transparent algorithms.<sup>49</sup> According to material collected by researchers at the University of Toronto's Citizen Lab, the chief credit data scientist of Alibaba's Ant Financial, Yu Wujie, has said, 'If you regularly donate to charity, your credit score will be higher, but it won't tell you how many payments you need to make every month ... but [development] in this direction [is undertaken with] the hope that everyone will donate.'<sup>50</sup> Tencent has revealed little about its credit system thus far, but the company already has access to a huge amount of users' social data, including chat logs, via WeChat, QQ and many of its gaming products.

Due to the lack of data protection laws, few, including state regulators, have an understanding of what kinds of data a private company can access and use.<sup>51</sup> It's also unclear whether online comments and activities deemed undesirable by the government would negatively affect a person's creditworthiness. The scheme is wide open to abuse by government authorities, including in tracking dissidents and exerting chilling effects on ordinary citizens.<sup>52</sup>





## International implications

The tensions between privacy protection and data collection will be felt not only in China. In recent years, companies and governments in both authoritarian and democratic countries have vowed to develop big-data-based surveillance technologies and tighten internet management in the name of public and national security.<sup>53</sup>

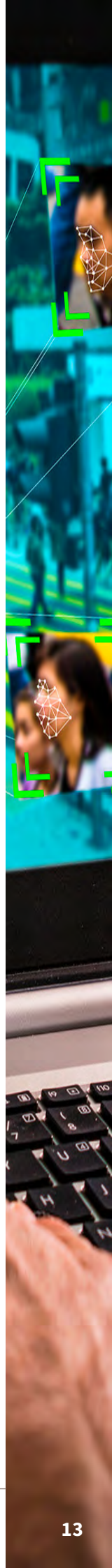
At the international level, cross-border transfers of personal information, courtesy of the increasingly interdependent global economy in the age of big data, have become a pressing issue for private and state actors. Following the enactment of the Cybersecurity Law, which sets data localisation requirements, China has released administrative documents and guidelines detailing the conditions companies need to meet for data export (Table 3).

**Table 3: Regulations on cross-border data transfer or data export**

Title	Issuer	Date issued	Relevance
Cybersecurity Law 网络安全法, <a href="#">online</a> .	Standing Committee of the National People's Congress	November 2016	Article 37: Personal information and important data collected and generated by critical information infrastructure operators in China must be stored domestically. For information and data that is transferred overseas due to business requirements, a security assessment will be conducted in accordance with measures jointly defined by China's cyberspace administration bodies and the relevant departments under the State Council. Related provisions of other laws and administrative regulations shall apply.
Circular of the State Internet Information Office on the Public Consultation on the Measures for the Assessment of Personal Information and Important Data Exit Security (Draft for Soliciting Opinions) 《个人信息和重要数据出境安全评估办法(征求意见稿)》, <a href="#">online</a> .	Cyberspace Administration of China	April 2017	Extends the scope of outbound data security assessment. While the Cybersecurity Law requires security evaluations to be conducted on critical information infrastructure operators (关键信息基础设施运营者), the measures stipulate that all network operators (网络运营者) must go through the check.  Establishes the basic framework for outbound data security assessment, including its processes, responsible parties and main focuses.
Information Security Technology: Guidelines for Data Cross-Border Transfer, <a href="#">online</a> . Security Assessment (second draft), <a href="#">online</a> . 《信息安全技术 数据出境安全评估指南(第二稿)》	National Information Security Standardisation Technical Committee	August 2017	Clarifies the definition of data cross-border transfer, which is 'the one-time or continuous activity in which a network operator provides personal information and important data collected and generated by network or other means in the course of operations within the territory of China to overseas institutions, organisations or individuals by means of directly providing or conducting business, providing services or products, etc.'  Further breaks down the conditions for initiating security self-assessment, government assessment and their processes.  Details what is 'important data' and 'personal data'.  Non-compulsory for companies.

Under these regulations, foreign companies will have to either invest in new data servers in China that may be subject to monitoring by the government or incur new costs to partner with a local server provider, such as Tencent or Alibaba. Apple's recent decision to migrate its China iCloud data to Guizhou Big Data and Amazon's [sell-off](#) of its China cloud assets to its local Chinese partner are just two examples of how China's tightening rules on data retention and transfers may affect foreign companies. By requiring data localisation, the Chinese Government is bringing data under Chinese jurisdiction and making it easier to access user data and penalise companies and individuals seen as violating China's vaguely defined internet laws and regulations.

Meanwhile, Chinese-manufactured tech devices and applications that have taken over large portions of overseas markets are raising questions about data security. The Australian Defence Department has recently banned staff and serving personnel from downloading WeChat, China's most popular social media app, onto their work phones.<sup>54</sup> The heads of six top US intelligence agencies, including the Federal Bureau of Investigation, the Central Intelligence Agency and the National Security Agency, told the Senate Intelligence Committee in February that they would not advise Americans to use products or services from Chinese telecommunications companies Huawei and ZTE. In April 2018, the tension escalated into a seven-year ban imposed by the US Commerce Department, prohibiting American companies from selling parts and software to ZTE, although at the time of publishing it's unclear whether this ban will be enforced or overturned.<sup>55</sup> In December 2017, the Ministry of Defence in India issued a new order to the Indian armed forces requiring officers and all security personnel to remove more than 42 Chinese apps, including Weibo, WeChat and UC Browser, which were classified as 'spyware'.





## Conclusion

This paper highlights the conflict between the fast-developing big data technologies and citizens' diminishing rights to privacy and data security in China. A review of major Chinese big-data-related policy initiatives shows that many of those policies reflect special interest from Chinese authorities, its public security forces in particular, in potentially using data-driven analytic technologies for more effective and extensive surveillance and social control.

Compared to the growing number of regulations and national plans that support the research and development of big data technologies, there's a lack of data protection laws and guidelines to hold relevant parties, especially the government, accountable for the collection and use of personal data. The ambivalent legal framework of data security and privacy protection, which enables state use of collected data, has led to multiple incidences of commercial disputes over access to users' data. It's likely we'll see more such cases in the future.

Addressing these conflicts and advocating for the protection of users' rights to privacy in China—where the state dominates every sector of society and suppresses civil society—is not easy. The Chinese state's approach is a reminder to users, both in China and elsewhere, of the importance of protecting personal privacy and online security.

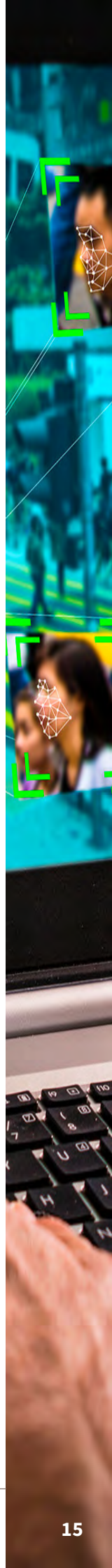
Using China as a case study also offers a number of takeaways for policymakers in other countries. International developments, such as ongoing privacy issues with Facebook data, show that tension between governments, businesses and users in the age of big data is not unique to any country. To that end, the EU's General Data Protection Regulation has set a good example for containing companies' exploitation of personal data.

There's a trend, in China and elsewhere, for governments to use the excuse of 'protecting user privacy' to justify a more powerful state and more state involvement in private companies' and organisations' operations. Civil society groups, whenever and wherever possible, should assume a stronger role in addressing these challenges and raising awareness. A US-based study released in April 2018, for example, [highlighted](#) consumer misconceptions about privacy while using popular browsers, including that they would 'prevent geolocation, advertisements, viruses, and tracking by both the websites visited and the network provider'.<sup>56</sup> Further work and support are needed to equip users with sufficient knowledge to understand how data-related technologies work and what those technologies mean to them in everyday life.

The attractiveness of the Chinese state's surveillance and social control systems to other authoritarian states means we may see other states adopt them, unless the negative aspects of these approaches are made more transparent. The consequences of reduced personal freedom combined with greater state control of societies and individuals are disturbing for advocates of the vitality and strength of open societies. Beyond these concerns, the strategic consequences of the tight integration of the Chinese tech sector with the Chinese state is an area for further analysis.

# Notes

- 1 中华人民共和国国务院, '国务院关于印发 新一代人工智能发展规划的通知', 国务院, 8 July 2017, [online](#).
- 2 China has permitted only some foreign direct investment through Chinese entities with partial or full foreign ownership in many tech sectors. See more detailed analysis by Paul Edelberg, 'Is China Really Opening Its Doors to Foreign Investment?', China Business Review, 8 November 2017, [online](#) and Jianwen Huang, 'China', The Foreign Investment Regulation Review - Edition 5, October 2017, [online](#).
- 3 Yang Ruan, Cheek, Social media in China: what Canadians need to know; Nicole Jao, 'WeChat now has over 1 billion active monthly users worldwide', Technode, 5 March 2018, [online](#).
- 4 Mason Hinsdale, 'Tencent wants to make WeChat a digital travel ID', Jing Travel, 6 June 2018, [online](#).
- 5 马化腾, '互联网像水和电一样成为'传统行业'', Digitaling.com, 12 August 2014, [online](#).
- 6 Catherine Shu, 'China attempts to reinforce real-name registration for internet users', Techcrunch.com, 1 June 2016, [online](#).
- 7 Hui Zhao, Haoxin Dong, 'Research on personal privacy protection of China in the era of big data', Open Journal of Social Sciences, 19 June 2017, 5:139–145, [online](#).
- 8 Boston Consulting Group, Data privacy by the numbers, March 2014, [online](#).
- 9 Linda Poon, 'Finally, Uber releases data to help cities with transit planning', CityLab.com, 11 January 2017, [online](#).
- 10 Linda Lew, 'How Tencent's medical ecosystem is shaping the future of China's healthcare', Technode.com, 11 February 2018, [online](#).
- 11 习近平, '决胜全面建成小康社会 夺取新时代中国特色社会主义伟大胜利——在中国共产党第十九次全国代表大会上的报告', Xinhua, 18 October 2017, [online](#).
- 12 State Council of the People's Republic of China, Premier Li and Internet Plus, 31 December 2015, [online](#).
- 13 'China unveils Internet Plus action plan to fuel growth', Xinhua, 4 July 2015, [online](#).
- 14 数据委, '2016年中国大数据相关政策盘点', 中国数据分析行业网, 21 December 2016, [online](#).
- 15 国家信息中心, 南海大数据应用研究院, '2017中国大数据发展报告', 1 March 2017, [online](#).
- 16 For example see Dr Samantha Hoffman's upcoming June 2018 ASPI International Cyber Policy Centre paper on China's Social Credit System, [online](#).
- 17 2017 Report of the big data development in China.
- 18 王歆, 公安信息化行业发展研究, 17 June 2015, [online](#).
- 19 Josh Chin, Liza Lin, 'China's all-seeing surveillance state is reading its citizens' faces', Wall Street Journal, 26 June 2017, [online](#).
- 20 'China: minority region collects DNA from millions', Human Rights Watch, 13 December 2017, [online](#).
- 21 Edward Schwarck, 'Intelligence and informatization: the rise of the Ministry of Public Security in intelligence work in China', The China Journal, 28 March 2018, [online](#).
- 22 Rachel Botsman, 'Big data meets Big Brother as China moves to rate its citizens', Wired, 21 October 2017, [online](#).
- 23 For example, according to Article 28 of China's Cybersecurity Law, 'Network operators shall provide technical support and assistance to public security organs and state security organs which are in accordance with the law safeguarding national security and investigating criminal activities.'; [online](#).
- 24 'National Intelligence Law of the People's Republic of China', Standing Committee of the National People's Congress, 27 June 2017, [online](#).
- 25 'Backing Big Brother: Chinese facial recognition firms appeal to funds', Reuters, 13 November 2017, [online](#).
- 26 年巍, '新华网评: 个人信息保护的法律 "利剑" 何时出鞘', Xinhua, 23 July 2016, [online](#).
- 27 齐爱民, '中华人民共和国个人信息保护法 (草案) 2017版', Sohu, 12 November 2017, [online](#).
- 28 Jon Russell, 'Tencent becomes the first Chinese tech firm valued over \$500b', Techcrunch, 20 November 2017, [online](#).
- 29 Yang Jie, Alyssa Abkowitz, Dan Strumpf, 'Two China Tech Titans Wrestle Over User Data', Wall Street Journal, 3 August 2017, [online](#).
- 30 杨鑫健, '工信部回应华为腾讯数据之争: 正组织调查·敦促企业规范搜集', 澎湃, 8 August 2017, [online](#).
- 31 周源, '华为腾讯数据冲突将成行业常态 个人用户几无存在感', 财经, 5 August 2017, [online](#).
- 32 熊聆, '复盘华为·腾讯数据争夺战 数据该如何'确权'?', 中国经济周刊, 16 January 2018, [online](#).
- 33 王梦妍, '菜鸟网络和顺丰同意从今日12时起全面恢复数据传输', 中央人民广播电台, 16 January 2018,
- 34 Josh Ye, 'Cainiao, SF Express in standoff over data, causing confusion among Chinese online shoppers', South China Morning Post, 2 June 2017, [online](#).
- 35 'Provisions on the Administration of Mobile Internet Applications Information Services', Lawinfochina.com, 28 June 2016, [online](#).
- 36 周子静, '公检法机关办理刑事案件时·可查看个人朋友圈、微博、网盘等', 澎湃, 20 September 2016, [online](#).
- 37 '收到违停告知单后发微信侮辱交警·安徽阜阳一女子被拘5日', 澎湃, 5 April 2017, [online](#).
- 38 '陕西男子发朋友圈称想炸镇政府 被行政拘留五日', 科技猫, 17 March 2017, [online](#).
- 39 '听声"识" 骗子 这项技术让安徽省内电话诈骗骤降八成', CNbeta.com, 28 February 2017, [online](#).
- 40 'China: minority region collects DNA from millions', Human Rights Watch, 13 December 2017, [online](#).
- 41 '国务院关于印发社会信用体系建设规划纲要 (2014—2020年) 的通知', 中华人民共和国国务院, 27 June 2014, [online](#).
- 42 '腾讯信用', 腾讯网, [online](#).
- 43 '芝麻信用', Zhima Credit, [online](#).



- 44 ‘自如信用’, Zroom.com, [online](#).
- 45 Amy Hawkins, ‘Chinese citizens want the government to rank them’, Foreign Policy, 24 May 2017, [online](#).
- 46 熊晓艳,罗韵姿, ‘建信用体系 忧隐私安全’, 南方都市报, 13 May 2014, [online](#).
- 47 ‘Sesame Credit’, Wikipedia, [online](#).
- 48 Josh Horwitz, ‘China’s Tencent is quietly testing a “social credit score” based on people’s online behavior’, Quartz, 9 August 2017, [online](#).
- 49 Shazeda Ahmed, ‘Cashless society, cached data: security considerations for a Chinese social credit system’, The Citizen Lab, 24 January 2017, [online](#).
- 50 Kumar, ‘你的信用积分够追姑娘吗?’, WTT: What the Tech, 16 February 2017, [online](#).
- 51 Lucy Hornby, Sherry Fei Ju, Louise Lucas, ‘China cracks down on tech credit scoring’, Financial Times, 4 February 2018, [online](#).
- 52 Jon Penney, ‘Chilling effects: online surveillance and Wikipedia use’, Berkeley Technology Law Journal, 27 April 2016, 31(1):117, [online](#).
- 53 George Joseph, ‘How police are watching you on social media’, CityLab, 14 December 2016, [online](#).
- 54 Angus Grigg, ‘Australia’s Defence Department bans Chinese app Wechat’, The Australian Financial Review, 11 March 2018, [online](#) and Danielle Cave, Fergus Ryan, Tom Uren, ‘Defence says no to WeChat’, The Strategist, 13 March 2018, [online](#).
- 55 Steve Stecklow, Karen Freifeld, Sijia Jiang, ‘US ban on sales to China’s ZTE opens fresh front as tensions escalate’, Reuters, 16 April 2018, [online](#).
- 56 Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, Blase Ur, ‘Your secrets are safe: how browsers’ explanations impact misconceptions about private browsing mode’, in WWW 18: Proceedings of the 2018 World Wide Web Conference, Lyon, France, 23–27 April 2018, [online](#).

## Acronyms and abbreviations

AI	artificial intelligence
EU	European Union
SCS	social credit system



# WHAT'S YOUR STRATEGY?

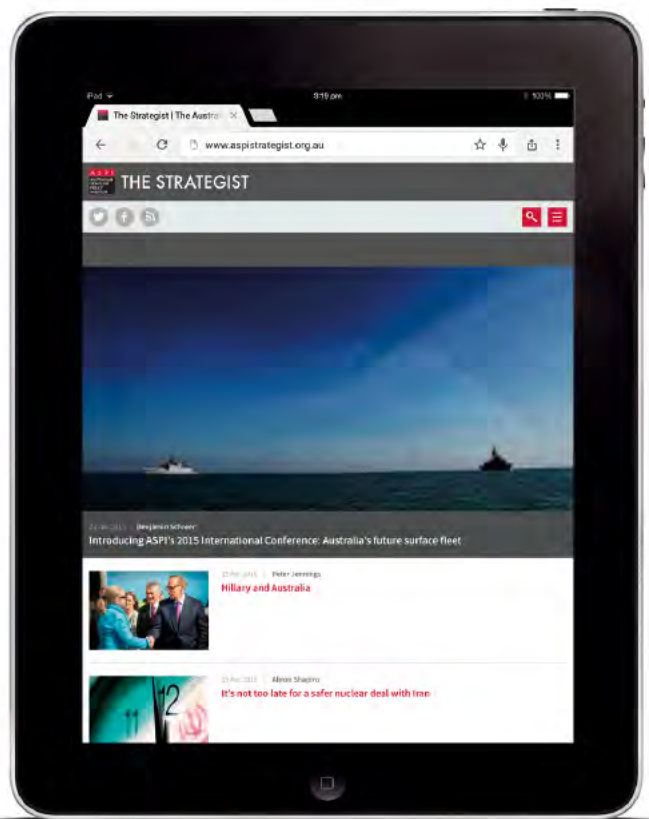


**Stay informed via the field's leading think tank,  
the Australian Strategic Policy Institute.**

**The Strategist**, ASPI's commentary and analysis website, delivers fresh ideas on Australia's defence and strategic policy choices as well as encouraging discussion and debate among interested stakeholders in the online strategy community. Visit and subscribe to an email digest at [www.aspistrategist.org.au](http://www.aspistrategist.org.au).

 [facebook.com/ASPI.org](https://facebook.com/ASPI.org)

 [@ASPI\\_org](https://twitter.com/ASPI_org)



Supported by



THALES



To find out more about ASPI go to [www.aspi.org.au](http://www.aspi.org.au)  
or contact us on 02 6270 5100 and [enquiries@aspi.org.au](mailto:enquiries@aspi.org.au).





# EXHIBIT 16

# Technological entanglement

Cooperation, competition and the dual-use dilemma in artificial intelligence

Elsa B. Kania





## About the author

**Elsa B. Kania** an Adjunct Fellow with the Center for a New American Security's Technology and National Security Program. She focuses on Chinese defense innovation in emerging technologies in support of the Artificial Intelligence and Global Security Initiative at CNAS, where she also acts as a member of the research team for the new Task Force on Artificial Intelligence and National Security. Her research interests include Chinese military modernization, information warfare, and defense science and technology. Elsa is an independent analyst, consultant, and co-founder of the China Cyber and Intelligence Studies Institute (CCISI). She was also a 2018 Fulbright Specialist with the Australian Strategic Policy Institute's International Cyber Policy Centre. Elsa works in support of the China Aerospace Studies Institute (CASI) through its Associates Program, and she is a consulting analyst with Pointe Bello and a policy advisor for the non-profit Technology for Global Security. Elsa has been named an official "Mad Scientist" by the U.S. Army's Training and Doctrine Command.

Elsa is a graduate of Harvard College (summa cum laude, Phi Beta Kappa), where her thesis on the evolution of the PLA's strategic thinking on information warfare was awarded the James Gordon Bennett Prize. Her prior professional experience includes time with the Department of Defense, the Long Term Strategy Group, FireEye, Inc., and the Carnegie-Tsinghua Center for Global Policy. While at Harvard, she worked as a research assistant at the Belfer Center for Science and International Affairs and the Weatherhead Center for International Affairs. Elsa was a Boren Scholar in Beijing, China, and she is fluent in Mandarin Chinese.

## What is ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

## ASPI International Cyber Policy Centre

The ASPI International Cyber Policy Centre's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia-Pacific.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various sponsors.

## Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

## ASPI

Tel +61 2 6270 5100

Fax + 61 2 6273 9566

Email [enquiries@aspi.org.au](mailto:enquiries@aspi.org.au)

[www.aspi.org.au](http://www.aspi.org.au)

[www.aspistrategist.org.au](http://www.aspistrategist.org.au)

[facebook.com/ASPI.org](https://www.facebook.com/ASPI.org)

[@ASPI\\_ICPC](https://twitter.com/ASPI_ICPC)

[www.aspi.org.au/icpc/home](http://www.aspi.org.au/icpc/home)

© The Australian Strategic Policy Institute Limited 2018

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers.

First published June 2018.

**Cover image:** Illustration by James Bareham, Creative Director at *The Verge* in the article [China and the US are battling to become the world's first AI superpower](#) published 3 August 2017. ASPI ICPC has attained a non-exclusive grant to use this image for this report. This image cannot be re-published unless permission is granted by Vox Media Inc.



# Technological entanglement

Cooperation, competition and the dual-use  
dilemma in artificial intelligence

Elsa B. Kania

Policy Brief  
Report No.7/2018



# Contents

<b>What's the problem?</b>	<b>03</b>
<b>What's the solution?</b>	<b>03</b>
<b>AI 'without borders'</b>	<b>04</b>
<b>China's global AI strategy and ambitions</b>	<b>05</b>
<b>China's integrated approach to indigenous innovation</b>	<b>07</b>
<b>The dual-use dilemma in China's AI development</b>	<b>08</b>
<b>Policy considerations and recommendations</b>	<b>09</b>
<b>Notes</b>	<b>12</b>
<b>Acronyms and abbreviations</b>	<b>15</b>



## What's the problem?

Despite frequent allusions to a race—or even an ‘arms race’—in artificial intelligence (AI), US leadership and China’s rapid emergence as an AI powerhouse also reflect the reality of cooperation and engagement that extend across the boundaries of strategic competition.<sup>1</sup> Even as China and the US, the world’s emergent ‘AI superpowers’,<sup>2</sup> are increasingly competing in AI at the national level, their business, technology and research sectors are also deeply ‘entangled’ through a range of linkages and collaborations. That dynamic stems from and reflects the nature of AI research and commercialization—despite active competition, it is open and often quite collaborative.<sup>3</sup> These engagements can, of course, be mutually beneficial, but they can also be exploited through licit and illicit means to further China’s indigenous innovation and provide an asymmetric advantage.<sup>4</sup> The core dilemma is that the Chinese party-state has demonstrated the capacity and intention to co-opt private tech companies and academic research to advance national and defence objectives in ways that are far from transparent.

This has resulted in a ‘dual-use dilemma’ in which the openness that’s characteristic of science and innovation in democracies can result in unforeseen consequences, undermining the values, interests and competitiveness of the US, Australia and other like-minded nations in these strategic technologies.<sup>5</sup> These ‘entanglements’ have included ties between US tech firms and Chinese partners with military connections,<sup>6</sup> as well as cooperation between Australian universities and the Chinese People’s Liberation Army (PLA).<sup>7</sup> Despite the genuine advantages they may offer, such problematic partnerships can also result in the transfer of dual-use research and technologies that advance Chinese military modernisation, perhaps disrupting the future balance of power in the Indo-Pacific, or facilitate the party-state’s construction of surveillance capabilities that are starting to diffuse globally. These adverse externalities have troubling implications for US military advantage, authoritarian regime resilience and even the future of democracy.<sup>8</sup> How should policymakers balance the risks and benefits of such entanglement,<sup>9</sup> while enhancing competitiveness in this strategic technology?

## What's the solution?

These unique and complex dynamics require a range of policy responses that balance the risks and benefits of these partnerships, collaborations and engagements. To enhance situational awareness, policymakers should examine closely research, academic and commercial partnerships that may prove problematic, and then consider updates and revisions to national export controls, defence trade controls and investment review mechanisms as targeted countermeasures. While there is a rationale for visa screening of foreign nationals who plan to study or research sensitive technologies, restrictions should be imposed only on the basis of evidence of direct and clear connections to foreign militaries, governments or intelligence services,<sup>10</sup> and scrutiny should focus more on organisations engaging in talent recruitment that are linked to the Chinese central and local governments or to the Chinese Communist Party (CCP). At the same time, there are compelling reasons to sustain scientific cooperation, with safeguards for risk mitigation, including transparency and the protection of sensitive data.

Critically, the US and Australia must pursue policies that actively enhance the dynamism of their own innovation ecosystems to ensure future competitiveness. It is vital to bolster declining support for science and commit to increasing funding for basic research and the long-term development of strategic technologies. Given the criticality of human capital, governments should prioritise improving the accessibility and affordability of STEM education at all levels, while attracting and welcoming talent through favourable immigration policies. In this quest for competitive advantage, the US and Australia must also pursue closer public-private partnerships and expand alliance cooperation on defence innovation.

## AI ‘without borders’

Today, national competition in AI is intensifying at a time when the engine for technological innovation in such dual-use technologies has shifted from governments to commercial enterprises. In today’s complex, globalised world, flows of talent, capital and technologies are rapid, dynamic and not readily constrained by borders. Chinese investments and acquisitions in Silicon Valley—and US investments in China—are sizable and increasing, despite intense concerns about the security risks of such investments,<sup>11</sup> which have motivated reforms to the Committee on Foreign Investment in the United States (CFIUS) and could result in discretionary implementation of China’s national security review mechanism in response.<sup>12</sup> This increased globalisation of innovation ecosystems has proven beneficial to AI development, and dynamic US and Chinese companies are emerging as world leaders in the field.

Increasingly, these enterprises are quite international in their outlook, presence and workforce while engaging in a global quest for talent.<sup>13</sup> For the time being, the US remains the centre of gravity for the top talent in AI, and Silicon Valley is the epicentre of this talent ‘arms race’.<sup>14</sup> While currently confronting major bottlenecks in human capital, China has great potential, given the number of graduates in science and engineering and the range of new training and educational programs dedicated to cultivating AI talent.<sup>15</sup> At the same time, the Chinese government is actively incentivising the return and recruitment of ‘strategic scientists’ via state talent plans.<sup>16</sup> At the forefront of the AI revolution, Baidu and Google epitomise in their strategic decisions and activities the linkages and interconnectivity among such global centres of innovation as Silicon Valley and Beijing.<sup>17</sup>

Baidu has prioritised AI and has emerged as a leading player in this domain. It created the Institute for Deep Learning in Beijing in 2013 and then established its Silicon Valley Artificial Intelligence Laboratory (SVAIL), which employs about 200 people, in 2014.<sup>18</sup> Baidu’s CEO, Li Yanhong (李彦宏, or Robin Li), advocated as early as 2015, prior to the Chinese Government’s decision to prioritise AI, for a ‘China Brain’ plan that would involve a massive national initiative in AI, including welcoming military funding and involvement.<sup>19</sup> Increasingly, Baidu has actively invested in and acquired US AI start-ups, including xPerception and Kitt.ai,<sup>20</sup> while seeking to expand its US-based workforce. The company has stated that Silicon Valley ‘is becoming increasingly important in Baidu’s global strategy as a base for attracting world-class talent.’<sup>21</sup> In March 2017, Baidu announced plans to establish a second laboratory in Silicon Valley, which is expected to add another 150 employees.<sup>22</sup> Notably, Baidu has also launched the Apollo project, which is a collaborative initiative to advance the development of self-driving cars that involves more than 100 tech companies and automakers, including Ford, NVIDIA, and Microsoft.<sup>23</sup> At the same time, Baidu is engaged in research on military applications of AI, particularly command and control.<sup>24</sup>

Google remains at the forefront of AI development, leveraging an international presence and global workforce. Beyond Silicon Valley, Google has opened AI research centres in Paris, New York and Tokyo,<sup>25</sup> and it will soon add Beijing and then Accra, Ghana.<sup>26</sup> When Google announced the opening of the Google AI China Center in December 2017, chief scientist Fei-Fei Li declared, ‘I believe AI and its benefits have no borders. Whether a breakthrough occurs in Silicon Valley, Beijing, or anywhere else, it has the potential to make everyone’s life better for the entire world.’<sup>27</sup> She emphasised, ‘we want to work with the best AI talent, wherever that talent is, to achieve’ Google’s mission.<sup>28</sup> Google’s decision to expand its presence and activities in China, after withdrawing its search product from the market due to concerns over censorship, surveillance and the theft of intellectual property via cyber espionage in 2010,<sup>29</sup> reflects this enthusiasm for the potential of future talent in China—and probably the availability of a sizable market and massive amounts of data as well.<sup>30</sup> At the same time, this decision presents an interesting counterpoint to Google’s recent issuing of a statement of principles that included a commitment not to build technologies used for surveillance.<sup>31</sup> Given the dual-use nature of these technologies, Google’s choice to engage in China may involve risks and raise ethical concerns,<sup>32</sup> especially considering the Chinese party-state’s agenda for and approach to AI.

## China’s global AI strategy and ambitions

At the highest levels, the Chinese Government is prioritising and directing strong state support to AI development, leveraging and harnessing the dynamism of tech companies that are at the forefront of China’s AI revolution. The New Generation Artificial Intelligence Development Plan (新一代人工智能发展规划), released in July 2017, recognised this strategic technology as a ‘new focal point of international competition’, declaring China’s intention to emerge as the world’s ‘premier AI innovation centre’ by 2030.<sup>33</sup> The Three-Year Action Plan to Promote the Development of New-Generation Artificial Intelligence Industry (促进新一代人工智能产业发展三年行动计划) (2018–2020), released in December 2017, called for China to achieve ‘major breakthroughs in a series of landmark AI products’ and ‘establish international competitive advantage’ by 2020.<sup>34</sup> China’s central and local governments are providing high and ever-rising levels of funding for research and development on next-generation AI technologies, while seeking to create a robust foundation for innovation by introducing new talent and education initiatives, developing standards and regulatory frameworks, and supporting the availability of data, testing and cloud platforms.<sup>35</sup>

China’s ambition to ‘lead the world’ in AI is self-evident.<sup>36</sup> These plans and policies should be contextualised by its tradition of techno-nationalism and current aspirations to emerge as a ‘science and technology superpower’ (科技强国).<sup>37</sup> In recent history, indigenous Chinese innovations, particularly defence technological developments, have been advanced and accelerated through licit and illicit means of tech transfer, including extensive industrial espionage.<sup>38</sup> However, pursuing a new strategy of innovation-driven development,<sup>39</sup> China is actively seeking to progress beyond more absorptive approaches to innovation and instead become a pioneer in emerging technologies, including through increasing investment in basic research.<sup>40</sup> To further this agenda, the Chinese government is avidly targeting overseas students and scientists, offering considerable incentives via talent plans and engaging in recruitment via ‘talent bases’ and organisations that are often linked to the CCP or to central or local governments.<sup>41 42</sup>

At this point, the success of these initiatives remains to be seen, and there are even reasons to question whether an AI bubble may arise due to excessive enthusiasm and investments. Although China's future potential for innovation shouldn't be dismissed or discounted, this 'rise' in AI often generates alarm and exuberance that can distract from recognition of major obstacles that remain. As its plans openly admit, China continues to lag behind the US in cutting-edge research and is attempting to compensate for current shortfalls in human capital.<sup>43</sup> Notably, China confronts continued difficulties in the development of indigenous semiconductors,<sup>44</sup> which will be critical to the hardware dimension of future advances in AI,<sup>45</sup> despite billions in investment and quite flagrant attempts to steal intellectual property from US companies.<sup>46</sup>

While gradually becoming more capable of truly independent innovation, China also intends to coordinate and optimise its use of both domestic and international 'innovation resources'.<sup>47</sup> Notably, the New Generation AI Development Plan calls for an approach of 'going out' (走出去) involving overseas mergers and acquisitions, equity investments and venture capital, along with the establishment of R&D centres abroad.<sup>48</sup> For instance, a subsidiary of the China Electronics Technology Group Corporation (CETC), a state-owned defence conglomerate, established an 'innovation centre' in Silicon Valley in 2014, which seeks to take advantage of that ecosystem with a focus on big data and other advanced information technologies.<sup>49</sup> In Australia,<sup>50</sup> CETC established a joint research centre with the University of Technology Sydney (UTS), which will focus on AI, autonomous systems and quantum computing, in April 2017.<sup>51</sup> Starting in 2018, CETC's Information Science Academy is also funding a project at UTS on 'A Complex Data Condition Based Public Security Online Video Retrieval System', which could have clear applications in surveillance.<sup>52</sup> There have been extensive collaborations on dual-use AI technologies between PLA researchers from the National University of Defence Technology and academics at UTS, the University of New South Wales and the Australian National University.<sup>53</sup> Meanwhile, Huawei is actively funding research and pursuing academic partnerships in the US and Australia, including through its Huawei Innovation Research Program.<sup>54</sup> China's 'One Belt, One Road' strategy is also concentrating on scientific and technological cooperation, including educational exchanges and research partnerships, such as a new Sino-German joint AI laboratory.<sup>55</sup> Some of these new collaborations will focus on robotics and AI technologies, often enabling access to new sources of data that may facilitate China's emergence as a global leader in AI development.<sup>56</sup> In certain instances, China's provision of funding to these initiatives may also reorient the direction of research based on its own priorities.<sup>57</sup>

As China seeks to advance indigenous innovation, the strategy of 'going out' is complemented by a focus on 'bringing in' (引进来) to ensure that vital talent and technologies are drawn back into China.<sup>58</sup> At the same time, the Chinese government is evidently seeking to ensure that innovation 'made in China' will stay in China. As the US undertakes reforms to CFIUS, China could respond by recalibrating the implementation of its own national security review process, which is ambiguous enough to allow for great discretion in its application, pursuant to an expansive concept of national or state security (国家安全).<sup>59</sup> Notably, the State Council has also issued a new notice that requires that scientific data generated within China be submitted to state data centres for review and approval before publication.<sup>60</sup> The policy purports to promote open access to and sharing of scientific data within China, while creating ambiguous new restrictions that, depending upon their implementation, could render future cooperation asymmetrical in its benefits.<sup>61</sup> Given these factors, while opportunities for research cooperation should often be welcomed, it is also important to ensure transparency regarding the research and intellectual property that may result from it, as well as the security of valuable or sensitive datasets.

## China's integrated approach to indigenous innovation

In pursuit of its dreams of AI dominance, China is pioneering a new paradigm of indigenous innovation that takes advantage of critical synergies through creating mechanisms for deeper integration among the party-state, technology companies and the military. The CCP seeks not only to support private Chinese companies in their quest for innovation but also to control and guide them, ensuring that the companies serve the needs of the party and don't become a threat to it. China's 'champions' in AI—Baidu, Alibaba, Tencent and iFlytek—are at the forefront of innovation in the field, and this 'national team' will be supported and leveraged to advance state objectives and national competitiveness.<sup>62</sup> For instance, Baidu is leading China's National Engineering Laboratory for Deep Learning Technologies and Applications (深度学习技术及应用国家工程实验室),<sup>63</sup> and iFlytek is leading the State Key Laboratory of Cognitive Intelligence (认知智能国家重点实验室).<sup>64</sup> It seems likely that the research in these new laboratories will be directed to dual-use purposes. These champions will also undertake the development of new open innovation platforms in AI: Baidu will be responsible for autonomous vehicles, Alibaba Cloud (Aliyun) for smart cities, Tencent for medical imaging and iFlytek for smart voice (e.g., speech recognition, natural-language processing, machine translation, etc.).<sup>65</sup> The platforms will be piloted in the Xiong'an New Area, a development southwest of Beijing that's intended to be a futuristic demonstration of Chinese innovation and to showcase AI technologies and applications in action.<sup>66</sup>

Meanwhile, Xi Jinping has recently reaffirmed the Mao-era sentiment that 'the party leads everything', and China's advances in AI must also be understood in the context of this system, in which the CCP is steadily increasing its control over private companies.<sup>67</sup> In recent years, the CCP has introduced representatives of party branches and committees into notionally private companies,<sup>68</sup> which have started to undertake more active 'party building' (党建) activities that are intended to expand the CCP's presence and influence.<sup>69</sup> Just about every major tech company, including Baidu, Alibaba, Tencent, Sohu, Sina and NetEase, has a party secretary, who is often a fairly senior figure within the company, and new requirements may even require all listed companies to 'beef up party building'.<sup>70</sup> For example, in March 2017, the CCP Capital Internet Association Commission (中共首都互联网协会委员会) convened a party committee expansion meeting and a work meeting on grassroots party building that brought together the leaders of many prominent companies.<sup>71</sup> At the meeting, Baidu Party Secretary Zhu Guang (朱光), who is also a Senior Vice President responsible for public relations and government affairs,<sup>72</sup> talked about innovation in 'party building work', including the development of a mobile solution for 'party building'. He committed Baidu to leveraging its capabilities in big data and AI applications, as well as its 'ecological advantage', to enhance the effectiveness of such efforts.<sup>73</sup> This blurring of the boundaries between the party-state and its champions may create a tension between national strategic objectives and these companies' global commercial interests.<sup>74</sup> Increasingly, the CCP is even attempting to extend its reach into, and authority over, foreign companies operating in China.<sup>75</sup>



## The dual-use dilemma in China's AI development

The future trajectory of AI in China will inherently be shaped and constrained by the interests and imperatives of the party-state, and international collaboration with Chinese research institutions and corporate actors needs to be understood, and engaged in, with this important context in mind. Critically, AI will enhance both economic development and military modernization, while reinforcing the party's ability to control its population through domestic surveillance, all of which are integral to the regime's security and legitimacy. China's AI plans and policies include the concern that AI will remain 'secure and controllable' (安全, 可控), given the risks of societal disruption, while highlighting the importance of AI 'to elevate significantly the capability and level of social governance, playing an irreplaceable role in effectively maintaining social stability', thus bolstering regime security.<sup>76</sup> Indeed, the pursuit of such 'innovations' in social governance through big data and AI has included the construction of predictive policing and surveillance capabilities, often developed with the assistance of start-ups such as SenseTime and Yitu Tech, that have often been abused, particularly in Xinjiang.<sup>77</sup> Given the party's attempts to extend its reach—and the trend towards deeper integration in civilian and military AI efforts in China—it can be difficult to disentangle notionally commercial activities from those directly linked to the party-state's agendas for social control, indigenous innovation and military modernisation.

China seeks to take full advantage of the dual-use nature of AI technologies through a national strategy of 'military-civil fusion' (军民融合). This high-level agenda is directed by the CCP's Military-Civil Fusion Development Commission (中央军民融合发展委员会) under the leadership of President Xi Jinping himself.<sup>78</sup> Through a range of policy initiatives, China intends to ensure that advances in AI can be readily turned to dual-use applications to enhance national defence innovation. Although the effective implementation of military-civil fusion in AI may involve major challenges, this approach is presently advancing the creation of mechanisms and institutions that can integrate and coordinate R&D among scientific research institutes, universities, commercial enterprises, the defence industry and military units.<sup>79</sup> For instance, in June 2017, Tsinghua University announced its plans to establish a Military-Civil Fusion National Defence Peak Technologies Laboratory (清华大学军民融合国防尖端技术实验室) that will create a platform for the pursuit of dual-use applications of emerging technologies, especially AI.<sup>80</sup> Notably, in March 2018, China's first 'national defence science and technology innovation rapid response small group' (国防科技创新快速响应小组) was launched by the CMC Science and Technology Commission in Shenzhen,<sup>81</sup> and is intended to 'use advanced commercial technologies to serve the military.'<sup>82</sup>

China's AI 'national champions' may often be engaged in support of this agenda of military-civil fusion. Notably, in January 2018, Baidu and the 28<sup>th</sup> Research Institute of the China Electronics Technology Group's (CETC), a state-owned defence conglomerate, established the Joint Laboratory for Intelligent Command and Control Technologies (智能指挥控制技术联合实验室), located in Nanjing.<sup>83</sup> The CETC 28<sup>th</sup> Research Institute is known as a leading enterprise in the development of military information systems, specializing in the development of command automation systems,<sup>84</sup> and it seeks to advance the use of new-generation information technology in defence 'informatization' (信息化).<sup>85</sup> This partnership is directly linked to China's national strategy of military-civil fusion, leveraging the respective advantages of CETC and Baidu to take advantage of the potential of big data, artificial

intelligence, and cloud computing. Going forward, the new joint laboratory will focus on increasing the level of ‘intelligentization’ (智能化) in command information systems, as well as designing and developing new-generation command information systems ‘with intelligentization as the core.’ Baidu’s involvement in this new laboratory reflects its active contribution to military-civil fusion, a strategy that is resulting in a further blurring of boundaries between commercial and defence developments.

## Policy considerations and recommendations

There is no single or simple solution, and policy responses must take into account the inherent complexities of these global dynamics, which necessitate highly targeted and nuanced measures to mitigate risk.<sup>86</sup> At the same time, real and serious concerns about China’s exploitation of the openness of our democracies must not lead to reactive or indiscriminate approaches that could cause collateral damage to the inclusivity and engagement that are critical to innovation. The benefits of scientific collaboration are compelling, and continued cooperation should be supported, with appropriate awareness and safeguards. In future, the quest to achieve an advantage in emerging technologies will only intensify, and the US and Australia must also look to enhance their own competitiveness in these strategic technologies.<sup>87</sup> The options for policy response include, but aren’t limited to, the measures detailed below.

### Policy recommendation: Strengthen targeted, coordinated countermeasures.

1. Review recent and existing research and commercial partnerships on strategic technologies that involve support and funding from foreign militaries, governments or state-owned/supported enterprises, evaluating the dual-use risks and potential externality outcomes in each case.
  - Evaluate early-stage research to determine the likelihood that it may turn out to have disruptive dual-use implications in the future.
  - Present a public report with findings and recommendations to raise awareness and ensure transparency.
  - Continue to push back against forced tech transfer in joint ventures.<sup>88</sup>
2. Explore updates and revisions to national export controls, defence trade controls and investment review mechanisms that take into account the unique challenges of dual-use commercial technologies; communicate those updates clearly and publicly to relevant stakeholders.
  - Share lessons learned and pursue coordination with allies and partners to account for the global scope and scale of these dynamics.
  - Ensure that these restrictions are applied to sensitive datasets associated with AI development, including data used for training purposes.

3. Engage in visa screening of foreign nationals who plan to study or research sensitive or strategic technologies, targeting scrutiny on the basis of whether or not students or researchers have direct and clear connections to foreign militaries, governments or intelligence services.
  - Deny visas to those who are determined to be likely to leverage their studies or research in support of a foreign military that is not a security partner.
  - Incorporate an independent review mechanism into the process to assess evidentiary standards and mitigate risks of bias in visa determinations.
4. Identify organisations engaging in talent recruitment that are linked to the Chinese central and local governments or to the CCP, and require their registration as foreign agents where appropriate.
5. Enhance counterintelligence capabilities, particularly by augmenting language and technical expertise.

**Policy recommendation: Encourage best practices and safeguards for risk mitigation in partnerships and collaborations, with a particular focus on universities.**

6. Introduce stricter accountability and reporting requirements, managed by departments of education, which make transparent international sources of funding for research strategic technologies
7. Engage in outreach to companies, universities and think tanks in order to highlight the potential for risk or unintended externalities in joint ventures and partnerships, including through developing and presenting a series of case studies based on past incidents.
8. Propose best practices for future academic collaborations and commercial partnerships, including transparency about the terms for scientific data and intellectual property, as well as clear standards on ethics and academic freedom.
  - Identify favourable domains to sustain open collaboration and engagement, such as issues of safety and standards.
9. Introduce, or where appropriate adjust, policies or guidelines restricting those who work for national or military research institutes and laboratories or receive public funding at a certain level from organisations accepting funding from or collaborating with a foreign military, state-owned enterprise or 'national champion' that is not an ally.

**Policy recommendation: Go on the offensive through policies to enhance national competitiveness in technological innovation.**

10. Increase and commit to sustaining funding for basic research and the long-term development of AI technologies.
11. Prioritise improving the accessibility and affordability of STEM education at all levels, including creating new scholarships to support those studying computer science, AI and other priority disciplines.

12. Sustain openness to immigration, welcoming graduating students and talented researchers, while potentially offering a fast-track option to citizenship.
13. Pursue closer public-private partnerships through creating new incubators and institutions that create a more diverse and dynamic community for innovation.<sup>89</sup>
  - Encourage dialogue and engagement between the tech and defence communities on issues of law, ethics and safety.
14. Explore the expansion of alliance coordination and cooperation in defence innovation, including collaboration in research, development and experimentation with new technologies and their applications.
15. Engage with like-minded nations to advance discussions of AI ethics and standards, as well as potential normative and governance frameworks.

# Notes

- 1 Elsa B Kania, 'The pursuit of AI is more than an arms race', *Defense One*, 19 April 2018, [online](#).
- 2 Kai-Fu Lee, *AI superpowers: China, Silicon Valley, and the new world order*, Houghton Mifflin Harcourt, 2018, forthcoming.
- 3 For prior writing on these issues, see Elsa Kania, 'Tech entanglement—China, the United States, and artificial intelligence', *Bulletin of the Atomic Scientists*, 5 February 2018, [online](#).
- 4 For a detailed study on these issues, see Office of the United States Trade Representative, Executive Office of the President, *Findings of the investigation into China's acts, policies, and practices related to technology transfer, intellectual property, and innovation under section 301 of the Trade Act of 1974*, 22 March 2018, [online](#).
- 5 Throughout this policy paper, I use the concept of 'entanglement' to characterise the close linkages and range of mechanisms for engagement in the research, development and commercialisation of technologies, particularly in the context of AI. In historical perspective, entanglement, whether in alliances or economics, has proven to be both a factor restraining conflict and a major source of friction.
- 6 'US tech companies and their Chinese partners with military ties', *New York Times*, 30 October 2015, [online](#).
- 7 Clive Hamilton, Alex Joske, 'Australian universities are helping China's military surpass the United States', *Sydney Morning Herald*, 27 October 2017, [online](#).
- 8 Josh Chin, Clément Bürge, 'Twelve days in Xinjiang: how China's surveillance state overwhelms daily life', *Wall Street Journal*, 19 December 2017, [online](#).
- 9 For the purposes of this paper, I target the proposed policy responses to the context of the US and Australia, but the suggested responses are intended to be applicable to other liberal democratic states.
- 10 These screenings should not extend to outright restrictions or unwarranted discrimination on the basis of nationality. For a compelling perspective on the imperative of keeping the door open to foreign scientists, read Yangyang Cheng, 'Don't close the door on Chinese scientists like me', *Foreign Policy*, 4 June 2018, [online](#).
- 11 For a notable report on these concerns, see Michael Brown, Pavneet Singh, *China's technology transfer strategy: how Chinese investments in emerging technology enable a strategic competitor to access the crown jewels of US innovation*, Defense Innovation Unit Experimental (DIUx), January 2018, [online](#).
- 12 'CFIUS reform: House and Senate committees unanimously clear bills that would greatly expand CFIUS authority', *Lexology*, 1 June 2018, [online](#). National/State Security Law of the People's Republic of China [中华人民共和国国家安全法], 7 July 2015, [online](#). For further discussion of the concept of 'state security', see Samantha Hoffman, 'China's state security strategy: "everyone is responsible"', *The Strategist*, 11 December 2017, [online](#).
- 13 For an interview that describes the campaign from the perspective of an organiser, see 'Tech workers versus the Pentagon', *Jacobin*, 6 June 2018, [online](#).
- 14 For a discussion of these plans and policies, see Elsa Kania, 'China's AI talent arms race', *The Strategist*, 23 April 2018, [online](#).
- 15 Kania, 'China's AI talent arms race'.
- 16 Fan Yang, 'Surveying China's science and technology human talents programs', *Study of Innovation and Technology in China*, 2015, [online](#).
- 17 For insights on the linkages between Silicon Valley and China, see Matt Sheehan's commentaries on the subject, including 'Silicon Valley's China paradox', *Macro Polo*, 26 June 2017, [online](#).
- 18 See 'Baidu, USA', *LinkedIn*, [online](#); 'China's Baidu increases US presence with new Silicon Valley office', *South China Morning Post*, 25 March 2017, [online](#).
- 19 Bien Perez, "'China Brain' project seeks military funding as Baidu makes artificial intelligence plans', *South China Morning Post*, 3 March 2015, [online](#); 'Li Yanhong: Establishing the "China Brain" plan to promote our nation's AI development' [李彦宏: 设立“中国大脑”计划推进我国人工智能发展], *Xinhua*, 9 March 2015, [online](#).
- 20 'China's Baidu buys US computer vision startup amid AI push', *Reuters*, 13 April 2017, [online](#); Ingrid Lunden, 'Baidu acquires natural language startup Kitt.ai, maker of chatbot engine ChatFlow', *Tech Crunch*, 5 July 2017, [online](#).
- 21 Lunden, 'Baidu acquires natural language startup Kitt.ai, maker of chatbot engine ChatFlow'.
- 22 'China's Baidu increases US presence with new Silicon Valley office', *South China Morning Post*, 25 March 2017, [online](#).
- 23 The official website of the project, [online](#). For more reporting on the launch of this program, see 'Baidu pledges to design your driverless car to "know you, and be your companion"', *South China Morning Post*, 15 August 2017, [online](#).
- 24 "China Electronics Science and Technology Group and Baidu Company established the "Joint Laboratory for Intelligent Command and Control Technology" to promote military-civil fusion in the field of new technologies" [中国电科28所与百度公司成立“智能指挥控制技术联合实验室”推动军民融合向新技术领域纵深迈进], January 23, 2018, [online](#).
- 25 Justina Crabtree, 'Google's next AI research center will be its first on the African continent', *CNBC*, 14 June 2018, [online](#).
- 26 Jeff Dean, Moustapha Cisse, 'Google AI in Ghana', *The Keyword*, [online](#).
- 27 Fei-Fei Li, 'Opening the Google AI China Center', *The Keyword*, 13 December 2017, [online](#).
- 28 Fei-Fei Li, 'Opening the Google AI China Center'.
- 29 For further details on these incidents, see Erica Naone, 'Google reveals Chinese espionage efforts', *MIT Technology Review*, 13 January 2010, [online](#).
- 30 For context, including the rationale from top current and former leaders at Google, see 'Google has a new plan for China (and it's not about search)', *Bloomberg*, 30 October 2017, [online](#).
- 31 Sundar Pichai, 'AI at Google: our principles', *The Keyword*, 7 June 2017, [online](#).



- 32 For one argument about the moral dimension of this issue, see Matt Sheehan, 'Google China 2.0 and the ethics of AI engagement', *Macro Polo*, 17 January 2018, [online](#).
- 33 *State Council notice on the issuance of the New Generation AI Development Plan* [国务院关于印发新一代人工智能发展规划的通知], 20 July 2017, [online](#).
- 34 *MIIT notice regarding the release of the Three Year Action Plan to Promote the Development of New-Generation Artificial Intelligence Industry (2018–2020)* [工业和信息化部关于印发《促进新一代人工智能产业发展三年行动计划(2018–2020年)》的通], 14 December 2017, [online](#).
- 35 Elsa Kania, 'China's AI agenda advances', *The Diplomat*, 14 February 2018, [online](#).
- 36 *State Council notice on the issuance of the New Generation AI Development Plan*.
- 37 'Scientific and technological innovation, a powerful engine for a world-class military' [科技创新·迈向世界一流军队的强大引擎], *Xinhua*, 15 September 2017, [online](#).
- 38 William C Hannas, James Mulvenon, Anna B Puglisi, *Chinese industrial espionage: technology acquisition and military modernisation*, Routledge, 2013.
- 39 'Xi Jinping: Comprehensively advance an innovation driven development strategy, promote new leaps in national defence and military construction' [习近平: 全面实施创新驱动发展战略 推动国防和军队建设实现新跨越], *Xinhua*, 13 March 2016, [online](#). See also the official strategy released on innovation-driven development: 'CCP State Council releases the "National Innovation-Driven Development Strategy Guidelines"' [中共中央 国务院印发《国家创新驱动发展战略纲要》], *Xinhua*, 19 May 2016, [online](#).
- 40 *State Council's several opinions regarding comprehensively strengthening basic research* [国务院关于加强基础科学研究的若干意见], 31 January 2018, [online](#).
- 41 For more context on talent plans, see Liming Salvino, 'China's talent recruitment programs: the road to a Nobel Prize and world hegemony in science?', *Study of Innovation and Technology in China*, 2015, [online](#).
- 42 For an example in Silicon Valley, see, for instance, 'Torch Hi-tech Zone Overseas Offshore Innovation Base (Silicon Valley) signing and opening ceremony held' [火炬高新区海外离岸创新基地(硅谷)签约暨揭牌仪式举行], *Xiamen Daily*, 30 September 2017, [online](#).
- 43 *State Council notice on the issuance of the New Generation AI Development Plan*.
- 44 Paul Triolo, Jimmy Goodrich, 'From riding a wave to full steam ahead', *New America*, 28 February 2018, [online](#).
- 45 Jimmy Goodrich, 'China's 13th Five-Year Plan: opportunities and challenges for the US semiconductor industry', written testimony prepared for the US–China Economic and Security Review Commission hearing on China's 13th Five-Year Plan, 27 April 2016, [online](#).
- 46 See, for instance, Keshia Hannam, 'Four US engineers charged with trying to steal chip designs for a Chinese startup', *Fortune*, 7 December 2017, [online](#).
- 47 *State Council notice on the issuance of the New Generation AI Development Plan*.
- 48 *Ibid.*
- 49 The subsidiary in question is as the CETC Software Information Services Co., Ltd. (中电科软件信息服务有限公司). See "About Us," [online](#).
- 50 Some of the other notable collaborations and partnerships in Australia include the following. During 2011 and 2012, the University of Technology Sydney established five research centres with Chinese universities, including the UTS – Shanghai Jiaotong University Joint Research Centre for Intelligent Systems, the UTS – Beijing Institute of Technology Joint Research Centre for Data Mining and Service Technology, and the UTS – Tsinghua University Joint Research Centre for Quantum Computation and Artificial Intelligence. As of 2017, the UTS – Northwestern Polytechnical University International Joint Laboratory for Digital Media and Intelligent Networks, which will work on research directions including AI, computer vision, machine learning, pattern recognition, image processing, was also established. Each of these Chinese partner universities is known to engage in some military and defence-related R&D. In April 2016, the Torch Innovation Precinct at the University of New South Wales was established as a joint China–Australia science and technology partnership, receiving \$100 million in funding, including for research on military-relevant technologies, including unmanned systems. As of June 2017, the University of Sydney launched a new \$7.5 million research centre, led by Professor Dacheng Tao, who has worked extensively with PLA researchers, in partnership with world-leading robotics company UBTECH Robotics, to explore AI research.
- 51 Danielle Cave, Brendan Thomas-Noone, 'CSIRO cooperation with Chinese defence contractor should raise questions', *The Guardian*, 3 June 2017, [online](#).
- 52 *CETC: a complex data condition based public security online video retrieval system*, University of Technology Sydney, [online](#).
- 53 Clive Hamilton, Alex Joske, 'Australian universities are helping China's military surpass the United States', *Sydney Morning Herald*, 27 October 2017, [online](#). I am indebted to Alex Joske for his insights and excellent research on these issues.
- 54 'Huawei in America: university partners', Huawei, [online](#).
- 55 'By 2030, the "One Belt, One Road" science and technology cooperation network system will be basically established' [2030年将基本建成“一带一路”科技合作网络体系], *Economics Daily*, 10 May 2017, [online](#); 'Qingdao's Science and Technology "bringing in" and "going out"' [青岛科技的“引进来”和“走出去”], *Jiaodong*, 19 May 2018, [online](#).
- 56 'Vice Minister Li Meng led a delegation to visit Greece, Sweden and Denmark' [李萌副部长率团访问希腊·瑞典·丹麦], Ministry of Science and Technology, 12 June 2018, [online](#).
- 57 For a potential example of these dynamics, see Chinese funding for the Torch Innovation Precinct at the University of New South Wales. Thanks so much to Alex Joske for raising this point.
- 58 'Qingdao's Science and Technology "bringing in" and "going out"'.
- 59 For a discussion of the legal questions that this process raises, see 'China publishes final rules on the National Security Review of Foreign Investment in Chinese Companies', *Jones Day*, September 2011, [online](#); 'National security review creates FDI hurdle', *Covington and Burling LLC*, 13 July 2015, [online](#); National/State Security Law of the People's Republic of China. For further discussion of the concept of 'state security', see Hoffman, 'China's state security strategy: "everyone is responsible"'.
- 60 'State Council General Office regarding measures for the administration of scientific data' [国务院办公厅关于印发科学数据管理办法的通知], 2 April 2018, [online](#).

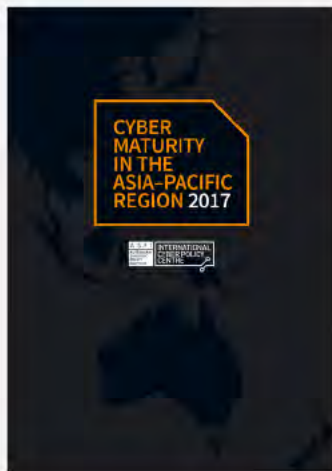
- 61 For discussion and reactions to the policy, see Dennis Normile, 'China asserts firm grip on research data', *Science*, 9 April 2018, [online](#).
- 62 'China recruits Baidu, Alibaba and Tencent to AI "national team"', *South China Morning Post*, 21 November 2017, [online](#).
- 63 'National Development and Reform Commission: Baidu to lead, BAT to build indigenous AI laboratories [发改委：百度牵头·BAT筹建“国字号”人工智能实验室], *EET*, 22 February 2017, [online](#); 'National Engineering Laboratory of Deep Learning Technologies and Applications unveiled at Baidu' [深度学习技术及应用国家工程实验室在百度揭牌], *Xinhua*, 2 March 2017, [online](#).
- 64 'Cognitive intelligence has a state key laboratory' [认知智能有了国家重点实验室], *Xinhua*, 21 December 2017, [online](#).
- 65 'AI "national team" Xiong'An debut! Will change your life' [人工智能“国家队”雄安登场！将改变你的生活], *Xiong'an*, 30 November 2017, [online](#).
- 66 'AI "national team" Xiong'An debut! Will change your life'.
- 67 Charlotte Gao, 'The CCP vows to "lead everything" once again', *The Diplomat*, 28 October 2017, [online](#); '19th Party Congress "Resolution on the Constitution of the People's Republic of China (Amendment)" [十九大关于《中国共产党章程（修正案）》的决议], *Xinhua*, 24 October 2017, [online](#).
- 68 Emily Feng, 'Chinese tech groups display closer ties with Communist party', *Financial Times*, 10 October 2017, [online](#).
- 69 David Bandurski, 'Tech firms tilt toward the party', *China Media Project*, 2 May 2018, [online](#).
- 70 'Internet companies "red flags": they are the party secretaries of BAT' [互联网公司“红旗谱”：他们是BAT公司的党委书记], 20 March 2017, [online](#).
- 71 '35 websites in Beijing conducted their first report on party building work for the first time' [北京市35家网站首次进行基层党建工作述职], 19 March 2017, [online](#).
- 72 See his biography and background as presented in English [online](#).
- 73 '35 websites in Beijing conducted their first report on party building work for the first time'.
- 74 For a great discussion of these tensions, see Danielle Cave, 'Huawei highlights China's expansion dilemma: espionage or profit?', *The Strategist*, 15 June 2018, [online](#).
- 75 Michael Martina, 'In China, the party's push for influence inside foreign firms stirs fears', *Reuters*, 24 August 2017, [online](#).
- 76 *State Council notice on the issuance of the New Generation AI Development Plan*.
- 77 Samantha Hoffman, 'Managing the state: social credit, surveillance and the CCP's plan for China', *China Brief*, 17 August 2017, [online](#); 'China: big data fuels crackdown in minority region', *Human Rights Watch*, 26 February 2018, [online](#).
- 78 'Military–Civil Integration Development Committee established' [军民融合发展委成立], *Xinhua*, 23 January 2017, [online](#).
- 79 *State Council notice on the issuance of the New Generation AI Development Plan*.
- 80 'Tsinghua starts to establish the Military–Civil Fusion National Defense Peak Technologies Laboratory' [清华启动筹建军民融合国防尖端技术实验室], *China Education Report*, 26 June 2017, [online](#).
- 81 Although the US and Australian governments can build upon and look to the precedents of arms control and export control regimes, it's also important to recognise that these existing frameworks and paradigms can be ill-suited to the challenge of technologies in which advances are driven by academic and commercial enterprises, where research is often open-sourced and readily available, and where competition for top talent extends across borders.
- 82 This team will leverage 'the innovation advantages of the Shenzhen Special Economic Zone to rapidly respond to the needs of national defence science and technology innovation through various forms and accumulate experience in promoting the formation of a flexible and highly efficient defence technology innovation value chain'.
- 83 'China Electronics Science and Technology Group and Baidu Company established the "Joint Laboratory for Intelligent Command and Control Technology" to promote military-civil fusion in the field of new technologies' [中国电科28所与百度公司成立“智能指挥控制技术联合实验室”推动军民融合向新技术领域纵深迈进], January 23, 2018, [online](#).
- 84 Ibid.
- 85 For more context on informatization, see: Elsa Kania and John Costello, "China's Quest for Informatization Drives PLA Reforms," *The Diplomat*, 4 March 2017, [online](#).
- 86 These policy responses are intended to be generalised so as to be applicable to the US, Australia and other countries confronting comparable challenges.
- 87 This policy paper concentrates on AI, but similar dynamics are in play in the cases of other emerging technologies, including biotechnology and quantum information science.
- 88 For more on this issue, see, for instance, Lee Branstetter, *China's 'forced' technology transfer problem—and what to do about it*, US–China Economic and Security Review Commission, 31 May 2018, [online](#).
- 89 For example, SOFWERX is a great example of an incubator that brings together a unique and dynamic community to advance defence innovation. For further details, see Stew Magnuson, 'SOFWERX: newest acquisition tool for special operators', *National Defense*, 1 May, 2016, [online](#).

## Acronyms and abbreviations

AI	artificial intelligence
CCP	Chinese Communist Party
CFIUS	Committee on Foreign Investment in the US
PLA	People's Liberation Army
R&D	research and development
SVAIL	Silicon Valley Artificial Intelligence Laboratory
UTS	University of Technology Sydney



## Some previous ICPC publications





# WHAT'S YOUR STRATEGY?

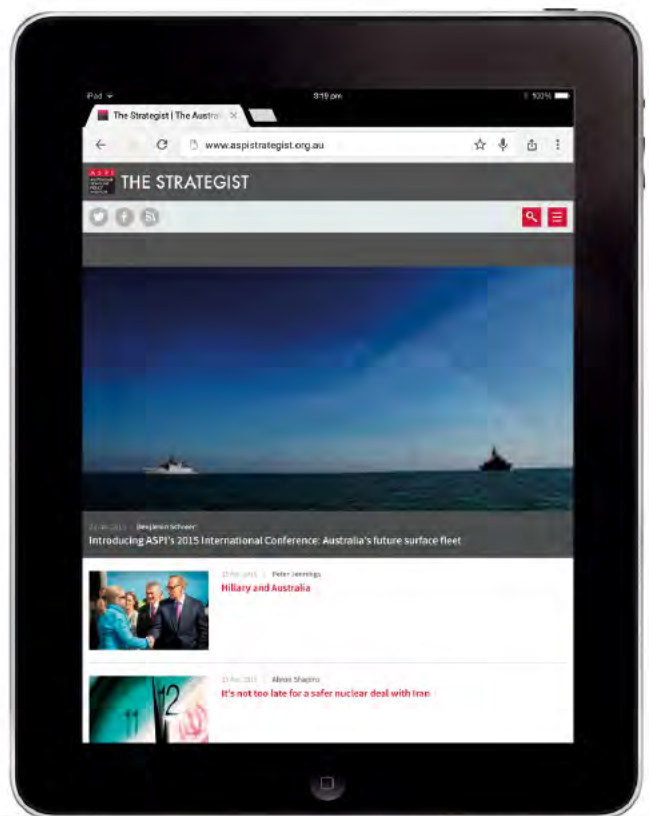


**Stay informed via the field's leading think tank,  
the Australian Strategic Policy Institute.**

**The Strategist**, ASPI's commentary and analysis website, delivers fresh ideas on Australia's defence and strategic policy choices as well as encouraging discussion and debate among interested stakeholders in the online strategy community. Visit and subscribe to an email digest at [www.aspistrategist.org.au](http://www.aspistrategist.org.au).

 [facebook.com/ASPI.org](https://facebook.com/ASPI.org)

 [@ASPI\\_org](https://twitter.com/ASPI_org)



Supported by



THALES



To find out more about ASPI go to [www.aspi.org.au](http://www.aspi.org.au)  
or contact us on 02 6270 5100 and [enquiries@aspi.org.au](mailto:enquiries@aspi.org.au).





# EXHIBIT 17



COMMENTARY / WORLD

## Worried about Huawei? Take a closer look at Tencent

BY SARAH COOK

Mar 28, 2019

**WASHINGTON** – It has long been understood that Tencent — the Chinese firm that owns WeChat and QQ, two of the world’s most widely used social media applications — facilitates Chinese government censorship and surveillance. But over the past year, the scale and significance of this activity have increased and become more visible, both inside and outside China.

During the last month alone, several events have illustrated the trend and Tencent’s close relationship with the Chinese authorities. On March 2, Dutch hacker Victor Gevers revealed that the content of millions of conversations on Tencent applications among users at internet cafes are being relayed, along with the users’ identities, to police stations across China. Just three days later, the company’s founder and chief executive, Pony Ma, took his seat among 3,000 delegates to the National People’s Congress, the country’s rubber-stamp parliament. Ma reportedly raised the issue of data privacy even as security agencies were using data from his company’s applications to root out unauthorized religious activity.

On March 16, China watcher Chenchen Zhang shared an anecdote on Twitter about a member of the Uyghur Muslim minority who was stopped at mainland China’s border with Hong Kong and interrogated for three days simply because someone on his WeChat contact list had recently “checked in” with a location setting of Mecca, Saudi Arabia. The authorities apparently feared that the Uyghur man had traveled on pilgrimage to Mecca without permission, warning that such a move could yield 15 years in prison.

As Tencent’s pattern of censorship and data-sharing with China’s repressive government continues and intensifies, now is the time to consider actions that might help protect the basic rights of all users, regardless of their location and nationality.

## **Tencent's role in China**

Founded in 1998, Tencent and its popular applications have quickly emerged as ubiquitous elements of China's communications, financial and social fabric. In January, the company declared that WeChat alone had a billion active daily users. While the company has been forced since its inception to comply with strict Chinese Communist Party information controls, the combination of growing government demands and WeChat's near market saturation in China has increased the scope and impact of its complicity.

In the realm of censorship, media reports and expert research indicate that WeChat has been refining the use of artificial intelligence to identify and delete images, which netizens commonly employ to evade censorship and surveillance of text communications. The platform has also shuttered thousands of social media accounts that produced unauthorized news and analysis.

These and other forms of censorship significantly distort the information received by Chinese users on vital topics. Analysis by researchers at Hong Kong University's WeChatscope project, which tracks deletions from some 4,000 public accounts on the platform, found that among the most censored topics in 2018 were major news stories like the U.S.-China trade dispute, the arrest in Canada of Huawei chief financial officer Meng Wanzhou, the #MeToo movement and public health scandals.

Monitoring of user activity on the platform has been made simpler by enhanced enforcement of real-name registration requirements for cellphones, the electronic payment features of WeChat, large-scale police purchases of smartphone scanners and new rules facilitating public security agencies' access to data centers. As indicated above, content from Tencent applications is being directly given to police in some cases.

This surveillance is increasingly leading to legal repercussions for ordinary users. A sample of cases tracked in Freedom House's China Media Bulletin over the past year feature penalties against numerous WeChat users for mocking President Xi Jinping, criticizing judicial officials, commenting on massive floods, sharing information about human rights abuses, or expressing views related to their persecuted religion or ethnicity, be they Uyghur Muslims, Tibetan Buddhists or Falun Gong practitioners. The punishments have ranged from several days of administrative detention to many years in prison, in some cases for comments that were ostensibly shared privately with friends. These dynamics have inevitably encouraged self-censorship on the platform.

## **Global expansion**

Although WeChat's primary user base is in China, an estimated 100 to 200 million people outside the country use the messaging service. Among them are millions of members of the Chinese diaspora in countries like Canada, Australia and the United States, but there is also broader expansion in much of Asia. Malaysia is reportedly home to 20 million WeChat users, out of a population of 31 million. In Thailand, an estimated 17 percent of the population has a WeChat account. In Mongolia, WeChat was the second most downloaded application in 2017. Merchants in Myanmar's Shan state along the border with China have taken up the app and the number of retailers in Japan that accept WePay (mostly when serving Chinese tourists) increased 35-fold last year. Tencent recently purchased a \$150 million stake in the news aggregator Reddit and is eyeing an entrance into the online video market in Taiwan, according to Taiwanese officials.

Evidence that politicized censorship and surveillance may affect Tencent users outside China has begun to emerge. A 2016 study by Citizen Lab found that conversations between an overseas user and a contact inside China were subject to certain forms of keyword censorship, and that once an account is registered with a Chinese phone number, it remains subject to Chinese controls even outside the country.

In Australia, a more recent study of news sources available to the Chinese diaspora found negligible political coverage of China on the WeChat channels of Chinese-language news providers. Incredibly, between March and August 2017, none of the WeChat channels published a single article on Chinese politics, despite the run-up to the important 19th Party Congress that fall. In Canada, WeChat censors have deleted a member of Parliament's message to constituents praising Hong Kong's Umbrella Movement protesters, manipulated dissemination of news reports related to Meng's arrest, and blocked broader media coverage of Chinese government corruption and leading officials.

Amid a crackdown in Xinjiang, Chinese police have also harnessed WeChat to connect with overseas Uyghurs, demand personal information or details about activists and insert state monitors into private groups.

## **How to respond**

Regardless of whether Tencent is a reluctant or an eager accomplice to the Chinese government's repressive policies, the reality is that Tencent employees can be expected to censor, monitor and report private communications and personal data, in many cases leading to innocent people's arrest and torture. This should be the starting point for anyone considering using, regulating, or investing in the company's services.



For those inside China, it is nearly impossible today to function without using WeChat to some extent. But users would be well advised to exercise caution, restricting the application to its most practical functions and consulting available guides on enhancing digital security and accessing information on current affairs more safely.

Users outside China, particularly those without family or friends on the mainland, should rethink whether WeChat is really essential to their daily lives. Individuals who do communicate with personal contacts in China can help protect them by directing them to more secure applications if a sensitive topic comes up, or using homonyms to replace potentially problematic terms, as some journalists have reported doing. Users in the Chinese diaspora should explore ways of expanding their sources of news and information beyond what is available on WeChat.

As governments around the world try to tackle problems related to “fake news,” political manipulation and weak data protections on social media platforms like Facebook and Twitter, Chinese counterparts like WeChat should be subject to at least as much scrutiny and regulation — and be held accountable for any violations. Governments and corporations should also restrict usage of WeChat among their employees, particularly those who work with sensitive information, as the governments of Australia and India have recently done. Politicians communicating with their Chinese-speaking constituents should make sure to do so across a diversity of platforms, not just those that are subject to Chinese government control.

International civil society groups can assist users and democratic governments by maintaining up-to-date digital security guides available in Chinese, documenting the extent to which content outside China is censored or monitored on WeChat and exploring legal recourse for those whose rights may have been violated by Tencent’s practices.

Lastly, investors in Tencent should consider the moral and political implications of their support for the firm. Anyone concerned about human rights, electoral interference by foreign powers or privacy violations by tech giants should divest from the firm, including retirement funds. Socially responsible investment plans should exclude Tencent from their portfolios if they have not already.

Even from a financial perspective, Tencent shares may not be a wise purchase. The price has dropped 19 percent over the past year, in part because of tighter government controls on user communications. Given that Chinese regulators are now turning their attention to the gaming industry, the firm’s most profitable area of activity, its value is likely to dip further. As stock analyst Leo Sun has warned, “Investors in Chinese tech companies should never underestimate the government’s ability to throttle their growth.”

No amount of pushback from users, democratic governments, civil society groups, or investors is likely to change Tencent's complicity with the Chinese government's repressive activities. Its very survival depends on dutiful adherence to Communist Party directives. But the steps suggested above would do a great deal to limit the current and potential future damage caused by the company's practices — for individual users, for the world's open societies and for the very concept of free expression in the digital age.

---

*Sarah Cook is a senior research analyst for East Asia at Freedom House and director of its China Media Bulletin. © 2019, The Diplomat; distributed by Tribune Content Agency*

---

---

#### KEYWORDS

---

SOCIAL MEDIA ([HTTPS://WWW.JAPANTIMES.CO.JP/TAG/SOCIAL-MEDIA/](https://www.japantimes.co.jp/tag/social-media/)), TENCENT ([HTTPS://WWW.JAPANTIMES.CO.JP/TAG/TENCENT/](https://www.japantimes.co.jp/tag/tencent/)), CHINESE CENSORSHIP ([HTTPS://WWW.JAPANTIMES.CO.JP/TAG/CHINESE-CENSORSHIP/](https://www.japantimes.co.jp/tag/chinese-censorship/))

---

#### RELATED PHOTOS

---



(<https://cdn.japantimes.2xx.jp/wp-content/uploads/2019/03/p7-cook-a-20190329.jpg>)

Tencent's pattern of censorship and data-sharing with the Chinese government is intensifying under the leadership of chairman and CEO Pony Ma. | AP



(<https://www.japantimes.co.jp/liveblogs/news/coronavirus-outbreak-updates/>)

# EXHIBIT 18



**2019**

**REPORT TO CONGRESS**

*of the*

**U.S.-CHINA ECONOMIC AND  
SECURITY REVIEW COMMISSION**

ONE HUNDRED SIXTEENTH CONGRESS  
FIRST SESSION

---

NOVEMBER 2019

---

Printed for the use of the  
U.S.-China Economic and Security Review Commission  
Available online at: <https://www.uscc.gov>

---

U.S. GOVERNMENT PUBLISHING OFFICE  
WASHINGTON : 2019



**U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION**

CAROLYN BARTHOLOMEW, *Chairman*  
ROBIN CLEVELAND, *Vice Chairman*

**COMMISSIONERS**

ANDREAS BORGEAS	KENNETH LEWIS
JEFFREY FIEDLER	MICHAEL A. MCDEVITT
Hon. CARTE P. GOODWIN	Hon. JAMES M. TALENT
ROY D. KAMPHAUSEN	MICHAEL R. WESSEL
THEA MEI LEE	LARRY M. WORTZEL

DANIEL W. PECK, *Executive Director*

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act of 2001, Pub. L. No. 106–398 (codified at 22 U.S.C. §7002), as amended by: The Treasury and General Government Appropriations Act, 2002, Pub. L. No. 107–67 (Nov. 12, 2001) (regarding employment status of staff and changing annual report due date from March to June); The Consolidated Appropriations Resolution, 2003, Pub. L. No. 108–7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of the Commission); The Science, State, Justice, Commerce, and Related Agencies Appropriations Act, 2006, Pub. L. No. 109–108 (Nov. 22, 2005) (regarding responsibilities of the Commission and applicability of FACA); The Consolidated Appropriations Act, 2008, Pub. L. No. 110–161 (Dec. 26, 2007) (regarding submission of accounting reports; printing and binding; compensation for the executive director; changing annual report due date from June to December; and travel by members of the Commission and its staff); The Carl Levin and Howard P. “Buck” McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113–291 (Dec. 19, 2014) (regarding responsibilities of the Commission). The Commission’s full charter and statutory mandate are available online at: <https://www.uscc.gov/about/uscc-charter>.



U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

NOVEMBER 14, 2019

The Honorable Chuck Grassley  
President Pro Tempore of the U.S. Senate, Washington, DC 20510  
The Honorable Nancy Pelosi  
Speaker of the U.S. House of Representatives, Washington, DC 20510

DEAR SENATOR GRASSLEY AND SPEAKER PELOSI:

On behalf of the U.S.-China Economic and Security Review Commission, we are pleased to transmit the Commission's 2019 Annual Report to Congress. This Report responds to our mandate "to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China." The Commission reached a broad and bipartisan consensus on the contents of this Report, with all 12 members voting unanimously to approve and submit it to Congress.

In accordance with our mandate, this Report, which is current as of October 4, includes the results and recommendations of our hearings, research, travel, and review of the areas identified by Congress in our mandate, as defined in Public Law No. 106-398 (October 30, 2000), and amended by Public Laws No. 107-67 (November 12, 2001), No. 108-7 (February 20, 2003), 109-108 (November 22, 2005), No. 110-161 (December 26, 2007), and No. 113-291 (December 19, 2014). The Commission's charter, which includes the 11 directed research areas of our mandate, is included as Appendix I of the Report.

The Commission conducted eight public hearings, taking testimony from 77 expert witnesses from government, the private sector, academia, think tanks, research institutions, and other backgrounds. For each of these hearings, the Commission produced a transcript (posted on our website at <https://www.uscc.gov>). This year's hearings included:

- What Keeps Xi Up at Night: Beijing's Internal and External Challenges;
- Risks, Rewards, and Results: U.S. Companies in China and Chinese Companies in the United States;
- An Emerging China-Russia Axis? Implications for the United States in an Era of Strategic Competition;
- China in Space: A Strategic Competition?;
- Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy;
- A "World-Class" Military: Assessing China's Global Military Ambitions;
- Exploring the Growing U.S. Reliance on China's Biotech and Pharmaceutical Products; and
- U.S.-China Relations in 2019: A Year in Review.

The Commission received a number of briefings by executive branch agencies and the Intelligence Community, including both unclassified and classified briefings on China's military modernization, the China-Russia relationship, U.S.-Hong Kong relations, China's ambitions in space, and U.S. strategy for responding to China's Belt and Road Initiative. The Commission is preparing a classified report to Congress on these and other topics. The Commission also received briefings by foreign diplomatic and military officials as well as U.S. and foreign nongovernmental experts.

Commissioners made official visits to Australia, Singapore, Hong Kong, and China to hear and discuss perspectives on China and its global and regional activities. In these visits, the Commission delegation met with U.S. diplomats, host government officials, business representatives, academics, journalists, and other experts.

The Commission also relied substantially on the work of our excellent professional staff and supported outside research (see Appendix IV) in accordance with our mandate (see Appendix I).

The Report includes 38 recommendations for congressional action. Our ten most important recommendations appear on page 24 at the conclusion of the Executive Summary.

We offer this Report to Congress in the hope that it will be useful for assessing progress and challenges in U.S.-China relations.

Thank you for the opportunity to serve. We look forward to continuing to work with Members of Congress in the upcoming year to address issues of concern in the U.S.-China relationship.

Yours truly,




Carolyn Bartholomew  
Chairman




Robin Cleveland  
Vice Chairman

Commissioners Approving the 2019 Report

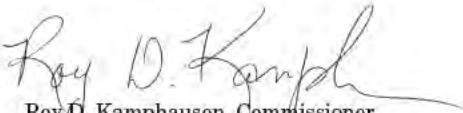
  
Carolyn Bartholomew, Chairman

  
Robin Cleveland, Vice Chairman

  
Andreas Borgeas, Commissioner

  
Jeffrey Fiedler, Commissioner

  
Carte P. Goodwin, Commissioner

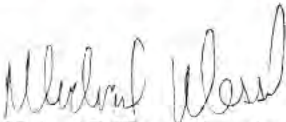
  
Roy D. Kamphausen, Commissioner

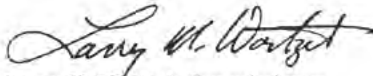


Michael A. McDevitt, Commissioner

  
Kenneth Lewis, Commissioner

  
James M. Talent, Commissioner

  
Michael R. Wessel, Commissioner

  
Larry M. Wortzel, Commissioner

CONTENTS

	Page
TRANSMITTAL LETTER TO THE CONGRESS .....	iii
COMMISSIONERS APPROVING THE REPORT .....	v
EXECUTIVE SUMMARY .....	1
KEY RECOMMENDATIONS .....	24
INTRODUCTION .....	29

2019 REPORT TO CONGRESS OF THE  
U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

<b>Chapter 1: 2019 in Review</b> .....	33
Section 1: Year in Review: Economics and Trade .....	33
Key Findings .....	33
Introduction .....	34
U.S.-China Trade .....	34
Bilateral Economic Tensions .....	38
Technological Conflict and Competition .....	46
China's Internal and External Economic Management .....	49
Section 2: Year in Review: Security, Politics, and Foreign Affairs .....	80
Key Findings .....	80
Introduction .....	81
A Year of Both Success and Setback .....	81
Chinese Diplomacy: Toward a China-Led World Order .....	89
Pressure on the Regional Balance .....	100
Tensions in U.S.-China Ties .....	104
<b>Chapter 2: Beijing's Internal and External Challenges</b> .....	119
Key Findings .....	119
Recommendations .....	120
Introduction .....	120
Internal Challenges to CCP Rule .....	121
China's Economic and Innovation Challenges .....	130
Resistance to Beijing's Ambitions Abroad: Economic, Military, and Political Challenges .....	136
Implications for the United States .....	153
<b>Chapter 3: U.S.-China Competition</b> .....	169
Section 1: U.S.-China Commercial Relations .....	169
Key Findings .....	169
Recommendations .....	170
Introduction .....	171
U.S.-China Economic Ties: An Unbalanced Relationship .....	171
Chinese Companies in the United States .....	172
U.S. Companies in China .....	182
Implications for the United States .....	191
Section 2: Emerging Technologies and Military-Civil Fusion: Artificial Intelligence, New Materials, and New Energy .....	205
Key Findings .....	205
Recommendations .....	206
Introduction .....	207

VIII

	Page
Military-Civil Fusion .....	208
Artificial Intelligence .....	214
New and Advanced Materials .....	220
Energy Storage .....	226
Civil Nuclear Power .....	229
Implications for the United States .....	230
<b>Section 3: Growing U.S. Reliance on China’s Biotech and Pharmaceutical</b>	
Products .....	248
Key Findings .....	248
Recommendations .....	249
Introduction .....	250
U.S. Reliance on Chinese Pharmaceutical and Medical Products .....	251
U.S. Government Oversight of Health Imports from China .....	257
China’s Pharmaceutical and Biotech Activities in the United States .....	261
U.S. Companies’ Access to Health Industries and Market Opportunities in China .....	265
U.S.-China Global Health Cooperation .....	269
Implications for the United States .....	269
<b>Chapter 4: China’s Global Ambitions</b> .....	283
<b>Section 1: Beijing’s “World-Class” Military Goal</b> .....	283
Key Findings .....	283
Recommendations .....	284
Introduction .....	285
A Military to Match Beijing’s Ambitions .....	285
Building a World-Class Military .....	288
A World-Class Military in Its Region and Beyond .....	296
Implications for the United States .....	303
<b>Section 2: An Uneasy Entente: China- Russia Relations in a New Era of Strategic Competition with the United States</b> .....	315
Key Findings .....	315
Recommendations .....	316
Introduction .....	316
A Deepening Entente .....	317
Mistrust and Power Asymmetry Limit Ties .....	327
Central Asia and Afghanistan, the Middle East, and the Arctic .....	335
Implications for the United States .....	343
<b>Section 3: China’s Ambitions in Space: Contesting the Final Frontier</b> .....	359
Key Findings .....	359
Recommendations .....	360
Introduction .....	361
National Rejuvenation and a “Space Dream” .....	362
Space Program Supports Geopolitical and Economic Goals .....	368
Space as the “Commanding Heights” of Future Military Conflict .....	379
Implications for the United States .....	383
<b>Section 4: Changing Regional Dynamics: Oceania and Singapore</b> .....	401
Key Findings .....	401
Recommendations .....	402
Introduction .....	402
Australia .....	403
Pacific Islands .....	418
Singapore .....	424
Implications for the United States .....	431
<b>Chapter 5: Taiwan</b> .....	445
Key Findings .....	445
Recommendations .....	446
Introduction .....	447
Cross-Strait Military and Security Issues .....	449
Taiwan’s External Relations .....	458
Economics and Trade .....	463
Implications for the United States .....	470



IX

	Page
<b>Chapter 6: Hong Kong</b> .....	481
Key Findings .....	481
Recommendations .....	482
Introduction .....	483
Proposed Extradition Bill Galvanizes Calls for Democracy .....	484
Hong Kong’s Autonomy under Continued Attack .....	496
Hong Kong’s Economic Relationship with Mainland China .....	505
Implications for the United States .....	513
<b>Comprehensive List of the Commission’s Recommendations</b> .....	537
 <b>Appendices:</b>	
Appendix I: Charter .....	547
Appendix II: Background of Commissioners .....	555
Appendix III: Public Hearings of the Commission During 2019 .....	565
Appendix IIIA: List of Witnesses Testifying Before the Commission During 2019 .....	569
Appendix IV: List of Research Material .....	573
Appendix V: Conflict of Interest and Lobbying Disclosure Reporting .....	577
Appendix VI: Acronyms and Abbreviations .....	579
<b>2019 Commission Staff and Acknowledgements</b> .....	581

## **EXECUTIVE SUMMARY**

### **Chapter 1: 2019 in Review**

#### **Section 1: Year in Review: Economics and Trade**

In 2019, the trade dispute between the United States and China entered its second year and remains mostly unresolved. The Chinese government's unwavering commitment to state management of its economy remains a major stumbling block. In response to decades of unfair economic practices, the United States wants the Chinese government to codify commitments to strengthen intellectual property protection, prohibit forced technology transfer, and remove industrial subsidies. But these practices are core features of China's economic system, and the Chinese government views U.S. demands as an attack on its national development. China continues to ignore the letter and the spirit of its World Trade Organization (WTO) commitments. The resulting impasse has led to multiple rounds of mutual tariff actions impacting more than \$500 billion in bilateral goods trade, and reducing trade between the two countries. In response to U.S. measures to address illegal activities of Chinese technology firms, China's government strengthened pursuit of technological self-reliance and its state-led approach to innovation, which uses licit and illicit means to achieve its goals. This will continue to pose a threat to U.S. economic competitiveness and national security.

Escalating trade tensions with the United States compounded China's domestic economic challenges, with the Chinese economy growing at its slowest pace in nearly 30 years in 2019. High debt levels constrain Beijing's ability to respond to the slowdown, and stimulus measures have so far been modest in comparison with past programs. The economic slowdown has disproportionately affected China's small and medium enterprises, which do not enjoy the same preferential treatment, access to credit, and government subsidies as state-owned or -supported enterprises. Meanwhile, regional banks have emerged as a key source of risk in China's financial system due to the high number of nonperforming loans on their balance sheets. China's government has also pursued limited market and financial system opening over the last year in an effort to attract foreign capital. These measures remain narrowly designed to address specific pressures facing China's economy and do not appear to herald a broader market liberalization of the kind that U.S. companies and policymakers have long advocated.

#### ***Key Findings***

- On-and-off trade negotiations between the United States and China to resolve a years-long trade dispute have failed to produce a comprehensive agreement. The impasse in negotiations

underscores, in part, China's commitment to preserving the government's dominant role in determining economic outcomes.

- The United States is confronting China in response to decades of unfair Chinese economic policies and trade-distorting practices. The Chinese Communist Party (CCP) increasingly perceives U.S. actions as an attack on its vision for China's national development. China's government has intensified nationalist rhetoric criticizing the United States, applied pressure on U.S. companies, and targeted key U.S. export sectors with tariffs in response.
- U.S. measures to address illegal activities by Chinese technology companies are leading China's government to push harder on technological self-reliance. The reinvigoration of the state-driven approach to innovation will pose a sustained threat to U.S. global economic competitiveness and national security.
- A range of domestic factors and trade tensions with the United States have slowed China's economic growth. In response, China's government has deployed infrastructure spending, tax cuts, and targeted monetary stimulus. While the stimulus enabled a modest recovery during the first half of 2019, China's rate of growth continues to slow.
- China's government continues to falsify official economic statistics, obscuring the true extent of its current economic slowdown. Independent observers estimate that China's true growth rate is at least 0.5 percentage points—and possibly as much as 3 percentage points—lower than Beijing's published figures.
- Beijing's deleveraging campaign has succeeded in containing China's corporate debt growth, but local governments continue to borrow. Expanding household debt and a rapid increase in the value of nonperforming loans also pose significant risks to China's financial system and are a major challenge for Chinese policymakers.
- China's state sector is strengthening and private companies are struggling. The deleveraging campaign and related crackdown on shadow banking had the unintended effect of cutting off credit to the private sector, which traditionally relies on informal finance.
- China's government has taken limited market opening steps, including incremental liberalization of China's foreign investment regime and financial system. However, these measures have been pursued in terms favorable to the Chinese government as opposed to the market, underscoring that any changes in China's economic practices will continue to be controlled by the state.

## **Section 2: Year in Review: Security, Politics, and Foreign Affairs**

In 2019, Beijing stepped up its efforts to promote itself as a global political and economic leader, offering the clearest evidence yet of its ambition to reshape the international order so it benefits Chinese interests and makes the world safe for the CCP. General Secretary of the CCP Xi Jinping continued to tout the CCP's model and "Chi-

nese wisdom” as solutions for the world’s problems and vowed to build a “community of common human destiny,” a CCP formulation for a China-led global governance regime. In the security realm, Beijing exhorted the People’s Liberation Army (PLA) to prepare itself for challenges in the years ahead while it continues its transformation into a “world-class” military able to conduct combat operations within and beyond the Indo-Pacific region. Meanwhile, as trade tensions between China and the United States deepened, General Secretary Xi declared that the CCP was now engaged in a “New Long March” and must prepare for a protracted, multidecade confrontation with Washington and its allies. At home, the CCP expanded its campaign of indoctrination and repression against Uyghurs, Tibetan Buddhists, Hui Muslims, Christians, and other religious groups and individuals the CCP considers to be politically unreliable.

Beijing also took new steps in 2019 to advance the aggressive approach to foreign and security policy it has taken in recent years. In the Indo-Pacific region, Beijing used displays of military force to intimidate its neighbors while applying informal economic sanctions against countries making decisions contrary to its interests. China also continued its efforts to influence or interfere with other countries’ political processes as well as global perceptions of its rise, including through United Front covert propaganda and co-optation activities, the targeting of U.S. and other foreign universities and media, arbitrary detentions of foreign citizens, and the export of censorship and surveillance technologies. Beijing also sought to shore up ties with key partners, such as North Korea and Iran, while growing its influence across the Western Hemisphere, Africa, and the Middle East.

The U.S.-China relationship deteriorated significantly over the past year as both sides blamed the other for issues such as the breakdown in trade negotiations and militarization of the South China Sea. Beijing’s views of the United States hardened as Chinese leaders took few meaningful steps to address issues of concern raised by Washington and Chinese state media intensified anti-U.S. propaganda. Meanwhile, the U.S. government increased its efforts to curb China’s influence and espionage activities in academic and commercial settings.

### ***Key Findings***

- In 2019, Beijing declared in unambiguous terms its intent to revise and reorder the international system in ways more befitting its national interests and repressive vision of governance. In a series of national addresses, Chinese leaders suggested the CCP viewed its “historic mission” as being not only to govern China, but also to profoundly influence global governance. The CCP took new steps to promote itself abroad as a model worthy of emulation, casting its political system and approach to economic development as superior alternatives to that of the United States and other democratic countries.
- Chinese leaders took a more strident tone in their discussion of military affairs, reinforcing a sense of urgency in the PLA’s preparations for a potential military conflict while indicating Beijing’s intent to position the PLA as a globally-oriented

military force. General Secretary Xi urged the PLA to make preparations for a possible conflict with the “powerful enemy adversary”—a phrase the CCP uses to refer to the United States—central to its modernization and training efforts.

- Despite signs of outward confidence, CCP leadership also revealed a growing unease over the mounting external resistance to its ambitions, which it viewed as threatening its objectives abroad and rule at home. In response to these challenges, the CCP deepened its control over the Chinese government and Chinese society and stepped up an ideological and nationalistic messaging campaign instructing key groups to “win the ideological war” against Western and other democratic countries.
- China continued its efforts to coerce or interfere in the domestic affairs of countries acting in ways contrary to its interests, detaining foreign citizens and carrying out an extensive influence campaign targeting foreign universities, media, and the Chinese diaspora. Beijing also expanded its global promotion of the Belt and Road Initiative (BRI), increasing military cooperation and exporting its censorship and surveillance technologies to countries under BRI auspices.
- In the Indo-Pacific region, China made new use of “gray zone” activities and military intimidation of its neighbors to secure its expansive sovereignty claims. Military tensions between China and Japan persisted in the East China Sea despite attempts by both countries to reset bilateral relations, while an annual poll of respondents in Southeast Asian countries found that fewer than one in ten saw China’s regional influence as benign.
- The U.S.-China relationship grew markedly more confrontational as tensions increased over political, economic, and security issues and polls reflected a significant drop in the U.S. public’s favorability toward China. Chinese leaders showed few signs of willingness to compromise on issues raised by Washington.

## **Chapter 2: Beijing’s Internal and External Challenges**

The CCP faces a number of significant internal and external challenges as it seeks to ensure its hold on power while sustaining economic growth, maintaining control at home, and advancing its regional and increasingly global ambitions. Despite a lengthy campaign to clean up its ranks, the CCP has growing concerns over widespread corruption, weakened control and cohesion, and ideological decay. Chinese policymakers credit their state-led economic model for the country’s rapid growth, but the contradictions in China’s approach are increasingly apparent as it faces a struggling private sector, high debt levels, and a rapidly-aging population. China remains deeply dependent on foreign technology and vulnerable to supply chain disruption, but is pouring vast amounts of resources toward encouraging domestic innovation.

Externally, BRI has come under growing international skepticism over China’s opaque lending practices, accusations of corruption, and encroachment on host countries’ sovereignty. CCP leaders are also worried about the PLA’s lack of recent warfighting experience and



have long harbored concerns about the loyalty, capabilities, and responsiveness of their security forces. Furthermore, Beijing's military modernization efforts, coercion of its neighbors, and interference in other countries' internal affairs have generated global apprehension about its geopolitical ambitions.

China's leadership is acutely aware of these challenges and is making a concerted effort to overcome them. Ultimately, the extent to which Beijing can address these vulnerabilities affects its ability to contest U.S. leadership and carve out a place for its own model of global governance. In the economic realm, Beijing's commitment to its state-led economic model likely will prolong U.S.-China trade frictions and worsen China's domestic challenges. Chinese leaders' concerns over the PLA's readiness for war will continue to influence their willingness to initiate a conflict that could prompt the intervention of a modern, capable adversary such as the United States, at least in the near term. Finally, General Secretary Xi's consolidation of power has created a dangerous echo chamber for decision making, which could lead to domestic policy missteps and complicate U.S.-China relations during times of heightened tensions or crisis.

### ***Key Findings***

- The CCP is facing internal and external challenges as it attempts to maintain power at home and increase its influence abroad. China's leadership is acutely aware of these challenges and is making a concerted effort to overcome them.
- The CCP perceives Western values and democracy as weakening the ideological commitment to China's socialist system of Party cadres and the broader populace, which the Party views as a fundamental threat to its rule. General Secretary Xi has attempted to restore the CCP's belief in its founding values to further consolidate control over nearly all of China's government, economy, and society. His personal ascendancy within the CCP is in contrast to the previous consensus-based model established by his predecessors. Meanwhile, his signature anti-corruption campaign has contributed to bureaucratic confusion and paralysis while failing to resolve the endemic corruption plaguing China's governing system.
- China's current economic challenges include slowing economic growth, a struggling private sector, rising debt levels, and a rapidly-aging population. Beijing's deleveraging campaign has been a major drag on growth and disproportionately affects the private sector. Rather than attempt to energize China's economy through market reforms, the policy emphasis under General Secretary Xi has shifted markedly toward state control.
- Beijing views its dependence on foreign intellectual property as undermining its ambition to become a global power and a threat to its technological independence. China has accelerated its efforts to develop advanced technologies to move up the economic value chain and reduce its dependence on foreign technology, which it views as both a critical economic and security vulnerability.

- China's senior leaders are concerned over perceived shortfalls in the PLA's warfighting experience and capabilities and its failure to produce an officer corps that can plan and lead. These concerns undermine Chinese leaders' confidence in the PLA's ability to prevail against a highly-capable adversary. The CCP has also long harbored concerns over the loyalty and responsiveness of the PLA and internal security forces to Beijing and the potential for provincial officials to co-opt these forces to promote their own political ambitions.
- China's BRI faces growing skepticism due to concerns regarding corruption, opaque lending practices, and security threats. However, this criticism has not been followed by an outright rejection of BRI because significant infrastructure gaps persist globally and China has few competitors in infrastructure financing.
- Beijing's military modernization efforts, coercion of its neighbors, and interference in other countries' internal affairs have generated resistance to its geopolitical ambitions. Countries in the Indo-Pacific and outside the region are accelerating their military modernization programs, deepening cooperation, and increasing their military presence in the region in an attempt to deter Beijing from continuing its assertive behavior.

### **Chapter 3: U.S.-China Competition**

#### **Section 1: U.S.-China Commercial Relations**

Chinese firms operate with far greater freedom in the United States than U.S. firms are permitted in China. The lack of reciprocity in market access, investment openness, regulatory treatment, and other areas have led to an environment where U.S. companies are disadvantaged in China's domestic market. Protected in their domestic market, Chinese companies are increasingly empowered to compete in third country markets. For this reason, many U.S. companies with operations in China, historically supportive of deepening engagement, have grown increasingly pessimistic about their ability to expand and participate in the Chinese market. The Chinese government's inbound foreign direct investment (FDI) regime has restricted foreign entry into some segments of the Chinese market, such as cloud computing and e-commerce. For high-priority sectors, China's government has made market entry conditional on transfer of technology and other concessions from U.S. and other foreign companies.

Much analysis has been done on Chinese FDI and capital raising in the United States, but little is known about Chinese companies' U.S. operations, governance, and impact on the broader U.S. economy. Chinese FDI in the United States peaked in 2016 and has subsequently fallen. By comparison, Chinese venture capital (VC) investment has not fallen as significantly. U.S. policymakers remain concerned about VC investment that might be directed by the Chinese government, as access to early-stage technologies could put U.S. national security and economic competitiveness at risk.

Beyond FDI, many Chinese companies raise capital on U.S. financial markets. Because Chinese companies frequently list in the United States using a variable interest entity, investments in U.S.-listed

Chinese companies are inherently risky, in part because the variable interest entity structure has been ruled unenforceable by China's legal system. The lack of disclosure by and oversight of U.S.-listed Chinese companies opens the door to adverse activities, such as insider trading, accounting fraud, and corporate governance concerns that could put U.S. investors, including pension funds, at risk.

### ***Key Findings***

- The nature of Chinese investment in the United States is changing. While Chinese FDI in the United States fell in 2018, VC investment in cutting-edge sectors has remained more stable. Broad trends in FDI from China mask VC investment. While lower than FDI, VC investment from Chinese entities could have more impact as it has prioritized potentially sensitive areas, including early-stage advanced technologies. This sustained Chinese investment raises concern for U.S. policymakers, as Beijing has accelerated its comprehensive effort to acquire a range of technologies to advance military and economic goals.
- U.S. laws, regulations, and practices afford Chinese companies certain advantages that U.S. companies do not enjoy. Chinese firms that raise capital on U.S. stock markets are subject to lower disclosure requirements than U.S. counterparts, raising risks for U.S. investors. The Chinese government continues to block the Public Company Accounting Oversight Board from inspecting auditors' work papers in China despite years of negotiations. As of September 2019, 172 Chinese firms were listed on major U.S. exchanges, with a total market capitalization of more than \$1 trillion.
- China's laws, regulations, and practices disadvantage U.S. companies relative to Chinese companies. China's foreign investment regime has restricted and conditioned U.S. companies' participation in the Chinese market to serve industrial policy aims. In addition, recent reports by the American and EU Chambers of Commerce in China suggest technology transfer requests have continued unabated. Technology transfer requests continue to compromise U.S. firms' operations.
- Chinese firms' U.S. operations may pose competitive challenges if they receive below-cost financing or subsidies from the Chinese state or if they can import inputs at less than fair value. There are serious gaps in the data that prevent a full assessment of the U.S.-China economic relationship. Analysis of Chinese companies' participation in the U.S. economy is constrained by the absence of empirical data on companies' operations, corporate governance, and legal compliance.

### **Section 2: Emerging Technologies and Military-Civil Fusion: Artificial Intelligence, New Materials, and New Energy**

U.S. economic competitiveness and national security are under threat from the Chinese government's broad-based pursuit of leadership in artificial intelligence (AI), new materials, and new energy. Because these technologies underpin many other innovations, China's government has prioritized their development, aiming to en-

courage transfer of foreign technology and know-how, build national champions, and attain self-sufficiency. Beijing's enhanced program of military-civil fusion seeks to mobilize civilian technological advances in support of China's military modernization and spur broader economic growth and innovation by eliminating barriers between the commercial and defense sectors.

Chinese military planners view AI in particular as an advantage that could allow China to surpass U.S. military capabilities. In seeking to become the dominant manufacturer of new energy vehicles, Chinese firms have established control over substantial portions of the global lithium-ion battery supply chain. China's efforts to localize high-value industries that use new and advanced materials, particularly aerospace manufacturing, jeopardize critical U.S. exports and position China to develop and deploy commercial and military advances ahead of the United States.

Compared to past technological modernization efforts, China's current initiatives pose far greater challenges to U.S. interests. China's ability to capitalize on new technology has been enhanced by what it learned or stole from foreign firms. By creating complex and opaque ties between China's civilian institutions and its defense sector, military-civil fusion increases the risk that U.S. firms and universities may advance China's military capabilities while endangering future U.S. economic leadership.

China's industrial planners coordinate policy across China's economy to channel resources to targeted industries and spur demand for domestic products, harnessing the strengths of China's robust manufacturing base and a network of government-led investment funds, while disadvantaging foreign firms. Outside China's borders, the state is financing Chinese state-owned enterprises' acquisitions of leading foreign robotics, machine tooling, and other firms; promoting Chinese influence in international standards-setting bodies; and cultivating export markets for Chinese goods and services around the world.

### ***Key Findings***

- China's government has implemented a whole-of-society strategy to attain leadership in AI, new and advanced materials, and new energy technologies (e.g., energy storage and nuclear power). It is prioritizing these focus areas because they underpin advances in many other technologies and could lead to substantial scientific breakthroughs, economic disruption, enduring economic benefits, and rapid changes in military capabilities and tactics.
- The Chinese government's military-civil fusion policy aims to spur innovation and economic growth through an array of policies and other government-supported mechanisms, including venture capital funds, while leveraging the fruits of civilian innovation for China's defense sector. The breadth and opacity of military-civil fusion increase the chances civilian academic collaboration and business partnerships between the United States and China could aid China's military development.
- China's robust manufacturing base and government support for translating research breakthroughs into applications allow it

to commercialize new technologies more quickly than the United States and at a fraction of the cost. These advantages may enable China to outpace the United States in commercializing discoveries initially made in U.S. labs and funded by U.S. institutions for both mass market and military use.

- *Artificial intelligence:* Chinese firms and research institutes are advancing uses of AI that could undermine U.S. economic leadership and provide an asymmetrical advantage in warfare. Chinese military strategists see AI as a breakout technology that could enable China to rapidly modernize its military, surpassing overall U.S. capabilities and developing tactics that specifically target U.S. vulnerabilities.
- *New materials:* Chinese firms and universities are investing heavily in building up basic research capabilities and manufacturing capacity in new and advanced materials, including through acquisition of overseas firms, talent, and intellectual property. These efforts aim to close the technological gap with the United States and localize production of dual-use materials integral to high-value industries like aerospace. They could also enable China to surpass the United States in applying breakthrough discoveries to military hardware.
- *Energy storage:* China has quickly built up advanced production capacity in lithium-ion batteries and established control over a substantial portion of the global supply chain, exposing the United States to potential shortages in critical materials, battery components, and batteries. China's heavily subsidized expansion in lithium-ion batteries will likely lead to excess capacity and drive down global prices. If Chinese producers flood global markets with cheaper, technologically inferior batteries, it would jeopardize the economic viability of more innovative energy storage technologies currently under development in the United States.
- *Nuclear power:* China is positioning itself to become a leader in nuclear power through cultivating future nuclear export markets along the BRI, particularly in sub-Saharan Africa, and attracting advanced nuclear reactor designers to build prototypes in China.

### **Section 3: Growing U.S. Reliance on China's Biotech and Pharmaceutical Products**

China is the largest producer of active pharmaceutical ingredients (APIs) in the world, and millions of U.S. consumers take life-saving drugs that contain ingredients made in China, even if the finished drugs themselves are not made in China. There are serious deficiencies in health and safety standards in China's pharmaceutical sector, and inconsistent and ineffective regulation by China's government. Nevertheless, U.S. imports of these health products—either directly from China or indirectly through companies in third countries—continue to increase. As the largest source of fentanyl, China also plays a key role in the ongoing U.S. opioid epidemic. Beijing's weak regulatory and enforcement regime allows chemical and pharmaceutical manufacturers to export dangerous controlled and uncontrolled substances.



U.S. consumers, including the U.S. military, are reliant on drugs or active ingredients sourced from China, which presents economic and national security risks, especially as China becomes more competitive in new and emerging therapies. The Chinese government is investing significant resources into the development of biotechnology products and genomics research, accumulating private and medical data on millions of U.S. persons in the process. The Chinese government also encourages mergers and acquisitions—as well as venture capital investments—in U.S. biotech and health firms, leading to technology transfer that has enabled the rapid development of China's domestic industry. U.S. health and biotech firms in China, meanwhile, continue to face regulatory and other market barriers. While the Chinese government has taken steps in recent years to streamline regulatory procedures and allow foreign medical products to enter the market more quickly, concerns remain over China's weak commitment to protecting intellectual property rights and willingness to favor domestic providers of health products.

### ***Key Findings***

- China is the world's largest producer of APIs. The United States is heavily dependent on drugs that are either sourced from China or include APIs sourced from China. This is especially true for generic drugs, which comprise most prescriptions filled in the United States. Drug companies are not required to list the API country of origin on their product labels; therefore, U.S. consumers may be unknowingly accepting risks associated with drugs originating from China.
- The Chinese government has designated biotechnology as a priority industry as a part of its 13th Five-Year Plan and the Made in China 2025 initiative. The development of China's pharmaceutical industry follows a pattern seen in some of its other industries, such as chemicals and telecommunications, where state support promotes domestic companies at the expense of foreign competitors.
- China's pharmaceutical industry is not effectively regulated by the Chinese government. China's regulatory apparatus is inadequately resourced to oversee thousands of Chinese drug manufacturers, even if Beijing made such oversight a greater priority. This has resulted in significant drug safety scandals.
- The U.S. Food and Drug Administration (FDA) struggles to guarantee the safety of drugs imported from China because of the small number of FDA inspectors in country, the large number of producers, the limited cooperation from Beijing, and the fraudulent tactics of many Chinese manufacturers. Because of U.S. dependency on China as a source of many critical drugs, banning certain imports due to contamination risks creating drug shortages in the United States.
- As a result of U.S. dependence on Chinese supply and the lack of effective health and safety regulation of Chinese producers, the American public, including its armed forces, are at risk of exposure to contaminated and dangerous medicines. Should Beijing opt to use U.S. dependence on China as an economic

weapon and cut supplies of critical drugs, it would have a serious effect on the health of U.S. consumers.

- Lack of data integrity in China presents challenges for U.S. and Chinese health regulators. In 2016, the China Food and Drug Administration investigated 1,622 drug clinical trial programs and canceled 80 percent of these drug applications after it found evidence of fraudulent data reporting and submissions of incomplete data, among other problems.
- China places great emphasis on genomic and other health-related data to enhance its biotech industry. Domestically, China established national and regional centers focused on big data in health and medicine. Investment and collaborations in the U.S. biotech sector give Chinese companies access to large volumes of U.S. medical and genomic data, but U.S. companies do not get reciprocal access.
- Foreign firms continue to face obstacles in China's health market. These obstacles include drug regulatory approval delays, drug pricing limitations, reimbursement controls, and intellectual property theft. U.S. companies must also compete with Chinese drug companies that introduce generic products or counterfeit drugs to the Chinese market shortly after a foreign patented drug is introduced.
- China is the largest source of fentanyl, a powerful synthetic opioid, in the United States. Although the Chinese government made multiple commitments to curtail the flow of illicit fentanyl to the United States, it has failed to carry out those commitments.

## **Chapter 4: China's Global Ambitions**

### **Section 1: Beijing's "World-Class" Military Goal**

In remarks before the CCP's 19th National Congress in October 2017, General Secretary Xi pledged to build the PLA into a "world-class" force by the middle of the 21st century. This milestone established a timeline for and helps define the goal of the CCP's sweeping ambition for growing China's military power—what General Secretary Xi declared shortly after assuming power in 2012 as China's "Strong Military Dream." This force would support the CCP's efforts to place China at the center of world affairs.

Beijing has instructed the PLA to remain primarily focused on a potential conflict with Taiwan, but has also directed the force to increase preparations for conflicts elsewhere around China's periphery, including with the United States, Japan, India, and other countries in the region. At the same time, it has given the PLA guidance to increase its operations beyond the Indo-Pacific region. One goal of this strategy is to defend China's overseas interests, which Beijing describes as being "crucial" and in recent years has elevated to a similar level of importance for the PLA as defending China's own territory. Another of Beijing's goals is to increase the difficulty the United States would face in intervening in a regional conflict.

Beijing's ambition to develop the PLA into a world-class force will create challenges for the United States and its allies and part-

ners. It would increase the confidence of Chinese leaders to employ the PLA to coerce China's neighbors into forfeiting their territorial claims and other sovereign interests. A military that is truly world-class in technology, training, and personnel would likely also allow China to prevail in a military conflict with any regional adversary. Moreover, Beijing could decide to initiate a military conflict even if it calculated the United States would intervene due to its confidence it would be able to effectively deter or defeat intervening U.S. military forces. Beyond armed conflict, a more robust overseas military presence will provide Beijing additional tools to support and influence countries around the world that pursue policies injurious to U.S. interests.

### ***Key Findings***

- In 2017, Beijing announced its goal to build the PLA into a world-class military, overcoming remaining shortfalls in the force's capabilities to establish China firmly among the ranks of the world's leading military powers. This objective is guided by CCP leaders' view that China is approaching the "world's center stage" and represents the military component of a multifaceted goal to establish China's leading global position in every important element of national power.
- Beijing views a world-class PLA as achieving parity in strength and prestige with the world's other leading militaries, especially with the U.S. armed forces, and being capable of preventing other countries from resisting China's pursuit of its national goals. Deterring outside intervention will be especially important in the Indo-Pacific region, where China aims to resolve territorial disputes with a number of important U.S. allies and partners—including through the use of military force if necessary—but will also extend to China's overseas interests.
- Once focused on territorial defense, China's military strategy has evolved in recent years to encompass a concept PLA strategists refer to as "forward defense," which would create greater strategic depth by extending China's defensive perimeter as far as possible from its own shores. China is developing key capabilities necessary for force projection centered on a sophisticated blue-water navy that Chinese naval leadership plans to use to combat the U.S. Navy in the far seas.
- To support this strategy, Beijing is expanding its military presence inside and beyond the Indo-Pacific, including by building a network of overseas "strategic strongpoints" consisting of military bases and commercial ports that can support military operations. China established its first permanent overseas military presence in Djibouti in 2017 and Argentina in 2018, and reportedly has reached an agreement for the PLA to operate from a naval base in Cambodia. The PLA is increasingly training and fielding capabilities for expeditionary operations, including by developing a third aircraft carrier and improving its amphibious assault capabilities.
- The PLA continues to prioritize the modernization of its maritime, air, information warfare, and long-range missile forces,

and is developing or has fielded cutting-edge capabilities in space, cyberspace, hypersonics, electronic warfare, and AI. Beijing is attempting to establish a leading position in the next global “revolution in military affairs” and is employing its “military-civil fusion” strategy to gain advantage in key emerging technologies. U.S. companies that partner with Chinese technology firms may be participants in this process.

- Notwithstanding its long-held policy of maintaining a “minimal nuclear deterrent,” Beijing is growing, modernizing, and diversifying its nuclear arsenal and delivery systems. China doubled the size of its nuclear arsenal over the last decade and U.S. officials estimate it will double it again in the next decade, while Beijing has increased the readiness and improved the accuracy of its nuclear forces.
- China continues to devote ample financial resources to its military modernization, with its officially-reported defense budget ranking second only to the United States since 2002. China’s overall defense spending has seen a nearly eight-fold increase over the past two decades, dwarfing the size and growth rate of other countries in the Indo-Pacific.

## **Section 2: An Uneasy Entente: China-Russia Relations in a New Era of Strategic Competition with the United States**

China-Russia relations have strengthened considerably over the last decade in the face of what both countries perceive to be an increasingly threatening external environment. Beijing and Moscow believe the United States and the international liberal order pose a threat to their regime survival and national security. At the same time, they view the United States and other democracies as in decline and see an opportunity to expand their geopolitical influence at the expense of Washington and its allies. The two countries frame their relationship as the best it has ever been, but insist that it is not an alliance. However, China and Russia’s common expectation of diplomatic support in a dispute, shared antipathy to democratic values, opposition to the U.S. alliance system, and deepening diplomatic and military cooperation have already begun to challenge U.S. interests around the globe.

Nevertheless, Russia chafes at being a weaker partner in this relationship and fears becoming a mere “raw materials appendage” of China. Already scarred by historical enmity, the China-Russia relationship remains constrained by divergence over key national interests including differing stances on territorial disputes and partnerships with countries regarded as rivals by the other. Each country also harbors concerns over the potential military and geopolitical threat posed by the other. Finally, China’s growing influence in regions Russia perceives as its traditional sphere of influence—such as Central Asia and the Arctic—complicates the creation of a formal alliance.

Despite their differences, Moscow and Beijing work either independently or together to counter the United States and erode the values underpinning U.S. global leadership. China’s and Russia’s use of influence operations, cyberwarfare, and disinformation have the potential to destabilize the United States and democracies around the world. Moreover, coordinated Sino-Russian military activity has

created new security challenges for the United States and its allies. Russian sales of advanced military technology to China have bolstered PLA capabilities, while combined exercises have sought to improve interoperability. Coordinated military activity between both countries in a single theater or separate theaters could test the ability of the United States and its allies to respond. One country's success in pursuing its interests in opposition to the United States may also embolden the other to take similar actions.

### ***Key Findings***

- China and Russia both object to the current international order and the interests it promotes, including human rights, democracy, and a rules-based economic system that imposes on them obligations they wish to evade. Both countries see the values of that order as a threat to their authoritarian models and view the United States as the leader and primary defender, along with its alliance networks, of that order. Based on that common perception and their mutual interest in opposing the United States and its allies, an entente between China and Russia has emerged in recent years as the two have increased their diplomatic, military, and economic cooperation.
- China and Russia perceive threats to their regime security emanating from democracy movements—which they allege are “color revolutions” instigated by the United States—and from the free, open internet. Both countries seek to combat these challenges by interfering in democratic countries’ political processes and jointly championing the idea that the internet should be subject to sovereign states’ control. The two countries have also coordinated efforts to act as a counterweight to the United States by supporting rogue or authoritarian regimes and opposing U.S.-led votes in the UN Security Council. More broadly, China and Russia’s promotion of norms conducive to authoritarianism aims to subvert key elements of the international order.
- Beijing and Moscow’s view that the United States and its allies are in decline has emboldened both countries to take more assertive action in their regions in ways inimical to U.S. interests. These actions include military and paramilitary activities pursued separately by China and Russia that threaten the sovereignty of their neighbors as well as coordinated activity that creates new challenges for the United States and its allies in responding to combined Sino-Russian military operations.
- China and Russia’s trade in oil and gas is an important avenue by which both countries circumvent U.S. tariffs and international sanctions. Russia is China’s top source of imported oil, and is poised to become a major provider to China of natural gas over the next decade. Major energy deals and high-level contacts serve to soften the blow of sanctions and tariffs on both countries’ products, while signaling that China and Russia can rely on each other if alienated by the United States and other countries.
- Nonetheless, the China-Russia relationship remains scarred by historical enmity and constrained by Moscow’s concerns over its



increasingly subordinate role in the partnership. Divergence in key national interests, such as different stances on territorial disputes and support for regional rivals, further limits bilateral cooperation. Each country also harbors concerns over the potential military and geopolitical threat posed by the other. Moreover, China's growing influence in regions Russia perceives as its traditional sphere of influence—such as Central Asia and the Arctic—complicates the creation of a formal alliance.

### **Section 3: China's Ambitions in Space: Contesting the Final Frontier**

China's government and military are determined to meet ambitious goals for space leadership, if not dominance, and China has connected its space program with its broader ambitions to become a terrestrial leader in political, economic, and military power. Beijing aims to establish a leading position in the future space-based economy and capture important sectors of the global commercial space industry, including promoting its space industry through partnerships under what it has termed the "Space Silk Road." Meanwhile, China has jumpstarted its domestic space industry by engaging in an extensive campaign of intellectual property theft, generous state support to commercial startups, and predatory pricing for Chinese space services in the global space market. Beijing has also used front companies to invest in U.S. space companies as part of its efforts to acquire U.S. technology by both licit and illicit means, while Chinese universities involved in developing space-related technology for the PLA have proactively pursued research collaboration with U.S. and other foreign universities.

China has aggressively pursued the development of counterspace weapons, which are inherently destabilizing. Chinese strategic writings on space warfare also appear to favor dangerously escalatory offensive tactics, raising concerns about whether it is possible to deter China from attacking U.S. space assets. China believes space is a "new commanding height in strategic competition" and views seizing dominance in space as a priority in a conflict. Beijing has also fought to promote its leadership role in international space governance institutions and indicated it may extend its vision of governance and sovereignty to outer space.

The United States retains many advantages in space, such as its international partnerships and its organizational and technical expertise, and China is in some ways attempting to follow in the footsteps of past U.S. achievements. Still, China's single-minded focus and national-level commitment to establishing itself as a global space leader harms other U.S. interests and threatens to undermine many of the advantages the United States has worked so long to establish. China is well-positioned to assume a commanding role in a future space-based economy, as its steps to dominate the global commercial launch and satellite sectors through generous subsidies and other advantages have already threatened to hollow out the U.S. space industrial base. Should the China Space Station proceed as planned and the International Space Station be retired, China may also replace the United States as many countries' default partner in human spaceflight.

***Key Findings***

- China's goal to establish a leading position in the economic and military use of outer space, or what Beijing calls its "space dream," is a core component of its aim to realize the "great rejuvenation of the Chinese nation." In pursuit of this goal, China has dedicated high-level attention and ample funding to catch up to and eventually surpass other spacefaring countries in terms of space-related industry, technology, diplomacy, and military power. If plans hold to launch its first long-term space station module in 2020, it will have matched the United States' nearly 40-year progression from first human spaceflight to first space station module in less than 20 years.
- China views space as critical to its future security and economic interests due to its vast strategic and economic potential. Moreover, Beijing has specific plans not merely to explore space, but to industrially dominate the space within the moon's orbit of Earth. China has invested significant resources in exploring the national security and economic value of this area, including its potential for space-based manufacturing, resource extraction, and power generation, although experts differ on the feasibility of some of these activities.
- Beijing uses its space program to advance its terrestrial geopolitical objectives, including cultivating customers for BRI, while also using diplomatic ties to advance its goals in space, such as by establishing an expanding network of overseas space ground stations. China's promotion of launch services, satellites, and the Beidou global navigation system under its Space Silk Road is deepening participants' reliance on China for space-based services.
- China is taking steps to establish a commanding position in the commercial launch and satellite sectors relying in part on aggressive state-backed financing that foreign market-driven companies cannot match. China has already succeeded in undercutting some U.S. and other foreign launch and satellite providers in the international market, threatening to hollow out these countries' space industrial bases.
- The emergence of China's indigenous space sector has been an early and notable success of Beijing's military-civil fusion strategy. The aggressive pursuit of foreign technology and talent gained through joint research and other means, especially from the United States and its allies and partners, continues to be central to this strategy and to China's space development goals in general.
- The Chinese government and military use Hong Kong-based companies to exploit legal loopholes and uneven enforcement in U.S. export controls to gain access to space capabilities which U.S. law prohibits Beijing from purchasing outright. Collaboration with foreign universities, including in the United States, is another important avenue in China's drive to acquire space technology. Chinese students enrolled in foreign science, technology, engineering, and mathematics programs are treated like

employees of China's defense industrial base, with defense enterprises regularly funding their studies in return for service commitments following graduation.

- China views space as a critical U.S. military and economic vulnerability, and has fielded an array of direct-ascent, cyber, electromagnetic, and co-orbital counterspace weapons capable of targeting nearly every class of U.S. space asset. The PLA has also developed doctrinal concepts for the use of these weapons encouraging escalatory attacks against an adversary's space systems early in a conflict, threatening to destabilize the space domain. It may be difficult for the United States to deter Beijing from using these weapons due to China's belief the United States has a greater vulnerability in space.

#### **Section 4: Changing Regional Dynamics: Oceania and Singapore**

China aims to replace the United States as a leading security and economic power in the Indo-Pacific region. While most countries in the region are aware of the risks posed by Beijing's increased assertiveness, they have struggled to effectively respond, due in part to a desire to continue benefiting from economic engagement with China.

Australia, a steadfast U.S. ally, maintains economic ties with China even as concern over Beijing's interference in its domestic politics has increased. As Australia's top trading partner, China wields significant economic leverage over Australia, which it has used during diplomatic disputes. Canberra has passed laws to address foreign political interference and economic espionage and is trying to address China's interference in Australian universities, but progress has been mixed. It has also taken measures to prevent Chinese investment in Australia's infrastructure that could harm Australia's national interest, while launching its largest military modernization effort since the Cold War to respond to China's growing military threat.

In recent years, Beijing has increased outreach to the Pacific Islands due to the region's strategic significance and voting power in the UN. Beijing's efforts have won it political support, including establishing diplomatic relations this year with the Solomon Islands and Kiribati, previously two of Taiwan's remaining diplomatic partners. Nevertheless, some South Pacific policymakers have grown concerned Chinese engagement could overwhelm these small countries and result in an excessive accumulation of debt to Beijing. China has also sought to raise its military profile in the Pacific Islands, while Australia and the United States have increased their engagement in the region in response to China's advances.

Singapore has pursued close relationships with both the United States and China while attempting to protect its autonomy in foreign affairs rather than side exclusively with either country. It remains dedicated to its relationship with the United States, as exemplified by its robust economic and security ties. At the same time, Beijing seeks a closer economic and military relationship with Singapore. Rhetorical commitment to greater security ties with China, as well as its role as a financial hub for China's BRI, demonstrates the challenges Singapore faces in hedging between the United States and China.

Beijing has benefited from popular conceptions that China is the most important economic partner to these Indo-Pacific countries, even as U.S. investment exceeds that from China. While Indo-Pacific countries understand the importance of the United States' continued presence, China's increasing influence threatens to alter the trajectory of U.S. relations with these countries absent strong U.S. involvement in the region.

### ***Key Findings***

- Beijing has used economic coercion, acquired strategically-significant assets, and interfered in the domestic politics of neighboring countries to advance its interests in the Indo-Pacific region. China seeks closer engagement with its neighbors not only for economic gain but also to gain influence over their decision making to eventually achieve regional dominance and replace the United States as a vital economic partner and preeminent regional security guarantor.
- Some targeted countries are becoming increasingly aware of these risks and are taking steps to respond to China's political interference and growing military strength. Still, countries have struggled to formulate comprehensive and effective responses.
- Australia wants to maintain positive economic ties with China, but is also wary of Beijing's increasing regional assertiveness and outright interference in Australia's political affairs. Its steps to mitigate the risks of engagement with China, including tightening foreign investment restrictions and cracking down on political interference, have had mixed success. The Australian business community still favors greater economic engagement with China while downplaying national security concerns.
- To address the growing military threat posed by China, Australia has launched its largest military modernization effort since the Cold War. Central to this effort are large-scale investments in new warships, submarines, and fighter aircraft. Australia is also standing up a new military unit dedicated to improving military coordination with Pacific Island countries and is working with the United States and Papua New Guinea to develop a naval base in the latter's territory, which will complement the already substantial U.S. military presence in Australia.
- China seeks engagement with the Pacific Islands to establish military access to the region, gain the benefit of these countries' voting power in the UN, undermine regional diplomatic support for Taiwan, and gain access to natural resources, among other goals. Pacific Island countries view China as a vital economic partner and source of infrastructure investment and aid, but some Pacific Island officials have expressed reservations about Beijing's increasing influence and presence in the region, particularly over growing indebtedness to China. As a result of China's growing inroads in the Pacific Islands, Australia has also increased its engagement in the region, though its efforts have also encountered some pushback.

- As a small country and regional economic hub, Singapore continues to work to maintain the balance between its relationships with the United States and China amid heightening U.S.-China tensions. Singapore is also concerned about China's attempts to undermine ASEAN's unity and its own ability to play a leading role in Southeast Asia. While Singapore remains a dedicated security partner of the United States, it also has close economic ties to China, including serving as an increasingly important financial and legal intermediary for BRI projects.

### **Chapter 5: Taiwan**

The Taiwan Relations Act, which set the foundation for ties between the United States and Taiwan following the United States' severing of diplomatic ties with the Republic of China (Taiwan), celebrated its 40th anniversary in 2019. In the 40 years since the Taiwan Relations Act's signing, Taiwan has become a thriving multiparty democracy. Taiwan has a robust civil society and rule of law that protects universal human rights, open public discourse, and a free and independent media. The vibrancy of Taiwan's democratic system is on display in the ongoing campaigns for the 2020 presidential and legislative elections. In addition to being a model of a successful democracy for the Indo-Pacific region, Taiwan has become an increasingly important economic and geostrategic partner for the United States.

Meanwhile, throughout 2019 Beijing adopted a more coercive policy toward Taiwan, seeking to isolate and intimidate Taipei into unification on Beijing's terms. In January 2019, General Secretary Xi delivered a major speech on Beijing's Taiwan policy in which he claimed that Taiwan's unification with the People's Republic of China was inevitable and indicated that the "one country, two systems" model was the only acceptable arrangement for unification. That model has been roundly rejected by the Taiwan public and multiple Taiwan presidential administrations.

In implementing its more coercive approach, Beijing sharply escalated its military, diplomatic, and economic pressure against Taiwan, including interfering in Taiwan's media to shape public opinion on China and cross-Straits relations. In the Taiwan Strait area, the PLA carried out a series of provocative operations not seen in 20 years, while Beijing enticed two more of Taiwan's remaining 17 diplomatic partners to switch recognition to Beijing. It also severely curtailed cross-Straits tourism flows by suspending all approvals for individual tourists to visit Taiwan. Beijing's multipronged pressure campaign limits Taipei's ability to fully engage with the international community and diversify its economy away from deep reliance on China.

The people of Taiwan are now observing Beijing's unification model unfold in Hong Kong, where millions of people are fighting for their civil liberties against an unbending authoritarian regime. Should Beijing succeed in coercing Taiwan into submitting to a similar unification agreement, it not only would damage U.S. national security interests but also could undermine the progress of democratic values and institutions in the region.



***Key Findings***

- In 2019, General Secretary Xi made clear his increasingly uncompromising stance toward Taiwan's independent status and sense of urgency regarding unification. Beijing intensified its multipronged campaign to coerce and isolate Taiwan, including by supporting Taiwan politicians Beijing finds palatable, while opposing and seeking to discredit those it does not, particularly Taiwan's elected government headed by President Tsai Ing-wen. Guided by this policy, Beijing redoubled its efforts to bypass Taiwan's central government by conducting negotiations with unelected political parties, groups, and individuals.
- The deliberate crossing of the Taiwan Strait median line by Chinese fighter aircraft in March 2019 was the first such crossing in 20 years and marked a sharp escalation in the military pressure Beijing has increasingly applied against Taipei since General Secretary Xi assumed power in 2012. China signaled that its intensifying campaign of military coercion had become official policy in a key policy document released in July 2019, while the continued growth of the PLA's capabilities and budget threatened to overturn any remaining semblance of cross-Strait military balance.
- As Beijing escalated diplomatic, economic, cultural, and political warfare against Taiwan, evidence emerged that it sought to influence Taiwan's November 2018 local elections, including through traditional Taiwan media and disinformation spread through social media to exacerbate social divisions and undermine public confidence in the ruling Democratic Progressive Party government. Allegations that Beijing intervened on behalf of Taiwan presidential challenger Han Kuo-yu of the Nationalist Party (Kuomintang, or KMT) in his 2018 Kaohsiung mayoral campaign raised questions over whether it may be doing so again in the lead-up to Taiwan's presidential election in January 2020.
- The CCP adopted new tactics to leverage Taiwan media in support of its political goals, with evidence building that Beijing has shaped coverage of cross-Strait relations and potentially Taiwan's presidential election through direct partnerships with some major Taiwan media outlets. These partnerships have included China's Taiwan Affairs Office commissioning stories and giving instructions to editorial managers.
- Concerns in Taiwan over Beijing's desired "one country, two systems" unification model for Taiwan were amplified by 2019's massive protest movement in Hong Kong, which is governed by the same model and has seen the autonomy the model promises steadily erode. Presidential contenders from both major political parties in Taiwan assailed the "one country, two systems" model as unacceptable for any future sovereign agreement between the two sides.
- Taiwan took a series of steps to enhance its military capabilities and implement its new Overall Defense Concept. These measures included the island's largest increase in its defense budget

in more than a decade, breaking ground on the facility that will build Taiwan's indigenous submarines, allocating funding for the procurement of 60 new small fast-attack missile boats, and expediting production of new missile defense systems and mobile land-based antiship missile platforms.

- U.S.-Taiwan cooperation expanded into new areas as the United States took significant steps to support Taiwan, including the Trump Administration's approval of a landmark arms sale of new fighter aircraft to Taiwan, the first meeting between U.S. and Taiwan national security advisors since 1979, and a more assertive approach to U.S. Navy transits of the Taiwan Strait. However, talks under the Trade and Investment Framework Agreement have stalled since October 2016.

## **Chapter 6: Hong Kong**

In 2019, the Hong Kong government's controversial bill that would allow for extradition to mainland China sparked a historic protest movement opposing the legislation and the Mainland's growing encroachment on the territory's autonomy. Millions of Hong Kong citizens participated in unprecedented mass demonstrations against the bill, causing its formal withdrawal, paralyzing the Hong Kong government, and dealing a major blow to Beijing. In the face of the Hong Kong authorities' intransigence and growing police violence against demonstrators, the movement's demands expanded while protesters strengthened their resolve to achieve Beijing's long-delayed promise of credible democratic elections. The protesters declared that democratic elections are essential to a truly representative government.

Instead of heeding the movement's calls for the preservation of Hong Kong's "high degree of autonomy," the CCP has used numerous tools to try to quell the demonstrations, including economic coercion, disinformation, and the apparent encouragement of pro-Beijing thugs to attack protesters. Meanwhile, the Hong Kong government, backed by Beijing, took new steps to erode the territory's freedom of expression, press freedom, rule of law, and freedom of assembly, making the territory more like any other Chinese city. These moves are having a harmful effect on Hong Kong's attractiveness as one of the world's preeminent trade and financial hubs. Hong Kong acts as a unique conduit for investment flows between mainland China and global financial markets, a role underpinned by international confidence in the strength of its institutions and the rule of law.

U.S. policy toward Hong Kong, as outlined in the U.S.-Hong Kong Policy Act of 1992, underscores U.S. support for Hong Kong's human rights and democratization, and is predicated on the territory retaining its autonomy under the "one country, two systems" framework. Beijing's growing encroachment on Hong Kong's autonomy in violation of its legal commitments has thus raised serious concerns for U.S. policymakers. The future direction of Hong Kong—and with it U.S.-Hong Kong policy—will rest upon the outcome of the anti-extradition bill protest movement and the extent to which the Hong Kong government and Beijing respect the aspirations of Hong Kong citizens.

***Key Findings***

- The Hong Kong government's proposal of a bill that would allow for extraditions to mainland China sparked the territory's worst political crisis since its 1997 handover to the Mainland from the United Kingdom. China's encroachment on Hong Kong's autonomy and its suppression of prodemocracy voices in recent years have fueled opposition, with many protesters now seeing the current demonstrations as Hong Kong's last stand to preserve its freedoms. Protesters voiced five demands: (1) formal withdrawal of the bill; (2) establishing an independent inquiry into police brutality; (3) removing the designation of the protests as "riots;" (4) releasing all those arrested during the movement; and (5) instituting universal suffrage.
- After unprecedented protests against the extradition bill, Hong Kong Chief Executive Carrie Lam suspended the measure in June 2019, dealing a blow to Beijing which had backed the legislation and crippling her political agenda. Her promise in September to formally withdraw the bill came after months of protests and escalation by the Hong Kong police seeking to quell demonstrations. The Hong Kong police used increasingly aggressive tactics against protesters, resulting in calls for an independent inquiry into police abuses.
- Despite millions of demonstrators—spanning ages, religions, and professions—taking to the streets in largely peaceful protest, the Lam Administration continues to align itself with Beijing and only conceded to one of the five protester demands. In an attempt to conflate the bolder actions of a few with the largely peaceful protests, Chinese officials have compared the movement to "terrorism" and a "color revolution," and have implicitly threatened to deploy its security forces from outside Hong Kong to suppress the demonstrations.
- In 2019, assessment of press freedom fell to its lowest point since the handover, while other civil liberties protected by the Basic Law (Hong Kong's mini constitution), including freedom of expression and assembly, faced increasing challenges.
- Throughout 2019, the CCP stepped up its efforts to intervene in Hong Kong's affairs, using an array of tools to increase its influence in the territory, most clearly by co-opting local media, political parties, and prominent individuals. Beijing also used overt and covert means to intervene in Hong Kong's affairs, such as conducting a disinformation campaign and using economic coercion in an attempt to discredit and intimidate the protest movement. These efforts included alleging without evidence that U.S. and other foreign "black hands" were fomenting the protests; directing and organizing pro-Beijing legislators, businesses, media, and other influential individuals against the movement; allegedly encouraging local gangs and mainland community groups to physically attack protesters and prodemocracy figures; and conducting apparent cyberattacks against Hong Kong protesters' communications and a prodemocracy media outlet.

- Hong Kong has a unique role as a conduit between Chinese companies and global financial markets. As Chinese companies are increasingly represented in key benchmark indices, analysts anticipate greater capital flows from the United States and other countries into Chinese companies through the stock and bond Connect platforms between mainland exchanges and Hong Kong. However, due to diminished confidence resulting from the extradition bill proposal and subsequent fallout, some foreign businesses are reportedly considering moving their operations away from Hong Kong.
- Hong Kong's status as a separate customs territory, distinct from mainland China, is under pressure. U.S. and Hong Kong officials cooperate on enforcing U.S. export controls of dual-use technologies, though U.S. officials continue to raise concerns about diversion of controlled items. Beijing's more assertive imposition of sovereign control over Hong Kong undermines the "high degree of autonomy" that underwrites trust in the Hong Kong government's ability to restrict sensitive U.S. technologies from being diverted to mainland China.

## THE COMMISSION'S KEY RECOMMENDATIONS

The Commission considers 10 of its 38 recommendations to Congress to be of particular significance. The complete list of recommendations appears at the Report's conclusion on page 537.

The Commission recommends:

1. Congress enact legislation to preclude Chinese companies from issuing securities on U.S. stock exchanges if:
  - The Public Company Accounting Oversight Board is denied timely access to the audit work papers relating to the company's operations in China;
  - The company disclosure procedures are not consistent with best practices on U.S. and European exchanges;
  - The company utilizes a variable interest entity (VIE) structure;
  - The company does not comply with *Regulation Fair Disclosure*, which requires material information to be released to all investors at the same time.
2. Congress enact legislation stating that all provisions and the special status of Hong Kong included in the U.S.-Hong Kong Policy Act of 1992 will be suspended in the event that China's government deploys People's Liberation Army or People's Armed Police forces to engage in armed intervention in Hong Kong.
3. Congress enact legislation requiring the following information to be disclosed in all issuer initial public offering prospectuses and annual reports as material information to U.S. investors:
  - Financial support provided by the Chinese government, including: direct subsidies, grants, loans, below-market loans, loan guarantees, tax concessions, government procurement policies, and other forms of government support.
  - Conditions under which that support is provided, including but not limited to: export performance, input purchases manufactured locally from specific producers or using local intellectual property, or the assignment of Chinese Communist Party (CCP) or government personnel in corporate positions.
  - CCP committees established within any company, including: the establishment of a company Party committee, the standing of that Party committee within the company, which corporate personnel form that committee, and what role those personnel play.
  - Current company officers and directors of Chinese companies and U.S. subsidiaries or joint ventures in China who currently hold or have formerly held positions as CCP officials and/or Chinese government officials (central and local), including the position and location.
4. Congress hold hearings assessing the productive capacity of the U.S. pharmaceutical industry, U.S. dependence on Chinese pharmaceuticals and active pharmaceutical ingredients (APIs), and the ability of the U.S. Food and Drug Administration (FDA) to



guarantee the safety of such imports from China, with a view toward enacting legislation that would:

- Require the FDA to compile a list of all brand name and generic drugs and corresponding APIs that: (1) are not produced in the United States; (2) are deemed critical to the health and safety of U.S. consumers; and (3) are exclusively produced—or utilize APIs and ingredients produced—in China.
  - Require Medicare, Medicaid, the U.S. Department of Veterans Affairs, the U.S. Department of Defense, and other federally funded health systems to purchase their pharmaceuticals only from U.S. production facilities or from facilities that have been certified by the FDA to be in compliance with U.S. health and safety standards and that actively monitor, test, and assure the quality of the APIs and other components used in their drugs, unless the FDA finds the specific drug is unavailable in sufficient quantities from other sources.
  - Require the FDA, within six months, to investigate and certify to Congress whether the Chinese pharmaceutical industry is being regulated for safety, either by Chinese authorities or the FDA, to substantially the same degree as U.S. drug manufacturers and, if the FDA cannot so certify, forward to Congress a plan for protecting the American people from unsafe or contaminated drugs manufactured in China.
5. Congress require the relevant departments and agencies of jurisdiction—including the U.S. Department of the Treasury, the U.S. Department of Commerce, and the U.S. Securities and Exchange Commission—to prepare a report to Congress on the holdings of U.S. investors in Chinese bonds and other debt instruments. Such a report shall include information on the direct, indirect, and derivative ownership of any of these instruments.
  6. Congress direct the National Space Council to develop a strategy to ensure the United States remains the preeminent space power in the face of growing competition from China and Russia, including the production of an unclassified report with a classified annex containing the following:
    - A long-term economic space resource policy strategy, including an assessment of the viability of extraction of space-based precious minerals, onsite exploitation of space-based natural resources, and space-based solar power. It would also include a comparative assessment of China's programs related to these issues.
    - An assessment of U.S. strategic interests in or relating to cislunar space.
    - An assessment of the U.S. Department of Defense's current ability to guarantee the protection of commercial communications and navigation in space from China's growing counter-space capabilities, and any actions required to improve this capability.

- A plan to create a space commodities exchange to ensure the United States drives the creation of international standards for interoperable commercial space capabilities.
  - A plan to streamline and strengthen U.S. cooperation with allies and partners in space.
  - An interagency strategy to defend U.S. supply chains and manufacturing capacity critical to competitiveness in space.
7. Congress direct the U.S. Department of Justice to reestablish a higher education advisory board under the Federal Bureau of Investigation. In concert with the U.S. Department of Commerce's Bureau of Industry and Security, U.S. Department of Homeland Security, and U.S. Department of State, the higher education advisory board would convene semiannual meetings between university representatives and relevant federal agencies to review the adequacy of protections for sensitive technologies and research, identify patterns and early warning signs in academic espionage, assess training needs for university faculty and staff to comply with export controls and prevent unauthorized transfer of information, and share other areas of concern in protecting national security interests related to academic research.
  8. Congress direct the U.S. secretary of state to submit to Congress a report on actions that have been and will be taken by the United States to counter Beijing's attempts to isolate Taiwan's democratically-elected leaders and to strengthen support for Taiwan's engagement with the international community, including actions the Administration will take should Beijing increase its coercion against Taiwan. The report should:
    - List measures the U.S. government has taken and will take to expand interactions between U.S. and Taiwan government officials in accordance with the Taiwan Travel Act.
    - Formulate a strategy to expand development aid and security assistance to countries that maintain diplomatic ties with Taiwan.
    - Detail steps to expand multilateral collaboration involving Taiwan and other democracies to address global challenges, such as the Global Cooperation and Training Framework's workshops on epidemics, cybersecurity, and media literacy.
  9. Congress direct the Office of the Director for National Intelligence to prepare a National Intelligence Estimate of China's and Russia's approaches to competition with the United States and revision of the international order. The assessment would consider the influence of both countries' ideologies on their foreign policies, including areas both of overlap and of divergence; potential "wedge issues" the United States might exploit; and the implications for the North Atlantic Treaty Organization of a two-front conflict involving both China and Russia.
  10. Congress amend the U.S.-Hong Kong Policy Act of 1992 to direct the U.S. Department of State to develop a series of specific benchmarks for measuring Hong Kong's maintenance of a "high

degree of autonomy” from Beijing. Such benchmarks should employ both qualitative and quantitative measurements to evaluate the state of Hong Kong’s autonomy in the State Department’s annual *Hong Kong Policy Act Report*.

duce products with core competitiveness, and [we] won't be beaten in intensifying competition."<sup>106</sup>

China's technology push under General Secretary Xi builds upon earlier efforts but differs in at least three key aspects: a greater emphasis on the strategic importance of reducing reliance on foreign core technologies, the critical role of private companies, and the mobilization of new funding channels.<sup>107</sup> According to Mr. Hirson, China's private technology companies\* "rather than state-owned behemoths like China Telecom, represent China's 'national champions' in next generation areas."<sup>108</sup> China's major technology giants, including Baidu, Alibaba, and Tencent, have made large investments in AI and consumer internet and fintech industries.<sup>109</sup> Following the ZTE sanctions, Baidu, Alibaba, and Tencent each responded to Beijing's call for self-reliance by taking steps to support the development of the semiconductor industry in China.<sup>†</sup><sup>110</sup> In recent months, China's technology sector has faced stepped-up government scrutiny and increased pressure to align with Party edicts after years of thriving under light regulation‡—a trend some analysts caution may undermine Beijing's national strategy for innovation driven development.<sup>111</sup>

### *Addressing Shortfalls in Defense Technology*

Beijing is deeply concerned about its defense industry's capacity to independently innovate and develop the cutting-edge technologies it views as critical to what the CCP terms China's "core national power."<sup>112</sup> China has made great strides in key defense technologies related to cyber, space, advanced computing, and AI, and is a world leader in hypersonic weapons. Nevertheless, Beijing believes China is still lagging behind the United States, noting in its most recent defense white paper that China's military is "confronted by risks from technology surprise and a growing technological generation gap."<sup>113</sup> General Secretary Xi has demonstrated particular concern over shortfalls in China's technological capabilities, which he has described as the "root cause of [China's] backwardness."<sup>114</sup> China's defense industry continues to struggle to produce some high-end military components—such as advanced aircraft engines, guidance and control systems, and microprocessors—forcing Beijing to remain reliant on foreign technologies in these areas.<sup>115</sup> China continues to rely in particular on foreign innovation systems from the United States and Japan for the core technologies and talent it views as necessary to its national security.<sup>116</sup>

\*In China, direct ownership is not the primary determinant of the government's ability to control a company's decision making; in other words, private companies can also be directed to carry out government objectives. As described by Curtis J. Milhaupt and Wentong Zheng, "Large, successful [Chinese] firms—regardless of ownership—exhibit substantial similarities in areas commonly thought to distinguish SOEs from [private companies]: market dominance, receipt of state subsidies, proximity to state power, and execution of the state's policy objectives." Curtis J. Milhaupt and Wentong Zheng, "Beyond Ownership: State Capitalism and the Chinese Firm," *Georgetown Law Journal* 103 (2015): 665.

†For instance, in July 2018 Baidu unveiled its self-developed, high-end AI chip designed for autonomous vehicles and data centers. In September 2018, Alibaba established a semiconductor subsidiary to produce AI chips made for autonomous vehicles, smart cities, and smart logistics. Paul Triolo and Graham Webster, "China's Efforts to Build the Semiconductors at AI's Core," *New America*, December 7, 2018.

‡For example, in September 2019 Chinese state media reported that Hangzhou, a major technology hub in China, plans on assigning government officials to work with 100 local private companies, including Alibaba. Josh Horwitz, "China to Send State Officials to 100 Private Firms Including Alibaba," *Reuters*, September 23, 2019.

These plans and standards guidelines build on the progress of earlier policy initiatives to improve digital infrastructure. These initiatives have provided a technological foundation for quickly advancing AI subdomains.\* For example, creating numerous cameras and sensors to monitor traffic conditions as part of China's smart cities development program now provides the data for urban management systems like Alibaba's City Brain in Hangzhou, which uses AI to monitor and redirect traffic to reduce congestion.<sup>63</sup>

### *Industry Overview*

China has emerged as a leader in several subdomains of AI, in particular computer vision, digital lifestyle products (e.g., ride hailing and delivery applications), robotics, and speech recognition.<sup>64</sup> China is ahead of or on par with the United States in technologies that are poised for transformational growth from the application of AI, such as commercial and military strike-capable drones incorporating autonomous navigation.<sup>65</sup> China trails the United States in autonomous vehicle (AV) technology but is rapidly catching up.<sup>66</sup>

Many Chinese AI companies that appear most competitive vis-à-vis the United States are an outgrowth of the country's broad adoption of mobile internet and use of mobile applications,† which gives China's leading mobile platforms like Baidu, Alibaba, and Tencent unparalleled access to consumer data.<sup>67</sup> By contrast, China's advances in industrial robotics have been driven by extensive government support and overseas acquisitions,‡ as well as some spillover from major international robot manufacturers locating production facilities in China.<sup>68</sup>

Computer vision falls somewhere in between, with private funding responding to a demand created by government policy. Chinese image recognition startups outperform and are far better funded than international peers, but China's Ministry of Public Security is a primary customer for facial recognition in surveillance systems and the National Development and Reform Commission, an economic planning agency, has issued policy encouraging use of AI in facial recognition.<sup>69</sup> China's widespread use of surveillance applications of

\*For instance, the white paper includes an appendix of ten applications of AI by Chinese companies to provide a template for different AI standards, but these technologies were in many cases supported by earlier industrial policies. In intelligent manufacturing, the white paper champions Haier's COSMOplat, a customizable manufacturing execution and supply chain management system that was developed under Made in China 2025. Standards Administration of China and China Electronic Standardization Institute, *White Paper on Artificial Intelligence Standardization* (人工智能标准化白皮书), January 2018, 96–98. Translation.

†China's mobile internet ecosystem developed with minimal competition from foreign firms due to mandated government monopolies in telecommunications, the Golden Shield Project (popularly known as the "Great Firewall") which prohibits access to popular foreign sites like Google and Facebook from within mainland China's borders, strict licensing requirements for provision of content over the internet, including via mobile applications, and increasingly demanding regulations on management of user data. Hugo Butcher Piat, "Navigating the Internet in China: Top Concerns for Foreign Businesses," *China Briefing*, March 12, 2019; Ashwin Kaja and Eric Carlson, "China Issues New Rules for Mobile Apps," *Inside Piracy*, July 1, 2016.

‡Chinese state-owned enterprises have concluded several major acquisitions of robotics and automation firms since Made in China 2025 encouraged closing China's technological gap through acquiring foreign firms, including Chinese air conditioner and refrigerator manufacturer Midea Group's acquisition of a majority stake in German robot maker Kuka AG, the world's largest producer of robots used in auto factories. U.S.-China Economic and Security Review Commission, *Hearing on Technology, Trade, and Military-Civil Fusion*, written testimony of Dan Coughlin, June 7, 2019, 4; Sun Congying, "Midea, Kuka Chase Automation Dreams with \$1.6 Billion Park," *Caixin*, March 29, 2018; Sun Yuyao, "Overseas Mergers and Acquisitions: Chinese Manufacturing Integrates into the Global Industrial System (海外并购并喷 中国制造融入全球产业体系)," *Advanced Manufacturing Daily*, December 29, 2012.



AI is driven in large part by the absence of privacy protections and by government repression of ethnic groups.<sup>70</sup> For example, law enforcement agencies across China are deploying facial recognition to identify and track Uyghurs, a Muslim minority from northwestern Xinjiang Province.<sup>71</sup>

Both the government and private sector are substantial investors in China's AI. In their AI development plans, the municipal governments of Shanghai and Tianjin each pledge to invest \$15 billion in AI, close to Google's parent Alphabet's \$16.6 billion in global R&D expenditure during 2017.<sup>\*72</sup> However, China's government guidance funds do not always raise or spend the money as planned due to a shortage of investors, inability to recruit qualified personnel to manage the funds, and lack of investment targets that meet the funds' investment criteria, among other reasons.<sup>73</sup> Nonetheless, in start-up funding, technology market research firm CB Insights estimates that Chinese companies (including Hong Kong-based companies) received 48 percent of global AI equity investment in 2017, ahead of the United States' 38 percent and up from 11 percent in 2016.<sup>74</sup> A handful of large foreign VC groups like Japanese conglomerate SoftBank and U.S. VC firm Sequoia are active investors in China's AI market.<sup>75</sup>

### China's AI "National Team"

In November 2017, China's Ministry of Science and Technology selected Baidu, Alibaba, and Tencent, as well as voice recognition firm iFlytek, to form a "National Team" charged with developing AI in a range of subdomains.<sup>†76</sup> According to the government plan, Baidu is to focus on autonomous driving, Alibaba is to focus on cloud computing and smart cities, Tencent is to focus on AI-powered medical diagnosis, and iFlytek is to continue working on voice intelligence.<sup>77</sup> Hong Kong-based facial recognition start-up SenseTime was subsequently tapped to focus on intelligent vision.<sup>78</sup>

In both design and execution, the national team approach differs from overt promotion of national champions.<sup>‡</sup> None of the firms are state-owned and all had established capabilities in their assigned subdomains before being selected.<sup>79</sup> In some respects,

<sup>\*</sup>Alphabet's financial disclosures do not distinguish investments in AI from other capabilities and products, but it is likely the world's largest corporate spender on AI. Alphabet Inc., *Form 10-K for the Fiscal Year Ended December 31, 2017*, February 5, 2018, 36; *Economist*, "Google Leads in the Race to Dominate Artificial Intelligence," December 7, 2017.

<sup>†</sup>Chinese agencies have occasionally designated a "national team" of companies with pre-existing capabilities to focus on building up capacity in a particular field, such as the Ministry of Commerce's 2010 policy to support well-established brick and mortar retailers in developing e-commerce operations. Companies in a national team do not receive anticompetitive policy support to the extent of national champions and have more autonomy to pursue business avenues other than those directed by the government. U.S.-China Economic and Security Review Commission, *Hearing on Technology, Trade and Military-Civil Fusion*, written testimony of Jeffrey Ding, June 7, 2019, 8. Tencent Technology, "China's Ministry of Commerce's Support for Three Large Companies in the 'Ecommerce National Team' Revealed" (商务部扶持电子商务 "国家队" 三大企业曝光), *China Information Industry Network*, March 3, 2010. Translation.

<sup>‡</sup>National champions are large, often state-owned firms that advance state interests, whether to establish capacity in a new sector or become competitive internationally in a particular sector. Typically, they receive policy support to assist in advancing state objectives, including subsidies, tax credits, guaranteed market share or monopoly access in certain industries, and supportive regulation and financing to acquire or displace smaller competitors or vertically integrate within other functions of an industry.

These plans and standards guidelines build on the progress of earlier policy initiatives to improve digital infrastructure. These initiatives have provided a technological foundation for quickly advancing AI subdomains.\* For example, creating numerous cameras and sensors to monitor traffic conditions as part of China's smart cities development program now provides the data for urban management systems like Alibaba's City Brain in Hangzhou, which uses AI to monitor and redirect traffic to reduce congestion.<sup>63</sup>

### *Industry Overview*

China has emerged as a leader in several subdomains of AI, in particular computer vision, digital lifestyle products (e.g., ride hailing and delivery applications), robotics, and speech recognition.<sup>64</sup> China is ahead of or on par with the United States in technologies that are poised for transformational growth from the application of AI, such as commercial and military strike-capable drones incorporating autonomous navigation.<sup>65</sup> China trails the United States in autonomous vehicle (AV) technology but is rapidly catching up.<sup>66</sup>

Many Chinese AI companies that appear most competitive vis-à-vis the United States are an outgrowth of the country's broad adoption of mobile internet and use of mobile applications,† which gives China's leading mobile platforms like Baidu, Alibaba, and Tencent unparalleled access to consumer data.<sup>67</sup> By contrast, China's advances in industrial robotics have been driven by extensive government support and overseas acquisitions,‡ as well as some spillover from major international robot manufacturers locating production facilities in China.<sup>68</sup>

Computer vision falls somewhere in between, with private funding responding to a demand created by government policy. Chinese image recognition startups outperform and are far better funded than international peers, but China's Ministry of Public Security is a primary customer for facial recognition in surveillance systems and the National Development and Reform Commission, an economic planning agency, has issued policy encouraging use of AI in facial recognition.<sup>69</sup> China's widespread use of surveillance applications of

\*For instance, the white paper includes an appendix of ten applications of AI by Chinese companies to provide a template for different AI standards, but these technologies were in many cases supported by earlier industrial policies. In intelligent manufacturing, the white paper champions Haier's COSMOplat, a customizable manufacturing execution and supply chain management system that was developed under Made in China 2025. Standards Administration of China and China Electronic Standardization Institute, *White Paper on Artificial Intelligence Standardization* (人工智能标准化白皮书), January 2018, 96–98. Translation.

†China's mobile internet ecosystem developed with minimal competition from foreign firms due to mandated government monopolies in telecommunications, the Golden Shield Project (popularly known as the "Great Firewall") which prohibits access to popular foreign sites like Google and Facebook from within mainland China's borders, strict licensing requirements for provision of content over the internet, including via mobile applications, and increasingly demanding regulations on management of user data. Hugo Butcher Piat, "Navigating the Internet in China: Top Concerns for Foreign Businesses," *China Briefing*, March 12, 2019; Ashwin Kaja and Eric Carlson, "China Issues New Rules for Mobile Apps," *Inside Piracy*, July 1, 2016.

‡Chinese state-owned enterprises have concluded several major acquisitions of robotics and automation firms since Made in China 2025 encouraged closing China's technological gap through acquiring foreign firms, including Chinese air conditioner and refrigerator manufacturer Midea Group's acquisition of a majority stake in German robot maker Kuka AG, the world's largest producer of robots used in auto factories. U.S.-China Economic and Security Review Commission, *Hearing on Technology, Trade, and Military-Civil Fusion*, written testimony of Dan Coughlin, June 7, 2019, 4; Sun Congying, "Midea, Kuka Chase Automation Dreams with \$1.6 Billion Park," *Caixin*, March 29, 2018; Sun Yuyao, "Overseas Mergers and Acquisitions: Chinese Manufacturing Integrates into the Global Industrial System (海外并购并喷 中国制造融入全球产业体系)," *Advanced Manufacturing Daily*, December 29, 2012.

Addendum I: China’s Development of AI Technologies

AI Technology	Applications	Key Industrial Policies	China’s Current Capabilities	Key Companies
Machine Learning, which includes Deep Learning	Foundational for other areas of AI	Cultivating talent in advanced machine learning and leading in machine learning theory are cornerstones of China’s Strategy to dominate in global AI by 2030, unveiled in 2017. The National Development and Reform Commission has also tapped search engine giant Baidu to lead a nationwide online deep learning lab in coordination with Tsinghua and Beihang universities.	Chinese researchers have closed the gap with the United States in publication volume, but China lacks talent in the top echelon. Engineers focus mostly on commercial gains, not fundamental breakthroughs. China’s advantages in sheer volume of data are curtailed by its ability to label and analyze this data. China also lags in producing chips optimized for machine learning.	General: Alibaba, Tencent, Baidu; Chips: Cambricon (used in Huawei phones), Horizon Robotics
Natural Language Processing (NLP)	Speech/voice recognition, information retrieval/extraction, query answering, sentiment analysis	NLP is listed as one of eight “key common technologies” to be developed in China’s AI strategy. Chinese universities are partnering with companies to develop NLP applications, and several Chinese industry associations have launched respected conferences.	In research, China has been second behind the United States for five years. In industry, China is leading in chatbots and is developing machine translation for Chinese to languages in BRI countries. iFlytek is a leader in speech recognition for spoken Chinese.	Baidu, iFlytek; Microsoft, Research Asia is a major player for machine translation and chatbots.
Computer Vision and Biometrics	Facial and other image recognition, machine vision (analyzing images for inspection and process control)	China’s smart cities initiative promotes surveillance technology, and many companies have contracts with public security bureaus. Computer vision accounted for 35 percent of China’s AI market in 2017.	Numerous facial recognition companies, including many startups, are powering China’s surveillance state. In turn, internet giants like Huawei are integrating this tech into—and exporting—“Safe City” systems.	SenseTime, Yitu, Megvii (Face++), Xloong, Zoloz, DeepGlint, Huawei

Chinese voices [that are critical of Beijing] can be silenced in Australia,” Dr. Medcalf contends, “they can be silenced anywhere.”<sup>13</sup>

***Responding to China’s Interference, Australia’s Progress Uncertain***

Since 2016, following revelations of Australia’s vulnerability to CCP interference, Canberra has passed several new laws to counter foreign interference.\* These new laws, which began to enter into force in 2018, target foreign interference in politics, economic espionage, and theft of trade secrets; establish a public register of foreign lobbyists; and require notification of political donations from those on the register or who disburse funds on behalf of a foreign principal.<sup>14</sup> Canberra has also formed a new Department of Home Affairs to integrate certain intelligence, law enforcement, and policy responsibilities across the government and ordered the most significant review of its intelligence agencies in 40 years, which is still ongoing.<sup>15</sup>

Huang Xiangmo, a former Australian permanent resident and prolific political donor accused of acting as a proxy for Beijing, has been a primary focus of much of the public debate surrounding CCP interference in Australia.<sup>16</sup> From 2014 to 2017, Mr. Huang was the president of the Australian Council for the Promotion of Peaceful Reunification of China, a political advocacy organization that frequently disguises the nature of its relationship to the Chinese government but is in fact directly subordinate to the CCP’s United Front Work Department.<sup>17</sup> He received scrutiny for his donations to both major Australian political parties totaling \$1.5 million (AUD 2 million) since 2012, and he was accused of being a CCP “agent of influence” by an Australian senator who resigned due to public disclosure of his collaboration with Mr. Huang.<sup>†</sup><sup>18</sup> In February 2019, the Australian government revoked Mr. Huang’s permanent residency and denied his application for citizenship, citing concerns about his character.<sup>19</sup>

Australia’s new Foreign Influence Transparency Scheme, passed in 2018 and based on the U.S. Foreign Agents Registration Act, was intended to introduce transparency into foreign lobbying in Canberra, but registration and enforcement have so far been lackluster. Canberra has yet to prosecute any United Front-connected entities, such as Confucius Institutes and most Chinese state media, for not registering, despite the fact United Front activities were a primary focus of the law.<sup>20</sup> As of July 2019, only 18 Chinese foreign principals had registered, mostly comprising mineral, energy, and investment companies, as well as China Radio International and China Telecom, state-owned media and telecommunications companies, respectively.<sup>‡</sup><sup>21</sup> Only three former Cabinet ministers or designat-

\*For more on the events leading to the passage of Australia’s new counter-foreign interference laws, see U.S.-China Economic and Security Review Commission, Chapter 3, Section 2, “China’s Relations with U.S. Allies and Partners,” in *2018 Annual Report to Congress*, November 2018, 304–339.

†Unless noted otherwise, this section uses the following exchange rate throughout: AUD 1 = \$0.68.

‡The United States Studies Center at the University of Sydney, which has an arrangement with the U.S. Department of State for “general political lobbying,” has registered. Australian Government Attorney-General’s Department, *United States Studies Center Foreign Influence Transparency Scheme Register Registration Record*, September 28, 2018.

ed position holders—a key type of lobbyist intended to be captured by the law—had registered as lobbyists for Chinese foreign principals by July 2019.\*<sup>22</sup> Notably, some of the most prominent former officials who became lobbyists for Beijing after their government service, such as former Minister of Trade and Investment Andrew Robb, former Foreign Minister Bob Carr, and former Premier of Victoria State John Brumby, left their lobbying positions before the law took effect, demonstrating some desire not to be perceived as working for Beijing.<sup>23</sup>

### *Australia Struggles with Disinformation and Censorship in Chinese-Language Media*

Disinformation is a serious concern for Australian media, particularly given the outsize influence of Chinese platforms, which are an important tool in Beijing's influence operations targeting the Chinese diaspora.<sup>24</sup> There are dozens of Chinese-language media outlets in Australia, and nearly all of them have been brought under the influence of Beijing to some degree. Over roughly the last ten years, the Chinese embassy and consulates in Australia have used coercion and threats to get these media to increasingly parrot the CCP's line.<sup>25</sup> For example, the Chinese consulate in Sydney repeatedly warned a local government† with a large ethnic Chinese population not to engage with one of the few remaining independent Australian Chinese-language media outlets, *Vision China Times*, including forcing its council to ban the paper from sponsoring a Lunar New Year celebration.<sup>26</sup> Beijing has long sought to pressure or coerce this newspaper into changing its coverage. *Vision China Times* general manager Maree Ma said in April 2019 that Chinese officials "don't like any media outlets that they cannot ... control."<sup>27</sup>

Most Australian Mandarin-speakers access news through WeChat, a social media app now indispensable among many Chinese communities for communication and other purposes, raising concerns about Beijing's ability to target them with disinformation spread over the platform.‡<sup>28</sup> The use of the platform has spread beyond the Chinese Australian community, with about 3 million Australians using WeChat by 2017, according to Australia's Special Broadcast

\*Designated position holders include Ministers, Members of Parliament, some Parliamentary staff, Agency heads and deputy heads (and equivalent offices), and Ambassadors or High Commissioners stationed outside Australia. As of July 2019, designated position holders registered under the Scheme included former Australian Senator Richard Allston, working on behalf of China Telecom (Australia); former Senator Nick Bolkus, working on behalf of Jiujiang Mining Australia; and former Ambassador to China Geoffrey Raby, working on behalf of Yancoal. Australian Government Attorney-General's Department, *Transparency Register: China*; U.S.-China Economic and Security Review Commission, *2018 Annual Report to Congress*, November 2018, 325.

†A local government is the third tier of government in Australia, below the state or territory level and the federal level. Its governing body is referred to as a council. Nick McKenzie, "China Pressured Sydney Council into Banning Media Company Critical of Communist Party," *Four Corners*, April 9, 2019; *Australian Collaboration*, "Democracy in Australia—Australia's Political System," May 3, 2013, via the Internet Archive Wayback Machine. <https://web.archive.org/web/20140127041502/http://www.australiancollaboration.com.au/pdf/Democracy/Australias-political-system.pdf>.

‡Based on WeChat penetration in mainland China, which reaches 93 percent in tier 1 cities, media researcher Wanning Sun estimated almost the entire Mandarin-speaking community in Australia—approximately 597,000 people as of 2016, or 2 percent of Australia's population—used WeChat. Wanning Sun, "How Australia's Mandarin Speakers Get Their News," *Conversation*, November 22, 2018; Lucy Lv, "Who Are the Australians That Are Using China's WeChat?" *Special Broadcasting System*, November 3, 2017; Australia's Bureau of Statistics, *Census Reveals a Fast Changing, Culturally Diverse Nation*, June 27, 2017; Wanning Sun, "Chinese-Language Media in Australia: Developments, Challenges, and Opportunities," *Australia-China Relations Institute*, 2016, 45–46.



# EXHIBIT 19



08 JAN 2018

## **An Orwellian future is taking shape in China**

By Fergus Ryan

When Google stopped operating its China-based search engine in 2010 in protest against censorship, scores of young people placed wreaths at the company headquarters in Beijing as a sign of mourning.

At the time, vibrant debate and commentary on Chinese social media platforms like Sina Weibo held out some promise for the emergence of an online civil society with the power to expose corruption and effect change.

The Chinese Communist Party was caught in a vice — seeing the internet as an avenue for pursuing economic growth, while at the same time fretting about the political disruption it augured.

But, seemingly against all odds, Beijing has managed to strike the balance between harnessing the internet for economic growth and guarding against its threats to security – something former president Bill Clinton once called the equivalent of "nailing Jell-O to a wall".

Since Google pulled its search engine from the market, China's digital economy has grown into a US\$3 trillion steamroller, fuelled by 750 million netizens.

Homegrown tech companies, protected from foreign competition by the "great firewall" have grown into behemoths.

Chinese tech giant Tencent has become the first Asian company ever to be valued above US\$500 billion. Rival tech giant Alibaba Group is nipping at its heels with a market capitalisation of \$US481 billion.

So far, the US tech giants and their Chinese rivals have been in a sort of detente, with neither making significant forays into each other's territory. But that is starting to change. In recent months, Tencent has been on a buying spree, investing in Tesla, Snap and Spotify.

The pressure for foreign tech companies to enter the Chinese market has increased. In a significant milestone, Google unveiled plans in December to return to the middle kingdom by opening an artificial intelligence research centre in Beijing.

China has some clear advantages for the next phase of digital growth: a strong corps of engineers, plenty of money and a huge amount of data, not to mention a lack of concern about privacy for making use of it.

Beijing has made no secret of its goal to become the world leader in AI by 2030. Other emerging fields like quantum computing, robotics, cloud computing, and smart cities are firmly in its sights.

Already, the beginnings of a truly Orwellian future in China are taking shape. Tencent is working with authorities to develop an "early-warning system" for predicting the size of crowds and their movement.

Alibaba founder Jack Ma has said that so-called smart cities powered by his company's computers and artificial-intelligence algorithms will make it possible to predict security threats. "Bad guys won't even be able to walk into the square," he told a Communist Party commission overseeing law enforcement last year.

What's now clear is that the Chinese Communist Party has shown a remarkable ability, not just to control the internet, but to harness it to achieve its desired ends.

Chinese tech companies have little choice but to cooperate with it. Whether foreign tech companies go along for the ride is still an open question.

**ORIGINALLY PUBLISHED BY: SYDNEY MORNING HERALD ON 08 JAN 2018**

---

## About the author(s)



### Fergus Ryan

Fergus is an Analyst working with International Cyber Policy Centre.



## Topics

## You may also be interested in



20 AUG 2020

## **Hunting the Phoenix**

By Alex Joske

---



## **China's feverish overreach wasted an opportunity offered by Covid-19**

By Huong Le Thu



# EXHIBIT 20

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284>

WORLD | ASIA | CHINA

# China's Tech Giants Have a Second Job: Helping Beijing Spy on Its People

Tencent and Alibaba are among the firms that assist authorities in hunting down criminal suspects, silencing dissent and creating surveillance cities



Alibaba Group's campus in Hangzhou, China, contains a police outpost.

PHOTO: QILAI SHEN/BLOOMBERG NEWS

By [Liza Lin](#) and [Josh Chin](#)

Nov. 30, 2017 10:38 am ET

HANGZHOU, China—Alibaba Group’s sprawling campus has collegial workspaces, laid-back coffee bars and, on the landscaped grounds, a police outpost.

Employees use the office to report suspected crimes to the police, according to people familiar with the operation. Police also use it to request data from Alibaba for their own investigations, these people said, tapping into the trove of information the tech giant collects through its e-commerce and financial-payment networks.

In one case, the police wanted to find out who had posted content related to terrorism, said a former Alibaba employee. “They came to me and asked me for the user ID and information,” he recalled. He turned it over.

---

MORE FROM THE WSJ

---



---

**Finance Pros Say You’ll Have to Pry Excel Out of Their Cold, Dead Hands**



RICHARD B. LEVINE/ZUMA PRESS

The Chinese government is building one of the world’s most sophisticated, high-tech systems to keep watch over its citizens, including surveillance cameras, facial-recognition technology and vast computers systems that comb through terabytes of data. Central to its efforts are the country’s biggest technology companies, which are openly acting as the government’s eyes and ears in cyberspace.

Companies including Alibaba Group Holding Ltd., Tencent Holdings Ltd. and Baidu Inc., are required to help China’s government hunt down criminal

suspects and silence political dissent. Their technology is also being used to create cities wired for surveillance.

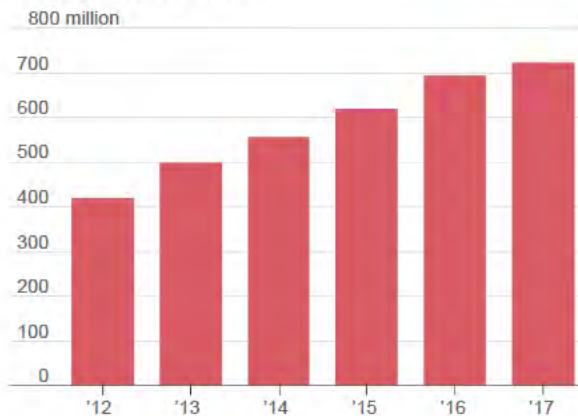


This assistance is far more extensive than the help Western companies extend to their governments, and the requests are almost impossible to challenge, a Wall Street Journal examination of Chinese practices shows.

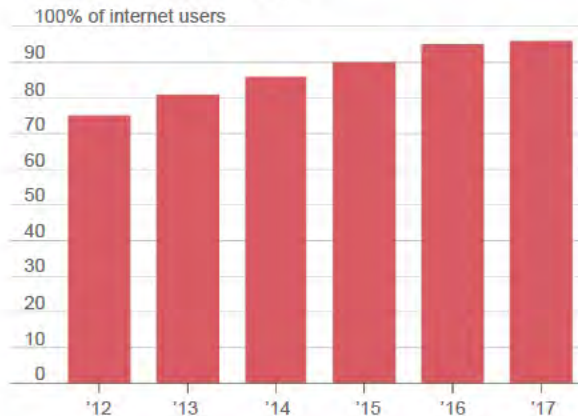
### Going Mobile

Mobile internet usage in China has grown rapidly.

#### Mobile internet users



#### Mobile internet penetration



Source: China Internet Network Information Center

Unlike American companies, which often resist U.S. government requests for information, Chinese ones talk openly about working with authorities. Tencent Chief Executive Ma Huateng, also known as Pony Ma, and Alibaba founder Jack Ma both have voiced support for private companies working with the government on law enforcement and security issues.

“The political and legal system of the future is inseparable from the internet, inseparable from big data,” Alibaba’s Mr. Ma told a Communist Party commission overseeing law enforcement last year. He said technology will soon make it possible to predict security threats. “Bad guys won’t even be able to walk into the square,” he said.

In practice, China’s internet giants, which have benefited from trade policies shielding them from foreign competition, have little choice but to

cooperate in a country where the Communist Party controls both the legal system and the right to function as a business.

Tencent, the world’s largest online videogame company, dominates Chinese cyberspace with news, video-streaming operations and its WeChat app, used by nearly one billion people to communicate and for mobile payments.

Beijing activist Hu Jia said he bought a slingshot online after a friend recommended it for relieving stress. He paid with WeChat's mobile-payment feature. Mr. Hu said he was later interrogated by a state security agent, who asked if he was planning to shoot out surveillance cameras near his apartment.



Beijing activist Hu Jia, on left in 2013, says 'everyone has a spy watching them. That spy is their smartphone.'

PHOTO: KIM KYUNG HOON/REUTERS

A few years earlier, Mr. Hu said, he had messaged a friend headed to Taiwan with the names of activists he might want to see while traveling there. Later, he said, state security agents showed up at the friend's house and warned him against meeting Mr. Hu's acquaintances.

"Experience has proven that WeChat is completely compromised," especially for people on the government's watch list, Mr. Hu said. "Everyone has a spy watching them. That spy is their smartphone."



Neither Tencent nor Chinese security officials responded to requests for comment.

When discussing their cooperation with the government, Chinese companies point to disclosures by former National Security Agency contractor Edward Snowden, which detailed how U.S. tech and telecommunications companies granted U.S. government agencies access to user data. Earlier, many American phone companies had complied with a secret National Security Agency program to intercept the communications of some U.S. citizens without a court warrant.

U.S. government requests for information about U.S. citizens or legal residents now have to be approved by a court. Chinese police, by contrast, can rely on a search warrant issued by the police themselves.

“I would disagree with the premise that the central government has access to all this corporate data. That’s just not true,” said Joseph Tsai, Alibaba’s executive vice chairman, at the Journal’s D.Live conference in October. “If they want data from you, just like in the U.S., they have to have a reason.”

Alibaba and other tech companies push back if they believe a Chinese government request for data isn’t warranted, said a Chinese police official familiar with the operations of the country’s cyberpolice. He said law enforcement must follow set procedures to gain access to private information.

China’s government, however, has the last word. There is no independent judiciary to approve or review government requests—or for companies to appeal to if they disagree with a demand.

It is unlikely any Chinese company could mount the sort of challenge Apple Inc. did when it refused to comply with a request by the U.S. Federal Bureau of Investigation to unlock the iPhone of a suspect in the San Bernardino mass shooting in 2015.



PHOTO: QILAI SHEN/BLOOMBERG NEWS

**The political and legal system of the future is inseparable from the internet, inseparable from big data.**

— Jack Ma, founder, Alibaba Group

Over the past year, Chinese regulators have ordered three popular internet platforms to stop streaming videos with political content not in line with government policy, and they more recently warned that companies that didn't comply with new social-media rules would be shut down. Facebook Inc. was banned in China in 2009, without a stated reason.

On June 1, a new cybersecurity law went into effect that requires companies running internet platforms in China to help authorities ferret out content that “endangers national security, national honor and interests.”

That goes far beyond U.S. government demands on internet service providers or platforms, which are required by law to report suspected instances of child pornography when they discover it and take down material that has been found to infringe on copyrights.

Chinese government authorities didn't respond to requests for comment for this article.

In one of the first significant actions under the new law, China's Cyberspace Administration this fall slapped maximum fines on Tencent, internet company Baidu and others for allowing users to spread banned content, including "false rumors" and pornography.

Tencent said it "sincerely accepted" the punishment and vowed to do a better job. Baidu outlined a plan to use big data and artificial intelligence to better identify and dispel rumors. A Baidu spokeswoman said the new platform was developed in collaboration with police and other public and private agencies, and was designed to ensure users get accurate information.



PHOTO: MIKE BLAKE/REUTERS

## **I would disagree with the premise that the central government has access to all this corporate data.**

— Joseph Tsai, executive vice chairman, Alibaba

Alibaba has data on hundreds of millions of Chinese citizens who use the company and its affiliated services to shop online, stream videos, pay rent, send text messages, make comments on social media and more.

The job of monitoring traffic on these platforms falls to its Alibaba Security Team, whose Chinese name—Shendun—can be translated as “Magic Shield.”

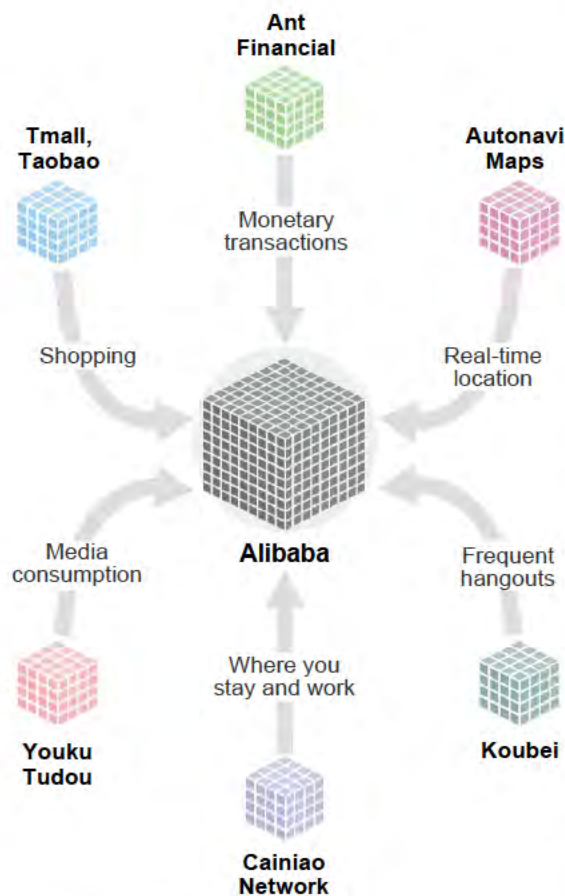
At the company’s Hangzhou campus, computer programs sweep Alibaba’s internet commerce sites and flag anything that might be prohibited, such as guns and pornography, according to current and former Magic Shield agents.



The security team scans the websites for suspicious sales, one former staffer said, such as tea being sold for an exorbitant price, an indication it might really be illegal drugs. Agents then review and remove objectionable content, and in cases of scams such as monetary fraud, will alert the police, the current and former agents said.

### Data Central

Chinese consumers use their smartphones for a wide variety of activities, giving Alibaba a vast trove of data through the portals it owns or has a stake in.



Source: Alibaba annual report

In a video published on the team's Twitter-like Weibo site, the Magic Shield team is shown working at computer screens. "Guns, rubber bullets, drugs," the narrator says. "As long as it's illegal, it will not escape our control."

The team has assisted police in "several thousand cases," the video says. The team also is called in to help police with criminal investigations, people familiar with the operations say.

Plans to set up police outposts at tech companies were disclosed in a 2015 posting on China's Ministry of Public Security website, which said the intent was to "find out about criminal activity at its first instance."

An Alibaba spokeswoman said the company's campus includes "a designated meeting space where law-enforcement staff visit occasionally to communicate the latest updates on regulation. If there are established criminal cases, our team will also use

this space to discuss the extent of our assistance in those investigations as required by law. There are no police officers stationed on our campus."



Unlike their Chinese counterparts, U.S. tech companies, including Apple, Facebook and Alphabet Inc.'s Google, routinely disclose their government cooperation in transparency reports.



Chinese President Xi Jinping, front, was applauded by Chinese and American technology CEOs and other executives at Microsoft Corp.'s campus in Redmond, Wash., in 2015.

PHOTO: TED S. WARREN/PRESS POOL/GETTY IMAGES

Google, whose services are mostly blocked in China, said there were 23 Chinese government requests for Google to remove content in the second half of 2016, mostly for national security reasons.

Apple disclosed that more than 35,000 user accounts were affected by 24 Chinese law-enforcement requests in the first half of this year, many in connection with fraud investigations. It said it provided information on about 90% of them.

Chinese companies don't release any information on the number of requests from the government, the nature of the requests or the compliance rate.

Tencent's online monitoring operations use computers to filter its streamed videos, news feeds and other online platforms for obscene and politically sensitive content, according to people familiar with the operation.

---

## SELF-POLICING THE INTERNET

---

Chinese and U.S. internet platforms face different government standards for policing content.

### PORNOGRAPHY:

- ✚ **U.S.:** Responsible for reporting child pornography
- ✚ **China:** Must be removed and reported. Liable for hosting content.

### TERRORISM CONTENT:

- ✚ **U.S.:** May voluntarily remove, but no legal responsibility to report.
- ✚ **China:** Must be removed and reported. Liable for hosting content.

### CONTENT PROMOTING GAMBLING:

- ✚ **U.S.:** Online gambling is mostly illegal. Should not accept online gambling ads and must not host, promote or support gambling activities.
- ✚ **China:** Must be removed and reported. Liable for hosting content.

### CONTENT CONTAINING STATE SECRETS:

- ✚ **U.S.:** Acquiring or leaking state secrets is prohibited, but re-publication of such material is protected by First Amendment. May voluntarily remove.
- ✚ **China:** Must be removed and reported. Liable for hosting content.

### CONTENT UNDERMINING PUBLIC MORALITY:

- ✚ **U.S.:** No legal responsibility to report.
- ✚ **China:** Must be removed and reported. Liable for hosting content.

*Sources: Stanford Law School, Baker McKenzie*

---

Censors at Chinese companies are responsible for blocking unfavorable references to the Communist Party and senior leaders, as well as foreign news stories casting China in a negative light. Computers are programmed to spot thousands of words and phrases and delete most of the offensive content, according to the people familiar with the censorship operations.

Users of Tencent's WeChat app who run large group chats say they have received automated warnings about politically sensitive content. Some political activists say their WeChat accounts have been suspended or closed for posts critical of the government.

During important political events, staffers with China's internet regulator set up shop at Chinese content providers to catch anything that might slip through the cracks, people familiar with the operations said. The regulator, the Cyberspace Administration of China, didn't respond to a request for comment.

Along with access to online data, China's government wants something else from tech companies—the cloud computing prowess to sort and analyze information. China wants to crunch data from surveillance cameras, smartphones, government databases and other sources to create so-called smart cities and safe cities.

Alibaba's computers and artificial-intelligence algorithms power a "city brain" in Hangzhou that improves traffic flow and clears the path for ambulances by using mobile mapping and data from traffic cameras to time traffic signals. The company said its cloud and data services also have helped manage aircraft parking in Guangzhou and deploy tour guides in Wuhan.



Chinese President Xi Jinping appeared on a screen during the annual World Internet Conference in Wuzhen, China, in 2016.

PHOTO: ALY SONG/REUTERS

The township of Wuzhen hosts an annual internet conference attended by political and technology leaders. Chinese citizens with grievances show up, too, hoping to get their attention. Police now work with Alibaba to use surveillance footage and data processing to identify “persons of interest” and keep them out, local police official Dai Jinming said at a recent conference sponsored by Alibaba.

---

## INSIDE CHINA’S SURVEILLANCE STATE

---

[Surveillance Cameras Made by China Are Hanging All Over the U.S.](#)

[China’s All-Seeing Surveillance State Is Reading Its Citizens’ Faces](#)

---

Tencent is working with police in the southern city of Guangzhou to build a cloud-based “early-warning system” that can track and forecast the size and movement of crowds, according to a statement from the Guangzhou police bureau.

Maya Wang, a Hong Kong-based researcher for Human Rights Watch, contends the proclaimed benefits of such wired cities mask their true purpose. “This whole safe city idea is a massive surveillance project,” she said.

The government-sponsored Smart Cities Work Committee didn’t respond to a request for comment.

China’s latest five-year development plan calls for 100 smart-city trials to be rolled out next year.

By 2020, the plan says, smart cities will make up a “ubiquitous system” that is expected to “achieve remarkable results.”

— *Xiao Xiao and Lingling Wei contributed to this article.*

*Appeared in the December 1, 2017, print edition as ‘China’s Tech Giants Have a Side Job: Helping Beijing Spy.’*

Copyright © 2020 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.



Columbia Journalism Review

Study: Chinese-American immigrants fall prey to WeChat's misinformation problem

By Chi Zhang

April 19, 2018

If you Google “Haissam Massalkhy,” you’ll find a handful of unremarkable news stories about a fatal traffic collision where the Lebanese motorist struck a Chinese jogger in Walnut, California. On WeChat, however, it was a different story altogether.

Within Chinese-language narratives on the mobile messaging app, the jogger’s death rallied cries of injustice. The story that spread went something like this: Massalkhy had intentionally killed the Chinese man so that he could go to prison and take advantage of loopholes created by sanctuary laws—instead of being deported as his visa expired. As one headline on the platform decried, “Kill a Chinese, get a green card.”

ICYMI: WeChat reaches audiences conventional media in China cannot

A new report from the Tow Center for Digital Journalism investigates the many dynamics of WeChat’s information problem, which have an especially large impact on first-generation Chinese immigrants trying to integrate to life in the US. As an increasingly central news ecosystem and online community for Chinese Americans, WeChat offers key clues to how political information and misinformation are constructed for and distributed among this emerging political constituency.

In the cases of misinformation examined in the report, an array of WeChat outlets generate multiple copies of the same false story—often with an agenda attached. And in an information ecosystem whose default is provocation and sensationalism, those focused on debunking misinformation have a hard time competing.

The information challenge of WeChat is as much a story about the platform as one about the communities it serves. For instance, the study finds a striking divergence between how much an issue was given attention on WeChat when it was not reported by English-language media. Top issues on the platform during the period of study, including affirmative action and census data disaggregation, hardly received any coverage in English-speaking media. The invisibility of these issues in mainstream media drives users to WeChat, where the topics become focal points of discussion and mobilization among first-generation Chinese. Another top issue on the platform that emerged was undocumented immigration, especially anger around sanctuary cities. The barrage of WeChat coverage aligned with recent protests by first-generation Chinese against sanctuary laws offering paths to citizenship for undocumented immigrants. Examples like these highlight the need to connect with the immigrant population served by this information ecosystem, understand which issues matter to them, and why distorted narratives may resonate.

Like other platforms, WeChat is home to a garden variety of political misinformation familiar to the English-speaking public, transplanted from hyperpartisan American news sites and social media. Relative to the liberal outlets on the platform, the conservative sphere appears to be more substantial in its

volume, reach, and singular ideology. This asymmetrical polarization means misinformation originating from right-wing, English-speaking media potentially gains wider traction, alongside stories relevant to Chinese Americans that are politicized according to hot-button issues particularly salient among the immigrant community. Stories like the Massalkhy case can take on origins, tropes, and a cast of characters specific to public discourse in China.

#### ICYMI: How WeChat became the primary news source in China

The content universe of WeChat is already inherently fertile ground for misinformation, because unlike other messaging apps and social media, the platform hosts a vast number of native content publishers vying for attention. While some of them—from individual influencers to traditional media—produce original content, many other WeChat outlets adopt the cheaper and faster model of repackaging and pirating content that already exists. At these outlets, a skeletal team of staff writers (often one person) scours the internet or WeChat itself for the most clickbaity bits of information, and then pieces them together or directly clones stories to share.

While local news is often championed as a bastion of democracy and source of trust in today's vortex of misinformation, locally oriented news outlets on WeChat contribute heavily to the amplification of misinformation. Many such outlets have emerged in an attempt to seize the thriving niche market as a major immigrant destination, promoting their usefulness by delivering practical information on where to shop and get services, how to prevent crime, and what events are happening locally. At the same time, these profit-driven local outlets have also become hotbeds for misinformation, especially as local policies such as sanctuary laws and marijuana legalization come under intense debate in the communities they target. Lack of credible local news, as in the Massalkhy story, creates a vacuum for misinformation to flourish.

To complicate matters, misinformation on WeChat travels in private networks, hidden from outside view or systematic analysis. The platform is mostly free of algorithmic and computational manipulation. Instead, chat groups, a mode of communication especially central to WeChat, play a pivotal role in the distribution of information. Among a sample of US-based WeChat users surveyed in the study, 79 percent said they read political news from chat groups.

Small groups with intimate ties such as family and close friends were most common, but 71 percent of users also reported belonging to groups larger than 100 people, where members may not know each other outside of WeChat. Local parents group, DIY hobby groups, and high school alumni groups can all become effective nodes in the propagation of political misinformation. As messaging apps like WeChat, Whatsapp, and Kakaotalk increasingly become venues for sharing and discussing news, this organic process of information distribution goes unregulated, falling prey to a set of psychological, social, and cultural drivers of misinformation.

The report offers several ways to combat WeChat's information problem, including understanding which issues define the attention and rally the emotions of WeChat audiences, and focusing counter-narratives around these areas. The challenge, of course, is constructing these counter-narratives from perspectives that are relevant to immigrant Chinese, and communicating them through accessible channels—whether in mainstream local news or on WeChat itself.

Nothing about WeChat's information problem lends itself to obvious or easy solutions. But understanding what the problem entails is a critical first step. At the very least, for journalists, government agencies, and community organizations, WeChat can serve as a venue for accessing and engaging with the individuals and communities often overlooked in mainstream discourse and outreach.

## LAWFARE

CHINA

## Unpacking TikTok, Mobile Apps and National Security Risks

By **Justin Sherman** Thursday, April 2, 2020, 10:06 AM**DayZero: Cybersecurity Law and Policy**

On March 12, Sen. Josh Hawley introduced a bill into the Senate to ban the downloading and use of TikTok, the Chinese social media app, on federal government devices. Hawley's bill carves out exceptions for such activities as law enforcement investigations and intelligence collection, but holds that

---

no employee of the United States, officer of the United States, Member of Congress, congressional employee, or officer or employee of a government corporation may download or use TikTok or any successor application developed by ByteDance or any entity owned by ByteDance on any device issued by the United States or a government corporation.

---

Currently, the Transportation Security Administration and the U.S. Army have also banned the app on employee phones.

But what's Hawley's objection to an app used widely for dance challenges and lip-syncing?

The narrative goes something like this: TikTok is a company incorporated within China; the Chinese government pervasively surveils within its borders and can get access to company-held data on a whim; thus, TikTok's potential collection of information on U.S. citizens is a security risk. Yet also thrown into the discussion are other allegations—TikTok removes political content at Beijing's behest, for example. The failure to decouple these risks only muddies the waters and makes it harder for policymakers and the general public to understand the threats at play.

In reality, TikTok carries five clear risks. Two pertain directly to national security, and three perhaps relate to it, though not as clearly. All have been conflated or blurred together, at one point or another, by pundits and others commenting on TikTok's risks. Policymakers and analysts would be wise to make meaningful distinctions among these risks and provide more nuance and detail around each specific threat.

Policymakers may clearly have many different interpretations of each of these risks' likelihood and severity. There's also no clear answer on what policymakers should do about the app. And, in reality, the problems raised by TikTok are much bigger than the app itself—representative of larger questions that must be answered around U.S. data security policy.

**Risk 1: TikTok Collecting Data on U.S. Government Employees**

The first risk posed by TikTok is the collection of data on U.S. government employees (including those working as contractors). These are people who either have security clearances or could have clearances in the future or at the very least perform tasks that, if not classified, may still be considered sensitive in an unofficial sense. Data collection on these individuals and their activities can therefore reveal important national security information or be used in a coercive manner (that is, blackmail) to target those individuals.

There are two considerations with this type of data collection risk: the kinds of data that are being or might be collected; and Beijing's ability to access that data.

The data collected by TikTok, at least on the surface, might seem relatively benign; after all, the app is a social media platform for sharing videos. Even if a U.S. federal government employee has the app, one could argue, that doesn't mean they're sharing any videos that somehow compromise their personal or professional activities. And they can use the app without jeopardizing sensitive information.

But where the risk gets more complicated is the reality that most phone apps collect *far* more information than what the average user would suspect they are handing over to the app. (This might even go beyond that single firm: Charlie Warzel at the New York Times, for example, has a great explanation of how “just by downloading an app, you’re potentially exposing sensitive data to dozens of technology companies, ad networks, data brokers and aggregators.”)

TikTok is reasonably upfront about the high volume of data it collects: its privacy policy for U.S. residents states,

---

We automatically collect certain information from you when you use the Platform, including internet or other network activity information such as your IP address, geolocation-related data (as described below), unique device identifiers, browsing and search history (including content you have viewed in the Platform), and Cookies (as defined below).

---

It notes further that “[w]e also collect information you share with us from third-party social network providers, and technical and behavioral information about your use of the Platform,” such as, potentially, contact lists on other social media services. This type of data collection can especially implicate national security—geolocations or internet search histories of federal employees can reveal quite sensitive information, such as the location of secret government facilities, details about events relevant to the government about which those employees are seeking publicly available information, and personal activities that could potentially be used to build files for blackmail.

TikTok is hardly alone in this kind of collection—go read the privacy policy of most major social media platforms and you’ll find similar if not more encompassing language.

But TikTok has a unique challenge: There are real questions about who beyond TikTok might have access to the collected data. This risk likely exists whether the app is downloaded on a government-owned device used by an employee, or on a personal device used by the employee.

So can the Chinese government compel the company to turn over data?

As Sam Sacks recently wrote, “Nothing is black and white, particularly when it comes to government access to data. Ultimately the Chinese government can compel companies to turn over their data, but this does not always happen.” In some cases, companies can and do push back against government requests, as they “have their own commercial interests to protect.” There are real risks of government access to data, and this does happen, but it’s not as clear-cut in practice as many might assume.

There are also real fears among some U.S. policymakers that data from a company like TikTok could be added into an enormous dataset Beijing continues to compile from incidents such as the Equifax breach and the hack of the Office of Personnel Management. The product of such data-hoarding, in this view, is a massive dossier on U.S. persons that the Chinese government can use for intelligence and security purposes—consisting of everything from communications to credit scores to travel histories.

It is clear that there are national security risks with TikTok’s collection of data on U.S. federal government employees. The question for policymakers comes down to one’s perceived likelihood of the risk, the severity of the risk and what to do about it.

## **Risk 2: TikTok Collecting Data on U.S. Persons Not Employed by the Government**



Second is the risk that TikTok collects data on U.S. persons *not* working for the federal government in ways that still potentially impact national security. The considerations here mirror those of TikTok's data collection on federal employees.

Yes, the link between data collection on federal personnel and national security threats (that is, counterintelligence operations) is clearer. One could imagine how a clearance-holding federal employee with an embarrassing internet search history could be blackmailed, or how the GPS movements of a clearance-holding federal employee would likewise be valuable to a foreign intelligence service.

Here, one danger is merely the *potential* for U.S. persons not currently employed by the government to have clearances or perform other sensitive government tasks in the future. There could also be the potential for collection to target individuals in the private sector working on proprietary and national security-related technologies.

The collection of this data could therefore have potential impacts on U.S. national security in ways that may give policymakers reason to consider wider action against TikTok. Policymakers' decisions to take wider action would depend on where and how they interpret specific risk cases. For instance, one could perceive a risk of higher severity for an engineer working on tightly held and cutting-edge satellite imaging technology than for your average person.

It is also possible, in a Cambridge Analytica-style fashion, that such information could be used to develop profiles on Americans in ways that lend themselves to enhanced microtargeting on social media and other platforms.

In terms of the kinds of data being collected, TikTok, like most social media companies, very likely just collects the same types of information on all of its users. So collection on federal employees is likely the same as for non-federal employees.

The same goes for the legal authorities governing Beijing's access to TikTok data: The risk remains largely similar to the risk for federal employees. Maybe Beijing has greater incentive to request access to certain kinds of information when data is on U.S. government employees than when it's not. That said, this may also not be the case. TikTok might collect information from private citizens that exposes security-sensitive corporate activities. And what about the microtargeting—could Beijing have an incentive to access the data if it lent itself to, say, pushing advertisements for Chinese Communist Party (CCP)-preferred candidates in a U.S. election?

### **Risk 3: TikTok Censoring Information *in* China at Beijing's Behest**

The third risk pertains to Beijing ordering, forcing, coercing or otherwise leading TikTok to remove information on the platform *in* China. (This could include TikTok preemptively self-censoring content out of concern over possible retribution from the Chinese government.) This is not directly a U.S. national security issue, but it merits attention because of the way it has been roped into conversations about TikTok's risks.

The Washington Post reported last fall, for example, on the ways in which certain content that the CCP dislikes—such as information on the Hong Kong pro-democracy protests—was strangely absent from TikTok.

Subsequently, amid this and other reports in the media about alleged TikTok censorship, Sens. Chuck Schumer and Tom Cotton sent a letter to the acting director of national intelligence, stating that

---

TikTok reportedly censors materials deemed politically sensitive to the Chinese Communist Party, including content related to the recent Hong Kong protests, as well as references to Tiananmen Square, Tibetan and Taiwanese independence, and the treatment of Uighurs. The platform is also a potential target of foreign influence campaigns like those carried out during the 2016 election on U.S.-based social media platforms.

---

In addition to raising concerns about the aforementioned risks of data collection on U.S. persons, the senators requested the intelligence community to investigate allegations that TikTok engages in political censorship at the direction of the Chinese government.

But many of the conversations about this political censorship do not distinguish between TikTok removing content within China's borders and TikTok removing that same content *globally*. This might seem like a trivial distinction, but it's not. In the former case, content would be removed (or perhaps algorithmically downplayed) for those accessing the mobile application from within China's geographic borders. Thus, this "geoblocking" would affect those physically located within China. If TikTok was censoring content globally, by contrast, once flagged, the offending content would be deleted from anyone's and everyone's TikTok feed.

The former issue of geoblocked content within China (that is, this third risk) is mostly a domestic issue in China. It is an issue of free speech and human rights, certainly, but it doesn't directly impact U.S. national security in the ways that it potentially would if content was removed globally at one government's behest.

#### **Risk 4: TikTok Censoring Information *Beyond* China at Beijing's Behest**

So what is the national security risk if TikTok did not limit its content takedowns to within China?

There is no clear evidence that Beijing has directly told TikTok to remove content around the world. TikTok's parent company responded to the Post investigation from last September by asserting that the platform's content moderation policies in the U.S. are handled by an American team and are not influenced by the Chinese government. But policymakers have expressed worries, in light of such observations as the aforementioned lack of Hong Kong protest videos on the platform, that TikTok is in fact (at Beijing's direct behest or not) removing those kinds of content globally. This risk centers on whether and how TikTok could remove, for anyone using the app, a video critical of the CCP or that talks about concentration camps in Xinjiang, for example. In this case, nobody in the world would be able to access the content on TikTok once removed; the takedowns would be global.

Again, the national security risks here are not as direct as with data collection. Yet there are genuine concerns about the Chinese government exporting its censorship through platforms like TikTok. The worry is that Beijing compels high-demand Chinese-incorporated internet platforms to remove content worldwide. Beijing's internet censorship practices, otherwise confined within Chinese borders, could hypothetically spread through this tactic.

This certainly presents risks to democracy and free speech. More teenagers in the United States are using TikTok to share political content. Political censorship is therefore not an insignificant issue. The takedown of certain critical videos could, for one thing, subtly influence platform users' views of Beijing. And there are real concerns, especially in light of such investigations as the Washington Post's report last November that "former U.S. [TikTok] employees said moderators based in Beijing had the final call on whether flagged videos were approved."

#### **Risk 5: Disinformation on TikTok**

Fifth and finally, there is concern among U.S. policymakers about potential disinformation on TikTok. Tons of U.S. teenagers use TikTok and consume political content through the application, so there is a concern that the users could amplify disinformation on the platform. This incursion of disinformation into U.S. public discourse is no doubt corrosive to the democratic process. Yet this is not a national security risk that is necessarily specific to TikTok.

Virtually every internet platform deals with disinformation; thus, that TikTok is Chinese incorporated in and of itself has nothing to do with it. But U.S. officials have expressed concern about the potential for disinformation on the platform. (These concerns aren't unfounded: See the false information that circulated on TikTok about the coronavirus.) One could certainly make the argument that the platform *responds* to disinformation—in light of political censorship concerns—might impact U.S. interests in undesirable ways. But the presence of disinformation on the platform is in many ways a distinct risk from the preceding four.

### Looking Beyond TikTok

These questions, and the policy responses to them, have implications well beyond TikTok. And they have become increasingly urgent, as these questions about mobile apps, data collection and national security grow more frequent and as more bills like Sen. Hawley's are introduced into Congress.

The issues here are complex. If the view is that any data collected by a Chinese internet company is a national security risk—because of Beijing's purportedly easy access to that data, and the ways it could be potentially combined with other datasets (for example, from the Office of Personnel Management hack)—then many applications fall into the bucket of risk. The widely used application WeChat, for example, could certainly be banned under that view.

But the problem is even more complicated. After all, China isn't the only country about which policymakers are or might be concerned.

Last fall, for example, Sen. Schumer sent a letter to the FBI requesting they investigate the security risks of Russian mobile apps. The letter cited "the legal mechanisms available to the Government of Russia that permit access to data" as reason for concern.

If Russian-made apps are also considered an unacceptable data collection risk for U.S. government employees, then how should the U.S. approach and maintain a list of countries that fit into that category?

The United States isn't alone in confronting these questions. And these aren't entirely novel problems. India's military, for example, has prohibited personnel from installing Chinese social platform WeChat due to security concerns. The Australian armed forces have also banned WeChat. The Pentagon banned the military's use of geolocating fitness trackers in August 2018 after live GPS data was found on the public internet: Researchers were able to track the location of troops on military bases and spies in safe houses.

This all raises challenging questions about where to draw the line: Is an app that, hypothetically, makes custom emojis and collects only a user's phone number more of a security risk than one that provides the weather based on current geographic location?

Meanwhile, it's worth remembering that apps are only one potential way for a government to get access to information on individuals: The highly unregulated data brokerage industry, which sells incredibly intimate information on all kinds of people to whomever is buying, could easily be exploited by foreign governments. Governments could buy information from brokerage firms and ascertain sensitive activities of, say, a U.S. federal employee with a security clearance or a non-government employee who happens to be running for Congress in the next election.

Policymakers might consider crafting legislation based on the people *on whom* data is being collected—that is, focusing on data collection of government employees, which presents immediate national security concerns, rather than about data collection on all Americans. Targeted bans on app downloads on government phones could be a solution, as Sen. Hawley proposed in his bill.

More broadly, one could imagine developing a framework of criteria to answer these questions that will arise again and again. This framework would function in the same way as would objective criteria by which to routinely evaluate other elements of digital supply chain security, another much-needed national security tool. For instance, the Committee on Foreign Investment in the United States could explicitly make data privacy and security a more central component of its investment screening process. Agencies like the Cybersecurity and Infrastructure Security Agency could lead an interagency process to determine government recommendations for baseline corporate cybersecurity standards writ large that, like with encryption, could be used subsequently by policymakers to evaluate protections implemented by firms like TikTok. Federal departments such as the Department of Defense could develop clear and at least semipublic frameworks by which they decide to prohibit employee use of mobile apps.

Again, though, even this route leads to more questions. What about American- or European-incorporated companies that collect disturbing amounts of sensitive personal information on U.S. government employees? Do they not fit these categories too? Policymakers need to consider these questions.

Policymakers also must consider whether these mobile app and data security decisions should depend less on the *kinds* of data collected and *on whom*, and more on the *legal structures in the countries* in which these companies are incorporated. Beijing, for instance, engages in unchecked surveillance. While the actual practice of Beijing getting data from private companies isn't as straightforward as some might imagine, it's certainly far easier than the U.S. government getting access to American company data. For some policymakers, that difference might be the end-all-be-all to allowing Chinese apps on U.S. government employee phones—forget about details like the kinds of data in question.

And this is all without even getting into the risks of content censorship in China, content censorship globally and disinformation—which pertain more to content management on an app like TikTok than they do directly to national security. This isn't to say (as clarified above) that *no* national security linkages exist or could exist to, say, TikTok removing political content worldwide at Beijing's behest. But, rather, I suggest that the links to a U.S. national security threat from censorship and disinformation are generally not as pronounced as those from the collection of geolocation data on a U.S. federal employee with an active security clearance, for example.

This isn't just a laundry list of academic questions.

Some observers might find a TikTok ban to be a relatively narrowly targeted and sensible policy response to a perceived threat of Chinese state access to data. But the reality is that decisions in this sphere of data security and U.S. data protection are not made in a vacuum. They have broader implications—first-order, second-order, and even third- or fourth-order effects. Many countries develop mobile apps, and many of them could be perceived as posing security risks in various ways. They, too, must be considered as part of the picture. A cohesive and repeatable strategy for making these decisions is far superior—from economic, national security and rights-protection perspectives—than a whack-a-mole-style approach that might yield a sensible policy but not with a sensible process.

All the while, it is important not to blur and conflate these risks. The national security risks of mobile apps made and managed by foreign-incorporated companies may take different forms and may differ in likelihood, severity and desired response. Blurring the lines makes it hard to develop targeted policies that address actual risks in ways that fully consider costs and benefits.

Many countries worldwide are grappling with these same questions. Many governments, like Washington, are also considering if, where and how they want to “decouple” elements of their technology systems from other countries. Here, Washington should tread very carefully because these broader and global implications demand much more thought.

**Topics:** China, Cybersecurity

**Tags:** China, Committee on Foreign Investment (CFIUS), data privacy, great power politics

---

Justin Sherman (@jshermcyber) is a fellow at the Atlantic Council's Cyber Statecraft Initiative. He also works with the Tech, Law, & Security Program at American University Washington College of Law and with Lawfare's Trustworthy Hardware and Software Working Group. He was previously a cybersecurity policy fellow at New America and a fellow at Duke Law School's Center on Law & Technology.

 @jshermcyber





The New York Times | <https://nyti.ms/3ISDHLZ>

# Forget TikTok. China's Powerhouse App Is WeChat, and Its Power Is Sweeping.

A vital connection for the Chinese diaspora, the app has also become a global conduit of Chinese state propaganda, surveillance and intimidation. The United States has proposed banning it.



By **Paul Mozur**

Sept. 4, 2020

Just after the 2016 presidential election in the United States, Joanne Li realized the app that connected her to fellow Chinese immigrants had disconnected her from reality.

Everything she saw on the Chinese app, WeChat, indicated Donald J. Trump was an admired leader and impressive businessman. She believed it was the unquestioned consensus on the newly elected American president. “But then I started talking to some foreigners about him, non-Chinese,” she said. “I was totally confused.”

She began to read more widely, and Ms. Li, who lived in Toronto at the time, increasingly found WeChat filled with gossip, conspiracy theories and outright lies. One article claimed Prime Minister Justin Trudeau of Canada planned to legalize hard drugs. Another rumor purported that Canada had begun selling marijuana in grocery stores. A post from a news account in Shanghai warned Chinese people to take care lest they accidentally bring the drug back from Canada and get arrested.

She also questioned what was being said about China. When a top Huawei executive was arrested in Canada in 2018, articles from foreign news media were quickly censored on WeChat. Her Chinese friends both inside and outside China began to say that Canada had no justice, which contradicted her own experience. “All of a sudden I discovered talking to others about the issue didn’t make sense,” Ms. Li said. “It felt like if I only watched Chinese media, all of my thoughts would be different.”

Ms. Li had little choice but to take the bad with the good. Built to be everything for everyone, WeChat is indispensable.

For most Chinese people in China, WeChat is a sort of all-in-one app: a way to swap stories, talk to old classmates, pay bills, coordinate with co-workers, post envy-inducing vacation photos, buy stuff and get news. For the millions of members of China’s diaspora, it is the bridge that links them to the trappings of home, from family chatter to food photos.

Woven through it all is the ever more muscular surveillance and propaganda of the Chinese Communist Party. As WeChat has become ubiquitous, it has become a powerful tool of social control, a way for Chinese authorities to guide and police what people say, whom they talk to and what they read.

It has even extended Beijing's reach beyond its borders. When secret police issue threats abroad, they often do so on WeChat. When military researchers working undercover in the United States needed to talk to China's embassies, they used WeChat, according to court documents. The party coordinates via WeChat with members studying overseas.

As a cornerstone of China's surveillance state, WeChat is now considered a national security threat in the United States. The Trump administration has proposed banning WeChat outright, along with the Chinese short video app TikTok. Overnight, two of China's biggest internet innovations became a new front in the sprawling tech standoff between China and the United States.

While the two apps are lumped in the same category by the Trump administration, they represent two distinct approaches to the Great Firewall that blocks Chinese access to foreign websites.

The hipper, better-known TikTok was designed for the wild world outside of China's cloistering censorship; it exists only beyond China's borders. By hiving off an independent app to win over global users, TikTok's owner, ByteDance, created the best bet any Chinese start-up has had to compete with the internet giants in the West. The separation of TikTok from its cousin apps in China, along with deep popularity, has fed corporate campaigns in the United States to save it, even as Beijing potentially upended any deals by labeling its core technology a national security priority.

Though WeChat has different rules for users inside and outside of China, it remains a single, unified social network spanning China's Great Firewall. In that sense, it has helped bring Chinese censorship to the world. A ban would cut dead millions of conversations between family and friends, a reason one group has filed a lawsuit to block the Trump administration's efforts. It would also be an easy victory for American policymakers seeking to push back against China's techno-authoritarian overreach.



Joanne Li. After she shared a news article on WeChat, four police officers showed up at her family's apartment, carrying guns and riot shields. The New York Times

Ms. Li felt the whipcrack of China's internet controls firsthand when she returned to China in 2018 to take a real estate job. After her experience overseas, she sought to balance her news diet with groups that shared articles on world events. As the coronavirus spread in early 2020 and China's relations with countries around the world strained, she posted an article on WeChat from the U.S. government-run Radio Free Asia about the deterioration of Chinese-Canadian diplomacy, a piece that would have been censored.

The next day, four police officers showed up at her family's apartment. They carried guns and riot shields.

"My mother was terrified," she said. "She turned white when she saw them."

The police officers took Ms. Li, along with her phone and computer, to the local police station. She said they manacled her legs to a restraining device known as a tiger chair for questioning. They asked repeatedly about the article and her WeChat contacts overseas before locking her in a barred cell for the night.

Twice she was released, only to be dragged back to the station for fresh interrogation sessions. Ms. Li said an officer even insisted China had freedom of speech protections as he questioned her over what she had said online. "I didn't say anything," she said. "I just thought, what is your freedom of speech? Is it the freedom to drag me down to the police station and keep me night after sleepless night interrogating me?"

Finally, the police forced her to write out a confession and vow of support for China, then let her go.

### 'The walls are getting higher'

WeChat started out as a simple copycat. Its parent, the Chinese internet giant Tencent, had built an enormous user base on a chat app designed for personal computers. But a new generation of mobile chat apps threatened to upset its hold over the way young Chinese talked to one another.

The visionary Tencent engineer Allen Zhang fired off a message to the company founder, Pony Ma, concerned that they weren't keeping up. The missive led to a new mandate, and Mr. Zhang fashioned a digital Swiss Army knife that became a necessity for daily life in China. WeChat piggybacked on the popularity of the other online platforms run by Tencent, combining payments, e-commerce and social media into a single service.

It became a hit, eventually eclipsing the apps that inspired WeChat. And Tencent, which made billions in profits from the online games piped into its disparate platforms, now had a way to make money off nearly every aspect of a person's digital identity — by serving ads, selling stuff, processing payments and facilitating services like food delivery.

The Beijing offices of Tencent, the parent company of WeChat. Wu Hong/EPA

The tech world inside and outside of China marveled. Tencent rival Alibaba scrambled to come up with its own product to compete. Silicon Valley studied the ways it mixed services and followed its cues.

Built for China's closed world of internet services, WeChat's only failure came outside the Great Firewall. Tencent made a big marketing push overseas, even hiring the soccer player Lionel Messi as a spokesman in some markets. For non-China users, it created a separate set of rules. International accounts would not face direct censorship and data would be stored on servers overseas.

But WeChat didn't have the same appeal without the many services available only in China. It looked more prosaic outside the country, like any other chat app. The main overseas users, in the end, would be the Chinese diaspora.

Tencent did not respond to a request for comment.

Over time, the distinctions between the Chinese and international app have mattered less. Chinese people who create accounts within China, but then leave, carry with them a censored and monitored account. If international users chat with users inside China, their posts can be censored.

For news and gossip, most comes from WeChat users inside China and spreads out to the world. Whereas most social networks have myriad filter bubbles that reinforce different biases, WeChat is dominated by one super-filter bubble, and it hews closely to the official propaganda narratives.

"The filter bubbles on WeChat have nothing to do with algorithms — they come from China's closed internet ecosystem and censorship. That makes them worse than other social media," said Fang Kecheng, a professor in the School of Journalism and Communications at the Chinese University of Hong Kong.

Mr. Fang first noticed the limitations of WeChat in 2018 as a graduate student at the University of Pennsylvania, teaching an online course in media literacy to younger Chinese.

Soft-spoken and steeped in the media echo chambers of the United States and China, Mr. Fang expected to reach mostly curious Chinese inside China. An unexpected group dialed into the classes: Chinese immigrants and expatriates living in the United States, Canada and elsewhere.

"It seemed obvious. Because they were all outside China, it should be easy for them to gain an understanding of foreign media. In their day-to-day life they would see it and read it," Mr. Fang said. "I realized it wasn't the case. They were outside of China, but their media environment was still entirely inside China, their channel for information was all from public accounts on WeChat."

Mr. Fang's six-week online courses were inspired by a WeChat account he ran called News Lab that sought to teach readers about journalism. With his courses, he assigned articles from media like Reuters along with work sheets that taught students to analyze the pieces — pushing them to draw distinctions between pundit commentary and primary sourcing.

During one course in 2019, he focused on the fire at Notre-Dame cathedral in Paris, which inspired many conspiracy theories on WeChat. One professor at the prestigious Tsinghua University reposted an article alleging that Muslims were behind the fire, which was untrue.

The classes were a big draw. In 2018, Mr. Fang attracted 500 students. The next year he got 1,300. In 2020, a year of coronavirus rumors and censorship, Tencent took down his News Lab account. He decided it was not safe to teach the class on another platform given the more “hostile” climate toward foreign media.

Still, he said that blocking WeChat would be unlikely to help much, as users could easily switch to other Chinese apps filled with propaganda and rumors. A better idea would be to create rules that force social media companies like Tencent to be more transparent, he said.

Creating such internet blocks, he said, rarely improved the quality of information.

“Information is like water. Water quality can be improved, but without any flow, water easily grows fetid,” he said.

In a class in 2019, he warned broadly about barriers to information flow.

“Now, the walls are getting higher and higher. The ability to see the outside has become ever harder,” he said. “Not just in China, but in much of the world.”

### ‘What it’s like to lose contact’

When Ferkat Jawdat's mother disappeared into China's sprawling system of re-education camps to indoctrinate Uighurs, his WeChat became a kind of memorial.

The app might have been used as evidence against her. But he, like many Uighurs, found himself opening WeChat again and again. It contained years of photos and conversations with his mother. It also held a remote hope he clung to, that one day she would again reach out.

When against all odds she did, the secret police followed.

If propaganda and censorship have found their way to WeChat users overseas, so too has China's government.

For ethnic minority Uighurs, who have been targeted by draconian digital controls at home in China, the chat app has become a conduit for threats from Chinese security forces. In court documents, the Federal Bureau of Investigation said China's embassies communicated on WeChat with military researchers who had entered the United States to steal scientific research. The Chinese Communist Party has used it to keep up ties and organize overseas members, including foreign-exchange students.

Not all uses are nefarious. During the pandemic, local governments used the app to update residents traveling and living abroad about the virus. China's embassies use it to issue travel warnings.



While the Chinese government could use any chat app, WeChat has advantages. Police know well its surveillance capabilities. Within China most accounts are linked to the real identity of users.

Mr. Jawdat's mother, sick and worn, was released from the camps in the summer of 2019. Chinese police gave her a phone and signed her into WeChat. At the sound of his mother's voice Mr. Jawdat fought back a flood of emotions. He hadn't been sure if she was even alive. Despite the relief, he noticed something was off. She offered stilted words of praise for the Chinese Communist Party.

Then the police reached out to him. They approached him with an anonymous friend request over WeChat. When he accepted, a man introduced himself as a high-ranking officer in China's security forces in the Xinjiang region, the epicenter of re-education camps. The man had a proposal. If Mr. Jawdat, an American citizen and Uighur activist, would quiet his attempts to raise awareness about the camps, then his mother might be given a passport and allowed to join her family in the United States.

"It was a kind of threat," he said. "I stayed quiet for two or three weeks, just to see what he did."

It all came to nothing. After turning down a media interview and skipping a speaking event, Mr. Jawdat grew impatient and confronted the man. "He started threatening me, saying, 'You're only one person going against the superpower. Compared to China, you are nothing.'"

The experience gave Mr. Jawdat little tolerance for the app that made the threats possible, even if it had been his only line to his mother. He said he knew two other Uighur Americans who had similar experiences. Accounts from others point to similar occurrences around the world.

"I don't know if it's karma or justice served, for the Chinese people to also feel the pain of what it's like to lose contact with your family members," Mr. Jawdat said of the proposed ban by the Trump administration. "There are many Chinese officials who have their kids in the U.S. WeChat must be one of the tools they use to keep in contact. If they feel this pain, maybe they can relate better to the Uighurs."

## ‘Then you are alone’

Ms. Li was late to the WeChat party. Away in Toronto when it exploded in popularity, she joined only in 2013, after her sister’s repeated urging.

It opened up a new world for her. Not in China, but in Canada.

She found people nearby similar to her. Many of her Chinese friends were on it. They found restaurants nearly as good as those at home and explored the city together. One public account set up by a Chinese immigrant organized activities. It kindled more than a few romances. “It was incredibly fun to be on WeChat,” she recalled.

Now the app reminds her of jail. During questioning, police told her that a surveillance system, which they called Skynet, flagged the link she shared. Sharing a name with the A.I. from the Terminator movies, Skynet is a real-life techno-policing system, one of several Beijing has spent billions to create.

The surveillance push has supported a fast-growing force of internet police. The group prowls services like WeChat for posts deemed politically sensitive, anything from a link to a joke mocking leader Xi Jinping. To handle WeChat’s hundreds of millions of users and their conversations, software analyzes keywords, links and images to generate leads.

Although Ms. Li registered her account in Canada, she fell under Chinese rules when she was back in China. Even outside of China, traffic on WeChat appears to be feeding these automated systems of control. A report from Citizen Lab, a University of Toronto-based research group, showed that Tencent surveilled images and files sent by WeChat users outside of China to help train its censorship algorithms within China. In effect, even when overseas users of WeChat are not being censored, the app learns from them how to better censor.

Wary of falling into automated traps, Ms. Li now writes with typos. Instead of referring directly to police, she uses a pun she invented, calling them golden forks. She no longer shares links from news sites outside of WeChat and holds back her inclination to talk politics.

Still, to be free she would have to delete WeChat, and she can’t do that. As the coronavirus crisis struck China, her family used it to coordinate food orders during lockdowns. She also needs a local government health code featured on the app to use public transport or enter stores.

“I want to switch to other chat apps, but there’s no way,” she said.

“If there were a real alternative I would change, but WeChat is terrible because there is no alternative. It’s too closely tied to life. For shopping, paying, for work, you have to use it,” she said. “If you jump to another app, then you are alone.”

Lin Qiqing contributed research.

Paul Mozur is a technology correspondent focused on the intersection of technology and geopolitics in Asia. He has been twice named a Pulitzer Prize finalist. @paulmozur

A version of this article appears in print on Sept. 6, 2020, Section BU, Page 1 of the New York edition with the headline: WeChat. WeThink. WeControl.

**Christopher Wray**

Director

Federal Bureau of Investigation

---

Hudson Institute, Video Event: China's Attempt to Influence U.S. Institutions  
Washington, D.C.

*July 7, 2020*

# **The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States**

*Remarks as delivered.*

Good morning. I realize it's challenging, particularly under the current circumstances, to put on an event like this, so I'm grateful to the Hudson Institute for hosting us today.

The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security—and by extension, to our national security.

As National Security Advisor O'Brien said in his recent remarks (<https://www.whitehouse.gov/briefings-statements/chinese-communist-partys-ideology-global-ambitions/>), we cannot close our eyes and ears to what China is doing—and today, in light of the importance of this threat, I will provide more detail on the Chinese threat than the FBI has ever presented in an open forum. This threat is so significant that the attorney general and secretary of state will

also be addressing a lot of these issues in the next few weeks. But if you think these issues are just an intelligence issue, or a government problem, or a nuisance largely just for big corporations who can take care of themselves—you could not be more wrong.



(<https://www.fbi.gov/image-repository/wray-hudson-070720e.jpg>)

FBI Director Christopher Wray discusses the threat China poses to U.S. economic and national security during a July 7, 2020 video event at the Hudson Institute in Washington, D.C.

It's the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history.

If you are an American adult, it is more likely than not that China has stolen your personal data.

In 2017, the Chinese military conspired to hack Equifax and made off with the sensitive personal information of 150 million Americans—we're talking nearly half of the American population and most American adults—and as I'll discuss in a few moments, this was hardly a standalone incident.

Our data isn't the only thing at stake here—so are our health, our livelihoods, and our security.

We've now reached the point where the FBI is opening a new China-related counterintelligence case about every 10 hours. Of the nearly 5,000 active FBI counterintelligence cases currently underway across the country, almost half are related to China. And at this very moment, China is working to compromise American health care organizations, pharmaceutical companies, and academic institutions conducting essential COVID-19 research.

But before I go on, let me be clear: This is not about the Chinese people, and it's certainly not about Chinese Americans. Every year, the United States welcomes more than 100,000 Chinese students and researchers into this country. For generations, people have journeyed from China to the United States to secure the blessings of liberty for themselves and their families—and our society is better for their contributions. So, when I speak of the threat from China, I mean the government of China and the Chinese Communist Party.

## **The Chinese Regime and the Scope of Its Ambitions**

To understand this threat and how we must act to respond to it, the American people should remember three things.

First: We need to be clear-eyed about the scope of the Chinese government's ambition. China—the Chinese Communist Party—believes it is in a generational fight to surpass our country in economic and technological leadership.



That is sobering enough. But it's waging this fight not through legitimate innovation, not through fair and lawful competition, and not by giving their citizens the freedom of thought and speech and creativity that we treasure here in the United States. Instead, China is engaged in a whole-of-state effort to become the world's only superpower by any means necessary.

## **A Diverse and Multi-Layered Approach**

The second thing the American people need to understand is that China uses a diverse range of sophisticated techniques—everything from cyber intrusions to corrupting trusted insiders. They've even engaged in outright physical theft. And they've pioneered an expansive approach to stealing innovation through a wide range of actors—including not just Chinese intelligence services but state-owned enterprises, ostensibly private companies, certain kinds of graduate students and researchers, and a whole variety of other actors working on their behalf.

### **Economic Espionage**

To achieve its goals and surpass America, China recognizes it needs to make leaps in cutting-edge technologies. But the sad fact is that instead of engaging in the hard slog of innovation, China often steals American intellectual property and then uses it to compete against the very American companies it victimized—in effect, cheating twice over. They're targeting research on everything from military equipment to wind turbines to rice and corn seeds.

Through its talent recruitment programs, like the so-called Thousand Talents Program, the Chinese government tries to entice scientists to secretly bring our knowledge and innovation back to China—even if that means stealing proprietary information or violating our export controls and conflict-of-interest rules.

Take the case of scientist Hongjin Tan, for example, a Chinese national and American lawful permanent resident. He applied to China's Thousand Talents Program and stole more than \$1 billion—that's with a "b"—worth of trade secrets from his former employer, an Oklahoma-based petroleum company, and got caught. A few months ago, he was convicted and sent to prison.

Or there's the case of Shan Shi, a Texas-based scientist, also sentenced to prison earlier this year. Shi stole trade secrets regarding syntactic foam, an important naval technology used in submarines. Shi, too, had applied to China's Thousand Talents Program, and specifically pledged to "digest" and "absorb" the relevant technology in the United States. He did this on behalf of Chinese state-owned enterprises, which ultimately planned to put the American company out of business and take over the market.

In one of the more galling and egregious aspects of the scheme, the conspirators actually patented in China the very manufacturing process they'd stolen, and then offered their victim American company a joint venture using its own stolen technology. We're talking about an American company that spent years and millions of dollars developing that technology, and China couldn't replicate it—so, instead, it paid to have it stolen.

And just two weeks ago, Hao Zhang was convicted of economic espionage, theft of trade secrets, and conspiracy for stealing proprietary information about wireless devices from two U.S. companies. One of those companies had spent over 20 years developing the technology Zhang stole.

These cases were among more than a thousand investigations the FBI has into China's actual and attempted theft of American technology—which is to say nothing of over a thousand more ongoing counterintelligence investigations of other kinds related to China. We're conducting these kinds of investigations in all 56 of our field offices. And over the past decade, we've seen economic espionage cases with a link to China increase by approximately 1,300 percent.

The stakes could not be higher, and the potential economic harm to American businesses and the economy as a whole almost defies calculation.

## **Clandestine Efforts**

As National Security Advisor O'Brien discussed in his June remarks, the Chinese government is also making liberal use of hacking to steal our corporate and personal data—and they're using both military and non-state hackers to do it. The

Equifax intrusion I mentioned just a few moments ago, which led to the indictment of Chinese military personnel, was hardly the only time China stole the sensitive personal information of huge numbers of the American public.

For example, did any of you have health insurance through Anthem or one of its associated insurers? In 2015, China's hackers stole the personal data of 80 million of that company's current and former customers.

Or maybe you're a federal employee—or you used to be one, or you applied for a government job once, or a family member or roommate did. Well, in 2014, China's hackers stole more than 21 million records from OPM, the federal government's Office of Personnel Management.

Why are they doing this? First, China has made becoming an artificial intelligence world leader a priority, and these kinds of thefts feed right into China's development of artificial intelligence tools.

Compounding the threat, the data China stole is of obvious value as they attempt to identify people for secret intelligence gathering. On that front, China is using social media platforms—the same ones Americans use to stay connected or find jobs—to identify people with access to our government's sensitive information and then target those people to try to steal it.

Just to pick one example, a Chinese intelligence officer posing as a headhunter on a popular social media platform recently offered an American citizen a sizeable sum of money in exchange for so-called “consulting” services. That sounds benign enough until you realize those “consulting” services were related to sensitive information the American target had access to as a U.S. military intelligence specialist.

Now that particular tale has a happy ending: The American citizen did the right thing and reported the suspicious contact, and the FBI, working together with our armed forces, took it from there. I wish I could say that all such incidents ended that way.

## **Threats to Academia**

It's a troublingly similar story in academia.

Through talent recruitment programs like the Thousand Talents Program I mentioned just a few moments ago, China pays scientists at American universities to secretly bring our knowledge and innovation back to China—including valuable, federally funded research. To put it bluntly, this means American taxpayers are effectively footing the bill for China's own technological development. China then leverages its ill-gotten gains to undercut U.S. research institutions and companies, blunting our nation's advancement and costing American jobs. And we are seeing more and more of these cases.

In May alone, we arrested both Qing Wang, a former researcher with the Cleveland Clinic who worked on molecular medicine and the genetics of cardiovascular disease, and Simon Saw-Teong Ang, a University of Arkansas scientist doing research for NASA. Both of these guys were allegedly committing fraud by concealing their participation in Chinese talent recruitment programs while accepting millions of dollars in American federal grant funding.

That same month, former Emory University professor Xiao-Jiang Li pled guilty to filing a false tax return for failing to report the income he'd received through China's Thousand Talents Program. Our investigation found that while Li was researching Huntington's disease at Emory, he was also pocketing half a million unreported dollars from China.

In a similar vein, Charles Lieber, chair of Harvard's Department of Chemistry and Chemical Biology, was indicted just last month for making false statements to federal authorities about his Thousand Talents participation. The United States has alleged that Lieber concealed from both Harvard and the NIH his position as a strategic scientist at a Chinese university—and the fact that the Chinese government was paying him, through the Wuhan Institute of Technology, a \$50,000 monthly stipend, more than \$150,000 in living expenses, and more than \$1.5 million to establish a laboratory back in China.

## **Malign Foreign Influence**

There's more. Another tool China and the Chinese Communist Party use to

manipulate Americans is what we call malign foreign influence.

Now, traditional foreign influence is a normal, legal diplomatic activity typically conducted through diplomatic channels. But malign foreign influence efforts are subversive, undeclared, criminal, or coercive attempts to sway our government's policies, distort our country's public discourse, and undermine confidence in our democratic processes and values.

China is engaged in a highly sophisticated malign foreign influence campaign, and its methods include bribery, blackmail, and covert deals. Chinese diplomats also use both open, naked economic pressure and seemingly independent middlemen to push China's preferences on American officials.

Just take one all-too-common illustration: Let's say China gets wind that some American official is planning to travel to Taiwan—think a governor, a state senator, a member of Congress. China does not want that to happen, because that travel might appear to legitimize Taiwanese independence from China—and legitimizing Taiwan would, of course, be contrary to China's "One China" policy.

So what does China do? Well, China has leverage over the American official's constituents—American companies, academics, and members of the media all have legitimate and understandable reasons to want access to Chinese partners and markets. And because of the authoritarian nature of the Chinese Communist Party, China has immense power over those same partners and markets. So, China will sometimes start by trying to influence the American official overtly and directly. China might openly warn that if the American official goes ahead and takes that trip to Taiwan, China will take it out on a company from that official's home state by withholding the company's license to manufacture in China. That could be economically ruinous for the company, would directly pressure the American official to alter his travel plans, and the official would know that China was trying to influence him.

That would be bad enough. But the Chinese Communist Party often doesn't stop there; it can't stop there if it wants to stay in power—so it uses its leverage even more perniciously. If China's more direct, overt influence campaign doesn't do the trick, they sometimes turn to indirect, covert, deceptive influence efforts.



To continue with the illustration of the American official with travel plans that the Chinese Communist Party doesn't like, China will work relentlessly to identify the people closest to that official—the people that official trusts most. China will then work to influence those people to act on China's behalf as middlemen to influence the official. The co-opted middlemen may then whisper in the official's ear and try to sway the official's travel plans or public positions on Chinese policy. These intermediaries, of course, aren't telling the American official that they're Chinese Communist Party pawns—and worse still, some of these intermediaries may not even realize they're being used as pawns, because they, too, have been deceived.

Ultimately, China doesn't hesitate to use smoke, mirrors, and misdirection to influence Americans.

Similarly, China often pushes academics and journalists to self-censor if they want to travel into China. And we've seen the Chinese Communist Party pressure American media and sporting giants to ignore or suppress criticism of China's ambitions regarding Hong Kong or Taiwan. This kind of thing is happening over and over, across the United States.

And I will note that the pandemic has unfortunately not stopped any of this—in fact, we have heard from federal, state, and even local officials that Chinese diplomats are aggressively urging support for China's handling of the COVID-19 crisis. Yes, this is happening at both the federal and state levels. Not that long ago, we had a state senator who was recently even asked to introduce a resolution supporting China's response to the pandemic.

The punchline is this: All of these seemingly inconsequential pressures add up to a policymaking environment in which Americans find themselves held over a barrel by the Chinese Communist Party.

## **Threats to the Rule of Law**

All the while, China's government and Communist Party have brazenly violated well-settled norms and the rule of law.

Since 2014, Chinese General Secretary Xi Jinping has spearheaded a program known as “Fox Hunt.” Now, China describes Fox Hunt as some kind of international anti-corruption campaign—it is not. Instead, Fox Hunt is a sweeping bid by General Secretary Xi to target Chinese nationals whom he sees as threats and who live outside China, across the world. We’re talking about political rivals, dissidents, and critics seeking to expose China’s extensive human rights violations.

Hundreds of the Fox Hunt victims that they target live right here in the United States, and many are American citizens or green card holders. The Chinese government wants to force them to return to China, and China’s tactics to accomplish that are shocking. For example, when it couldn’t locate one Fox Hunt target, the Chinese government sent an emissary to visit the target’s family here in the United States. The message they said to pass on? The target had two options: return to China promptly, or commit suicide. And what happens when Fox Hunt targets refuse to return to China? In the past, their family members both here in the United States and in China have been threatened and coerced, and those back in China have even been arrested for leverage.

I’ll take this opportunity to note that if you believe the Chinese government is targeting you—that you’re a potential Fox Hunt victim—please reach out to your local FBI field office.

## **Exploiting Our Openness**

Understanding how a nation could engage in these tactics brings me to the third thing the American people need to remember: that China has a fundamentally different system than ours—and it’s doing all it can to exploit the openness of ours while taking advantage of its own closed system.

Many of the distinctions that mean a lot here in the United States are blurry or almost nonexistent in China—I’m talking about distinctions between the government and the Chinese Communist Party, between the civilian and military sectors, and between the state and the “private” sector.

For one thing, an awful lot of large Chinese businesses are state-owned enterprises—literally owned by the government, and thus the Party. And even if they aren't, China's laws allow its government to compel any Chinese company to provide any information it requests—including American citizens' data.

On top of that, Chinese companies of any real size are legally required to have Communist Party "cells" inside them to keep them in line. Even more alarmingly, Communist Party cells have reportedly been established in some American companies operating in China as a cost of doing business there.

These kinds of features should give U.S. companies pause when they consider working with Chinese corporations like Huawei—and should give all Americans pause, too, when relying on such a company's devices and networks. As the world's largest telecommunications equipment manufacturer, Huawei has broad access to much that American companies do in China. It's also been charged in the United States with racketeering conspiracy and has, as alleged in the indictment, repeatedly stolen intellectual property from U.S. companies, obstructed justice, and lied to the U.S. government and its commercial partners, including banks.

The allegations are clear: Huawei is a serial intellectual property thief, with a pattern and practice of disregarding both the rule of law and the rights of its victims. I have to tell you, it certainly caught my attention to read a recent article describing the words of Huawei's founder, Ren Zhengfei, about the company's mindset. At a Huawei research and development center, he reportedly told employees that to ensure the company's survival, they need to—and I quote—"surge forward, killing as you go, to blaze us a trail of blood." He's also reportedly told employees that Huawei has entered, to quote, "a state of war." I certainly hope he couldn't have meant that literally, but it's hardly an encouraging tone, given the company's repeated criminal behavior.

In our modern world, there is perhaps no more ominous prospect than a hostile foreign government's ability to compromise our country's infrastructure and devices. If Chinese companies like Huawei are given unfettered access to our telecommunications infrastructure, they could collect any of your information that traverses their devices or networks. Worse still: They'd have no choice but to

hand it over to the Chinese government if asked—the privacy and due process protections that are sacrosanct in the United States are simply non-existent in China.

## **Responding Effectively to the Threat**

The Chinese government is engaged in a broad, diverse campaign of theft and malign influence, and it can execute that campaign with authoritarian efficiency. They're calculating. They're persistent. They're patient. And they're not subject to the righteous constraints of an open, democratic society or the rule of law.

China, as led by the Chinese Communist Party, is going to continue to try to misappropriate our ideas, influence our policymakers, manipulate our public opinion, and steal our data. They will use an all-tools and all-sectors approach—and that demands our own all-tools and all-sectors approach in response.

Our folks at the FBI are working their tails off every day to protect our nation's companies, our universities, our computer networks, and our ideas and innovation. To do that, we're using a broad set of techniques—from our traditional law enforcement authorities to our intelligence capabilities.

And I will briefly note that we're having real success. With the help of our many foreign partners, we've arrested targets all over the globe. Our investigations and the resulting prosecutions have exposed the tradecraft and techniques the Chinese use, raising awareness of the threat and our industries' defenses. They also show our resolve and our ability to attribute these crimes to those responsible. It's one thing to make assertions—but in our justice system, when a person, or a corporation, is investigated and then charged with a crime, we have to prove the truth of the allegation beyond a reasonable doubt. The truth matters—and so, these criminal indictments matter. And we've seen how our criminal indictments have rallied other nations to our cause—which is crucial to persuading the Chinese government to change its behavior.

We're also working more closely than ever with partner agencies here in the U.S. and our partners abroad. We can't do it on our own; we need a whole-of-society response. That's why we in the intelligence and law enforcement communities are working harder than ever to give companies, universities, and the American people themselves the information they need to make their own informed decisions and protect their most valuable assets.

Confronting this threat effectively does not mean we shouldn't do business with the Chinese. It does not mean we shouldn't host Chinese visitors. It does not mean we shouldn't welcome Chinese students or coexist with China on the world stage. But it does mean that when China violates our criminal laws and international norms, we are not going to tolerate it, much less enable it. The FBI and our partners throughout the U.S. government will hold China accountable and protect our nation's innovation, ideas, and way of life—with the help and vigilance of the American people.

Thank you for having me here today.

## **Watch**

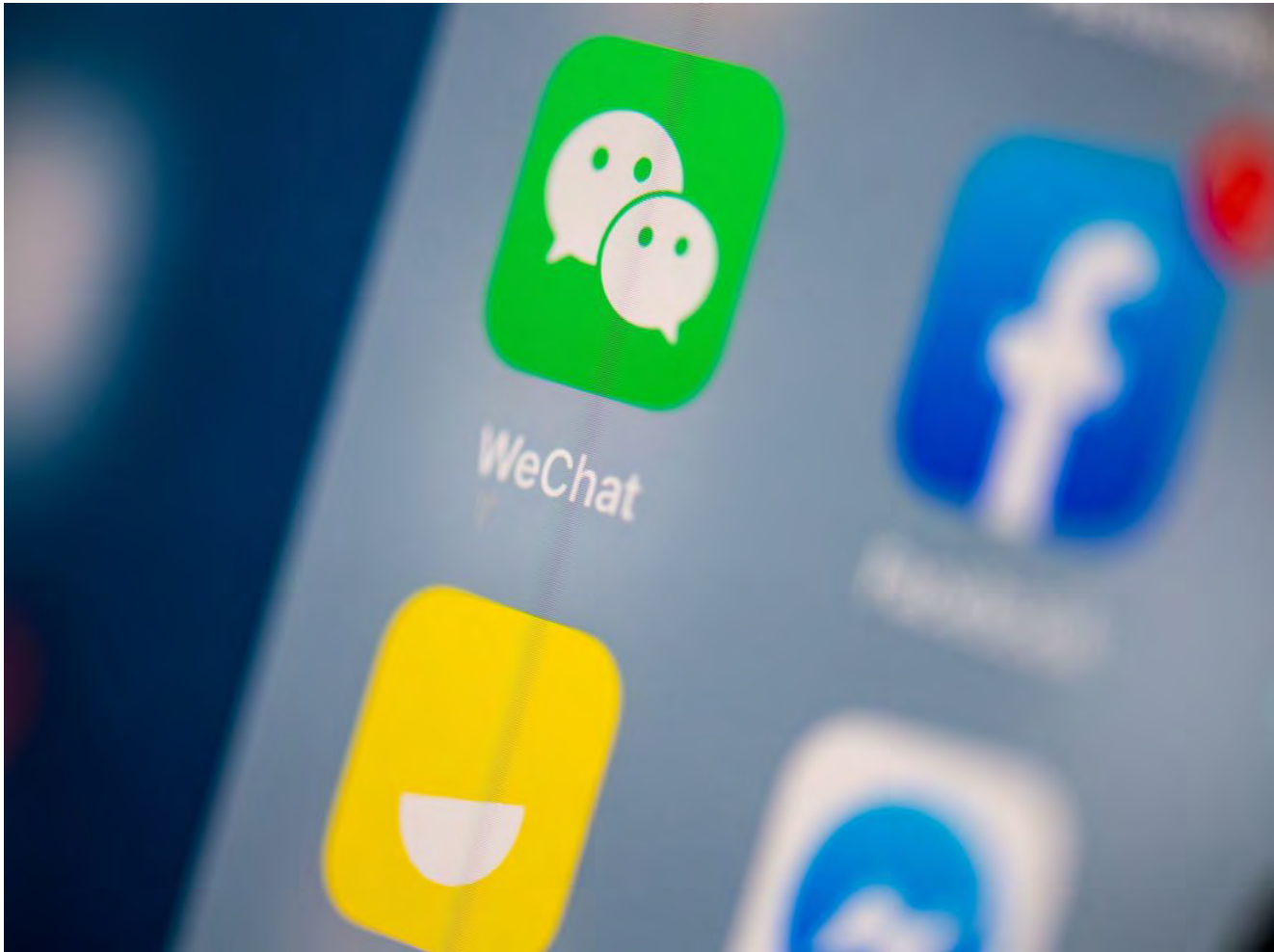
- Hudson Institute Video Event | China's Attempt to Influence U.S. Institutions: A Conversation with FBI Director Christopher Wray  
(<https://www.hudson.org/events/1836-video-event-china-s-attempt-to-influence-u-s-institutions-a-conversation-with-fbi-director-christopher-wray72020>)



## China Intercepts WeChat Texts From U.S. And Abroad, Researchers Say

[npr.org/2019/08/29/751116338/china-intercepts-wechat-texts-from-u-s-and-abroad-researcher-says](https://www.npr.org/2019/08/29/751116338/china-intercepts-wechat-texts-from-u-s-and-abroad-researcher-says)

Emily  
Feng

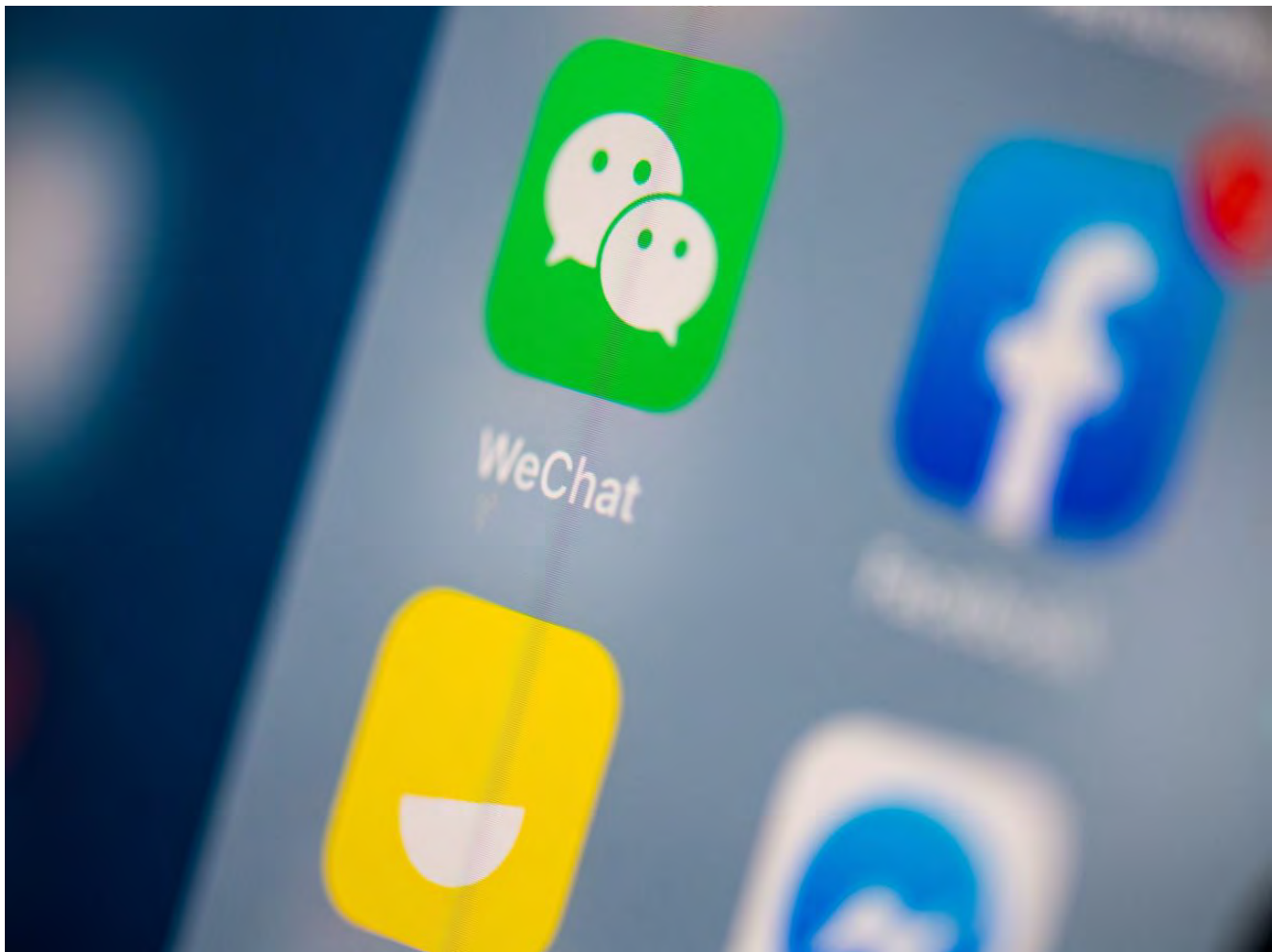


[Enlarge this image](#)

Owned by Tencent, one of China's biggest companies, the WeChat app has more than 1 billion monthly users in China and now serves users outside the country, too. **Martin Bureau/AFP/Getty Images** hide caption

**toggle caption**

Martin Bureau/AFP/Getty Images



Owned by Tencent, one of China's biggest companies, the WeChat app has more than 1 billion monthly users in China and now serves users outside the country, too.

Martin Bureau/AFP/Getty Images

**Updated on Sept. 19 at 10:23 a.m. ET**

The popular Chinese messaging app WeChat is Zhou Fengsuo's most reliable communication link to China.

That's because he hasn't been back in over two decades. Zhou, a human rights activist, had been a university student in 1989, when the pro-democracy protests broke out in Beijing's Tiananmen Square. After a year in jail and another in political reeducation, he moved to the United States in 1995.

But WeChat often malfunctions. Zhou began noticing in January that his chat groups could not read his messages. "I realized this because I was expecting some feedback [on a post] but there was no feedback," Zhou tells NPR from his home in New Jersey.



[Enlarge this image](#)

Chinese American human rights activist Zhou Fengsuo says he will continue using WeChat in spite of its vulnerabilities. "I have to use it to communicate. I just have to know what's going on" in China, he says. **Don Emmert/AFP/Getty Images** **hide caption**

**toggle caption**

Don Emmert/AFP/Getty Images



Chinese American human rights activist Zhou Fengsuo says he will continue using WeChat in spite of its vulnerabilities. "I have to use it to communicate. I just have to know what's going on" in China, he says.

Don Emmert/AFP/Getty Images

Chinese cyberspace is one of the most surveilled and censored in the world. That includes WeChat. Owned by Tencent, one of China's biggest companies, the chat-meets-payment app has more than 1 billion monthly users in China and now serves users outside the country, too, although it does not divulge how many. Researchers say its use abroad has extended the global reach of China's surveillance and censorship methods.

As Chinese technology companies expand their footprint outside China, they are also sweeping up vast amounts of data from foreign users. Every day, millions of WeChat conversations held inside and outside China are flagged, collected and stored in a database connected to public security agencies in China, say cyber researchers.

"The intention of keeping people safe by building these systems goes out the window the moment you don't secure them at all," says Victor Gevers, the Dutch co-founder of the nonprofit GDI Foundation, an open-source data security collective.



Zhou is not the only one experiencing recent issues. NPR spoke to three other U.S. citizens who have been blocked from sending messages in WeChat groups or had their accounts frozen earlier this year, despite registering with U.S. phone numbers.

"It doesn't matter where the user is, as long as I send a message to more than three people, my message cannot be seen in any group," says Stephen, a Chinese American technology professional. He declined to share his full name because he fears his criticism could draw retaliation against himself or his family by the authorities in China, where he travels often and where most of his family lives.

Stephen is baffled that he was blocked. He doesn't consider himself political. "It isn't shocking that China has that kind of censorship," he says. "The shocking piece is that China is exporting that kind of censorship to other parts of the world."

According to the Citizen Lab, an Internet watchdog group at the University of Toronto, WeChat's parent company Tencent created an extraordinarily advanced censorship algorithm to automatically identify combinations of keywords in messages and online articles that it then blocks. The censorship occurs whenever a Chinese-registered WeChat account receives or sends a message with flagged phrases.

"Using this sort of technique, Tencent has the ability to more precisely target content," says Jeffrey Knockel, a postdoctoral fellow at the Citizen Lab.

Since 2013, Citizen Lab has been monitoring how WeChat filters keywords and found it often updates which words are flagged in response to current events.

"We suspect that humans have some control over adding things to the list [of filtered keywords], but it's an open question whether these automated methods can add by themselves to the list," Knockel says.

From 3.784.309.399 messages, 3.698.798.784 were written in Chinese. 59.378.236 in English and 26.132.379 in another language. 98% of the Chinese messages had a GPS location in China. 68% of the English messages were sent in China. More than 19 million were sent from outside   
[pic.twitter.com/Va8Lfk3dnw](https://pic.twitter.com/Va8Lfk3dnw)

0xDUDE (@0xDUDE) April 22, 2019

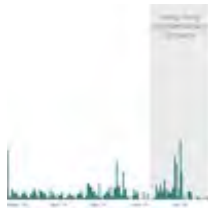
The Dutch researcher Gevers has studied Chinese social platforms as well and has exposed a large number of online vulnerabilities in their networks.

This March, Gevers found a Chinese database storing more than 1 billion WeChat conversations, including more than 3.7 billion messages, and tweeted out his findings. Each message had been tagged with a GPS location, and many included users' national



identification numbers. Most of the messages were sent inside China, but more than 19 million of them had been sent from people outside the country, mostly from the U.S., Taiwan, South Korea and Australia.

He says the system resembles the global surveillance methods used by the U.S. National Security Agency.



## **World**

---

### **China Used Twitter To Disrupt Hong Kong Protests, But Efforts Began Years Earlier**

---

For decades, the U.S. had unparalleled capabilities to monitor Internet traffic passing through servers within its borders. But Chinese tech companies like Tencent are now global, meaning this dragnet is believed to be sweeping up information about users from outside China.

"I think that really raises serious questions and challenges for users but also for regulators outside China," says Sarah Cook, a senior research analyst at Freedom House, an independent democracy watchdog.

Estimates of total WeChat accounts outside China are hard to come by, and the number is believed to be low — possibly in the tens of thousands — in the U.S. compared with popular networks like Facebook and its Messenger and WhatsApp platforms.

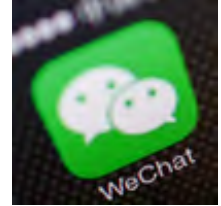
Cook points out that WeChat is used internationally not just by traveling Chinese citizens, but also by politicians in democracies communicating with Chinese constituents and dissident communities. "They're communicating with somebody else who's outside of China who has WeChat, but they're still for the most part often operating under the rules that are inside China," she says.

For some, the censorship came in stages. For example, a user could be temporarily blocked, as though to encourage better behavior. Sometimes a cat-and-mouse ensues between the censors and users.

Last February, David, a Chinese American doctor who does not want to use his last name for fear of backlash against his relatives still living in China, noticed his posts on WeChat's Moments— akin to a Facebook news feed — were not going through. Undeterred, he kept

sharing politically charged articles.

Within days, he couldn't send messages to any group chat: "Although I was able to read the other people's messages, when I posted my message, nobody could see it. It was like I wasn't there," he says.



## **Parallels**

---

### **The App That Helps The Chinese Masses Mobilize Online**

---

David then dialed back his sharing of news articles, limiting his conversations to trivial chitchat and music-sharing. His group chat function was quickly restored. Emboldened, he began sharing his political posts in group chats, only to find himself blocked again.

"Now I am very careful [on WeChat]. I feel like this censorship has affected both my psychology and my behavior," says David. He says he has abandoned his old account and created a new WeChat account to talk to loved ones in China. He lost thousands of contacts in the process. "This is just my main connection to my Chinese friends inside and outside of China."

Tencent, WeChat's owner headquartered in the southeastern city of Shenzhen, declined to comment.

Whether China's government can compel companies to hand over data access is a key question facing the country's major technology companies as they seek a larger share of world markets. For instance, telecommunications giant Huawei is trying to build a mobile network upgrade, known as 5G, around the world and says it would refuse Chinese government requests for data access. But legal experts say national security trumps privacy in China, even if companies put up a fight. U.S. officials allege that Huawei is controlled by the Chinese government, something the company and China's government have repeatedly denied.

"It's a bit of a red herring I think to argue about what the law says or does not say," says Donald Clarke, a George Washington University professor who specializes in Chinese law. Despite economic reforms, Clarke says, "China is essentially a Leninist state in which the government does not recognize any limits on its power."



## **World**

---

### **GitHub Has Become A Haven For China's Censored Internet Users**

---

Back in New Jersey, the activist Zhou says he will continue using WeChat in spite of its vulnerabilities. His work depends too much on it.

"I have to use it to communicate. I just have to know what's going on [in China]. But it is very dangerous," he concedes. "It's a natural choice. We have to use WeChat even though I know it's under surveillance all the time."

---

***Editor's note:*** An earlier version of this article said Victor Gevers found certain word patterns on WeChat that were flagged and archived. NPR has learned that his analysis used a set of keywords created previously by the Citizen Lab at the University of Toronto. We have amended the story to report on the original research the Citizen Lab conducted.

# EXHIBIT 21

TLP: WHITE



# EXECUTIVE ORDER 13873 RESPONSE

METHODOLOGY FOR ASSESSING THE MOST CRITICAL INFORMATION  
AND COMMUNICATIONS TECHNOLOGIES AND SERVICES

April 2020



**CISA**  
CYBER+INFRASTRUCTURE

TLP: WHITE



**TLP: WHITE**

This page is intentionally left blank.

**TLP: WHITE**

## KEY FINDINGS

- The Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center (NRMCC) identified 61 Information and Communication Technology (ICT) elements organized into five roles (Local User Access, Transmission, Storage, Processing, and System Management) and 11 sub-roles.
- The 11 sub-roles are:
  - Broadcast Networks
  - Wireless Local Area Networks
  - Mobile Networks
  - Satellite Access Points
  - Cable Access Points
  - Wireline Access Points
  - Core Networking Systems
  - Long and Short Haul Networks
  - Storage and Cloud Based Services
  - End User and Edge Networking Equipment
  - Security and Operations

Contents

Key Findings..... 2

Background..... 4

Scope..... 4

    Caveats and Limitations..... 4

Methodology Overview ..... 5

    Step 1: Developing an ICT Framework .....5-12

    Step 2: Assessing Criticality ..... 12-13

Implications for the 5G Network ..... 13

Future Analysis..... 13-13

Appendix A: National Critical Functions..... 15-16

Appendix B: Glossary ..... 17-19

DHS Point of Contact..... 20

Figures

Figure 1. ICT Framework.....6

Tables

Table 1. Element List and Element Definitions.....6-12

Table 2. National Critical Functions.....15

## BACKGROUND

On May 15, 2019, the President signed Executive Order (EO) 13873: Securing the Information and Communications Technology and Services Supply Chain. This EO addresses the threat posed by the unrestricted acquisition or use of Information and Communications Technology (ICT) and services “designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries,” and declares a national emergency with respect to this threat.

The EO requires the Secretary of the Department of Homeland Security (DHS) to produce a written assessment within 80 days and annually thereafter that would “assess and identify entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to the national security of the United States.”<sup>1</sup> The assessment “shall include an evaluation of hardware, software, or services relied upon by multiple information and communications technology or service providers, including the communications services relied upon by critical infrastructure entities identified pursuant to Section 9 of Executive Order 13636.”

Within DHS, the responsibility to execute the assessment was assigned to CISA/NRMC on behalf of the Secretary. In its response to this EO, the NRMC coordinated with federal and private partners to assess what ICT hardware, software, and services (referred to individually in this report as elements) present the greatest vulnerabilities in U.S. infrastructure and pose the greatest consequences.

## SCOPE

Information technology and communications technology intersects almost every aspect of operations essential to national security, the Nation’s critical infrastructure, and National Critical Functions (NCFs). NCFs are those functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof. DHS, through coordination with federal and industry partners, scoped its response to the Executive Order to accomplish the following:

- Develop a taxonomy of ICT elements based on Information Technology (IT) and Communication roles and sub-roles.<sup>i</sup>
- Assess the criticality of ICT element classes based on their sub-role and in the context of the IT or Communications sector function it supports.

This paper describes DHS’s methodology for assessing ICT element criticality.

## Caveats and Limitations

NRMC faced several challenges in responding to the EO including:

- Conducting a broad assessment with a short timeline that also allows a reasonable amount of time for vetting and validation with industry subject matter experts (SMEs), sector specific agencies (SSAs), and coordinating councils.
- Providing a general assessment of ICT element criticality independent from the application of the element in any specific network or system.<sup>ii</sup>
- Assessing an element known to support critical functions in some systems and non-critical functions in other contexts.

---

<sup>i</sup> In its response to the EO, DHS is assessing classes of elements rather than makes, models, and versions of elements, but will be able to use these assessments to assess specific makes, models, and versions within the most critical classes of elements in future iterations of analysis.

<sup>ii</sup> A system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- Identifying existing system-specific security measures that mitigate potentially risky attributes of technologies acquired through the supply chain.
- Handling technology trends geared to enable remote access, monitoring, administration, and control.

DHS will work to minimize and address these limitations as it develops its annual assessment as required by Executive Order 13873, as well as augment its assessments with additional analysis.

## METHODOLOGY OVERVIEW

With support from Argonne National Laboratory and Sandia National Laboratories, DHS developed a two-step approach to assessing the criticality of ICT hardware, software, and services (ICT elements) in the IT and Communications sectors.<sup>iii</sup> In step 1, DHS developed an ICT Framework to decompose the basic roles and sub-roles ICT elements provide within the IT and Communications sectors, and then identified the elements that support each sub-role. In step 2, DHS developed and executed a repeatable approach for analyzing the criticality of ICT elements.

Each step of the methodology required extensive contributions from ICT SMEs. NRMCC partnered with industry through a government established ICT Supply Chain Risk Management (SCRM) Task Force (ICT SCRM TF) to ensure the perspectives and expertise of critical infrastructure owners and operators could provide acute insight into operations and operational use of ICT. The ICT SCRM TF is a Critical Infrastructure Partnership Advisory Council (CIPAC) Cross Sector Working Group where the respective IT and Communications Sector Coordinating Council Chairs serve as the industry co-chairs. Accordingly, the co-chairs were able to solicit representative members from across the IT and Communications sectors, a majority of which are members of the Task Force, to provide input based on their experience and expertise. Additionally, the TF engaged non-member SMEs as necessary to provide inputs to inform the TF recommendations.

### Step 1: Developing an ICT Framework

In step 1, DHS developed an ICT Framework to serve as a generic representation of IT and Communications sector roles and sub-roles, which would then be used to identify and bin ICT elements to draw basic judgements about criticality. The ICT Framework is organized into five roles (Local User Access, Transmission, Storage, Processing, and System Management) and 11 sub-roles, shown in figure 1 below.

To narrow the scope of the required EO assessment to a manageable, but meaningful initial response, DHS focused on the NCFs most closely aligned to the Communications sector and the portions of the Information Technology sector that the Communications sector depends on. These select NCFs, which align closely with the “Connect” theme, were chosen due to their extensive dependence on ICT elements, their criticality to other NCFs, and the criticality to national security of not just U.S. interconnectivity, but global interconnectivity. These NCFs enable all forms of communications in the United States, without which, all U.S. operations would be impacted with potentially catastrophic consequences:

- Operate Core Networks
- Provide Cable Access Network Services
- Provide Internet Routing, Access, and Connection Services
- Provide Radio Broadcast Access Network Services
- Provide Satellite Access Network Services
- Provide Wireless Access Network Services
- Provide Wireline Access Network Services

<sup>iii</sup> Due to time limitations, DHS was unable to analyze ICT elements for all critical infrastructure sectors. DHS chose to analyze the IT and Communications sectors because of their criticality for all other sectors.



TLP: WHITE

These NCFs were selected due to their dependence on ICT elements and their criticality for other functions. See Appendix A for more information on NCFs.

When NCFs are decomposed into the ICT elements that support them, each element is organized into the ICT Framework (roles and sub-roles) shown below in figure 1:

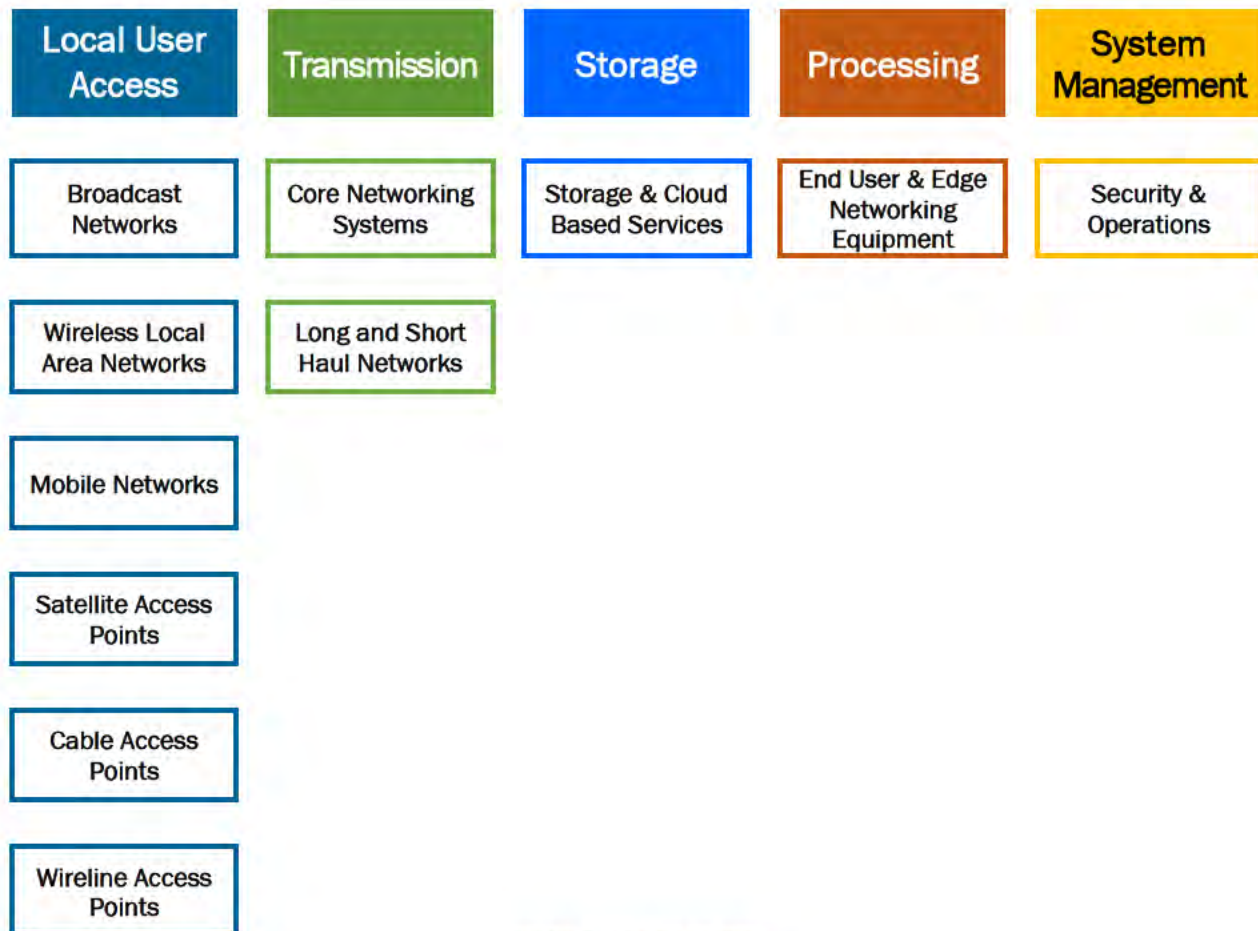


FIGURE 1—ICT FRAMEWORK

DHS identified 61 ICT elements (i.e. hardware, software, or services) that support 11 sub-roles of the ICT Framework. The list of 61 elements with definitions is below in table 1.

TABLE 1—ELEMENTS AND DEFINITIONS

ELEMENT	DEFINITION
<b>BROADCAST NETWORKS</b>	
Emergency Alert System (EAS) Encoder/Decoder	EAS encoder/decoders allow TV broadcast stations to take audio signals containing data and filter them for geographic region and emergency event information.
Station to Transmitter Link (STL)	The STL transports program material from a local station's studio to the station's transmitter site for broadcast.

TLP: WHITE

TLP: WHITE

ELEMENT	DEFINITION
Transmitter	A transmitter takes baseband audio, video, or digital signal and converts it to a radio frequency and amplifies it to drive a broadcast transmission antenna.
<b>WIRELESS LOCAL AREA NETWORKS</b>	
Distributed Antenna System (DAS)	A DAS is a network of spatially separated antennas that provide wireless service within a geographic area or structure. DAS will be applicable in Fifth Generation (5G); however, small cells and differing spectrum bands may change how a DAS is utilized.
Small Cells/Micro Cell	A small cell is a miniature base station that transmits short-range radio signals. Due to the limited range and non-penetrative signal of high frequency radio wave bands, 5G will require numerous small cells to support its infrastructure. Together, these cells would form a dense network that relays data through multiple small cells.
<b>MOBILE NETWORKS</b>	
Base Station Controller (BSC)	BSC controls facilitate communication between one or more base stations or cell sites.
Base Station Subsystem (BSS)	In a mobile cellular network, the BSS handles traffic between the cell phone and the network switching subsystem.
Base Transceiver Station (BTS)	A BTS is a 2G fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
Cell Session Control Function	A system that manages the signaling from end-user to services and other networks, providing the end-to-end connectivity across networks.
eNodeB	An eNodeB is a Fourth Generation (4G) Long-term Evolution (LTE) fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
gNodeB/5G NR	A gNodeB/5G NR is a 5G fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
NodeB	A NodeB is a 4G fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
Home Agent	A router on a home network which enables communication to provider networks.

TLP: WHITE

TLP: WHITE

ELEMENT	DEFINITION
Home Location Register (HLR)	In a mobile cellular network, the HLR is the main database of permanent subscriber Personally Identifiable Information (PII) for a mobile network.
Home Subscriber Server (HSS)	The HSS is the master user database that supports the IP Multimedia Subsystem (IMS) network entities that handle calls and sessions. It contains user profiles, performs authentication and authorization of the user, and can provide information about the physical location of user.
Mobility Management Entity (MME)	The MME is responsible for idle mode user equipment tracking, paging procedure, activation and deactivation process, call handover, and user authentication.
Mobile Switching Center (MSC)	The MSC is the hub that handles many of the communication switching functions, including call setup, routing, release, messaging, and advanced features.
Equipment Identity Register (EIR)	The EIR is a database that contains a record of the all equipment that is allowed in a network and all equipment that is blacklisted.
Policy Decision Function	A ruleset engine that arbitrates the overall features and functions on the network that are available to users, and the allocation of resources and bandwidth available.
Mobile Positioning Center (MPC)	MPC is a service or function that that works to determine the position of a mobile device.
Gateway Mobile Location Center (GMLC)	GMLC is a service or function that that works to determine the position of a mobile device in mobile cellular networks. It is also expected to go away once there is a full conversion to 5G networks.
Media Gateway	A Media Gateway translates media content between various network and communication protocols.
Media Gateway Control Function (MGCF)	An MGCF performs switching and conversion between control switched and packet switched domains, connecting the mobile and standard telephony systems.
Gateway GPRS Support Node (GGSN)	A GGSN provides switching between the General Packet Radio Service (GPRS) network and packet switched networks, and routing on the GPRS mobile network.
Serving GPRS Support Node	A serving GPRS support node provides supporting functions for packet switched data within the network, such as user authentication and management.

TLP: WHITE

TLP: WHITE

ELEMENT	DEFINITION
Session Border Controller (SBC)	SBCs are used by all interconnected Voice over Internet Protocol (VoIP) providers and carriers to establish, maintain, and tear down phone calls through IP based networks.
Operation Support System (OSS)	OSS is comprised of hardware and software systems that allow network operators to perform network monitoring and management functions, such as configuration and provisioning. It also contains a large database of customer information and manages billing information.
SATELLITE ACCESS POINTS	
Satellite Payload	The space-based functional component of the communications platform. The satellite payload is the means by which the satellite mission is accomplished. Example satellite payloads include communications, PNT, signal detection, Overhead Persistent Infrared (OPIR), radar, imaging, etc. The payload may include some of the same component types as the satellite bus (e.g., communications transmitter/receiver, power amplifier, antenna, etc.) and often depends upon the satellite bus for a number of functions including power source, data processing, communication services, etc.
Satellite Bus	The space-craft system hosting the communications payload, which includes satellite navigation components, flight dynamics, fuel tank(s), thrusters, reaction wheels, solar panels, batteries, wiring harnesses, radiation shielding, the frame structures, power distribution, and a basic communication system for receiving instructions called TT&C (telemetry, tracking, and command). The satellite mission will determine the bus design or, conversely, the bus design will constrain the types of missions that can be supported by the satellite. For communications satellites, the payload may be integrated with the communications components of the satellite bus.
Satellite Ground Control Station (SGCS)	Facility providing satellite telemetry, tracking, and command (TT&C) connectivity from the Spacecraft Operations Center to the satellite.
Spacecraft Operations Center (SOC)	Terrestrial-based spacecraft operations facility that maintains the health and safety of the spacecraft and, if applicable, satellite mobility.
Communications Ground Station/Teleport	Ground equipment and facilities for managing subscribers, controlling subscriber access to services, providing billing for services, and providing interoperation between subscriber sessions and other networks.
Satellite Network Operations Center (SNOC)	Provides functionality to maintain network operations, such as providing user access, account management, and network health and operation.
Teleport Network	Terrestrial mesh of multi-terminal ground stations (Teleports) providing bulk space-ground connectivity, as well as interconnecting the various elements of Operations and Gateway Segments.

TLP: WHITE



TLP: WHITE

ELEMENT	DEFINITION
Uplink Facility	Terrestrial-based facility that provides uplink of content to be distributed to subscriber equipment.
<b>CABLE ACCESS POINTS</b>	
Core Server	A core server is a hardware and software system that provides functionality to other devices in the telecommunications backbone or core network, including data, processing, and management services.
Core Router	A core router directs packets through the network, specially designed for handling large volumes of data at high speeds as part of the telecommunications backbone.
Core Switch	A core switch performs packet switching operations, specially designed for handling large volumes of data at high speeds as part of the telecommunications backbone.
<b>WIRELINE ACCESS POINTS</b>	
Access Infrastructure Data Link	An access infrastructure data link is a communications pathway that provides data transmission services to wireline subscribers.
Access Infrastructure Digital Loop	An access infrastructure digital loop provides connectivity from the service provider to wireline subscribers.
<b>CORE NETWORKING SYSTEMS</b>	
Core Infrastructure SONET/SDH	Core Infrastructure SONET/SDH is a widely deployed technology used in implementing high-speed, large-scale Internet Protocol (IP) networks.
Core Infrastructure DWDM/OTN	Core Infrastructure DWDM/OTN are technologies that increase capacity on networks and optimize the existing resources of transportation networks.
Core Infrastructure IP/Internet	Core Infrastructure IP/Internet delivers data from the source host to the destination host within a communication network.
Core Infrastructure CDN Cache	A CDN is a system of distributed servers that deliver web pages and other content to users based on their geographic locations.

TLP: WHITE



TLP: WHITE

ELEMENT	DEFINITION
Core Infrastructure IP/MPLS	IP/Multiprotocol Label Switching (MPLS) refers to a network backbone that uses the IP augmented with MPLS routing. MPLS is a mechanism for routing traffic within a telecommunications network, as data travels from one network node to the next.
Data Center MPLS Routers	MPLS routers that support a data center.
Metro MPLS Routers	MPLS routers that support a metro area.
LONG AND SHORT HAUL NETWORKS	
Fiber Optic Cable	Fiber optic cable is the medium in which transmission of information as light pulses occurs along a glass, plastic strand, or fiber. Fiber optic cable is used across all domains (e.g., enterprise, long and short haul, cable, oceanic, etc.).
Repeaters	A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than what would be capable with the original signal.
STORAGE AND CLOUD BASED SERVICES	
Server	A server is a hardware and software system that provides functionality to other devices in the system, including data, processing, and management services.
END USER EQUIPMENT & EDGE NETWORKING EQUIPMENT	
LAN Equipment (sensitive) <sup>iv</sup>	Local Area Network Equipment (sensitive) facilitates communication between one or more computers and other devices in a limited geographic area within a sensitive system. Typical equipment includes routers, switches, network interfaces cards, and cables.
LAN Equipment (non-sensitive)	Local Area Network Equipment (non-sensitive) facilitates communication between one or more computers and other devices in a limited geographic area that is not within a sensitive system. Typical equipment includes routers, switches, network interfaces cards, and cables.
Mobile Devices (sensitive)	Mobile devices (sensitive) are handheld, portable computing devices that can connect to a cellular network and process classified or sensitive information. Commonly refers to cellular phones, but can also refer to tablets, e-readers, and other devices that can connect to a cellular network.
Mobile Devices (non-sensitive)	Mobile devices (non-sensitive) are handheld, portable computing devices that can connect to a cellular network and process information that is not classified or sensitive. Commonly refers to cellular phones, but can also refer to tablets, e-readers, and other devices that can connect to a cellular network.

<sup>iv</sup> An element is designated as sensitive if it resides within a network or system that contains classified or sensitive data such that, if the data's confidentiality, integrity, or availability were to be compromised, there could be severe consequences. Examples of such networks include federal, military, and certain critical infrastructure networks.

TLP: WHITE

TLP: WHITE

ELEMENT	DEFINITION
Computers (sensitive)	Computers (sensitive) are general-purpose computers designed to be used by a single end-user (to include business staff one at a time) within a sensitive network or system, or process classified or sensitive data.
Computers (non-sensitive)	Computers (non-sensitive) are general-purpose computers designed to be used by a single end-user (to include business staff one at a time) and are not located within a sensitive network or system, nor process classified or sensitive data.
<b>SECURITY &amp; OPERATIONS</b>	
Domain Name System (DNS)	DNS translates internet domains and hostnames to IP addresses.
Systems Software (sensitive)	Systems software (sensitive) includes the programs that are dedicated to managing the computer itself, such as the operating system, security software, and file management utilities, and have been installed on sensitive systems.
Systems Software (non-sensitive)	Systems software (non-sensitive) includes the programs that are dedicated to managing the computer itself, such as the operating system, security software, and file management utilities and have not been installed on a sensitive system.
Applications Software (sensitive)	Applications software (sensitive) includes software that enables the user to complete tasks, such as creating documents, spreadsheets, databases and publications, doing online research, sending email, designing graphics, and running businesses and has been installed on a sensitive system.
Applications Software (non-sensitive)	Application software (non-sensitive) includes software that enables the user to complete tasks, such as creating documents, spreadsheets, databases and publications, doing online research, sending email, designing graphics, and running businesses and is not installed on a sensitive system.

## Step 2: Assessing Criticality

In step 2, DHS developed and executed a repeatable approach for assessing the criticality of ICT elements. DHS assessed the criticality of each ICT element in the context of the IT or Communications sector function it supports. This enabled DHS to distinguish the criticality of similar elements used in different sub-roles, for example, the difference in the criticality of routers used in core networks responsible for routing terabytes of data as opposed to routers used in home networks for personal use.

DHS worked with SMEs from CISA, industry partners, and national laboratories to collect data to analyze element criticality. Elements were assessed at the following criticality levels:<sup>v</sup>

- **Critical:** Compromise of the element could create an unacceptable amount of risk to the national security of the United States. There would likely be significant regional or national impacts, including

<sup>v</sup> DHS assessed the criticality of element classes based on how their compromise could affect the sub-role they support. With the exception of edge ICT elements (end user equipment, edge networking equipment, and end user software) which DHS assessed based on whether they were used in sensitive or non-sensitive networks, DHS did not identify specific elements that may be more or less critical based on what entities rely on them. For example, an element that supports military functions may be more critical than a similar element that does

TLP: WHITE

affecting operations and the confidentiality, integrity, or availability of data or the system, and the ability to effectively mitigate these risks is uncertain or unsatisfactory.

- **Manageably Critical:**<sup>vi</sup> Compromise of the element could potentially have significant regional or national impacts, including affecting the confidentiality, integrity, or availability of data or the system, but risks can be mitigated with reliable and reasonable measures when properly implemented, such as using encryption or having redundant components supplied by multiple vendors and manufacturers.
- **Not Critical:** Compromise of the element is unlikely to have significant regional or national impacts.

DHS assessed the criticality of 61 ICT elements from the perspective of an administrator or network operator with privileged access. The ICT element criticality assessments can be analyzed collectively to prioritize supply chain risk management efforts.

DHS conducted and continues to refine its assessments<sup>vii</sup> of element criticality and risk. This analysis contains sensitive information and is not included in this public document.

## IMPLICATIONS FOR THE FIFTH GENERATION (5G) NETWORK

5G, the next generation mobile network, represents a complete transformation of telecommunication networks. Combining new and legacy elements and infrastructure, 5G will build upon previous generations in an evolution that will occur over many years, utilizing existing infrastructure and technology. As 5G technologies are deployed, some elements may become more or less critical due to increasing or decreasing reliance upon them, or changes in how they are used. Distributed antenna systems will continue to be used in 5G, but the use of small cells<sup>viii</sup> and differing spectrum bands may change how a DAS is utilized. eNodeB/5G NR are 5G fixed communications locations that relay information to and from a transmitting or receiving unit, such as a mobile phone. eNodeB/5G performs a similar function as eNodeB (4G LTE) and NodeB (4G) elements, and as we move towards 5G, the criticality of elements from previous generations may require reassessment. GMLC are expected to go away completely once there is a full conversion to 5G networks. It is likely that 5G's development and deployment and other changes to the IT and Communications sectors will require the reevaluation of some elements' criticality, and potentially the introduction of new elements to this assessment.

## FUTURE ANALYSIS

DHS' initial analysis in response to Executive Order 13873 is foundational and will support future ICT supply chain analysis. Topics for future analysis may include:

- **Identify and Assess the Criticality of Elements in Other Sectors:** DHS will work with SMEs from other sectors and expand upon this analysis to identify and assess the ICT elements critical to those sectors.
- **Identify and Assess Specific Makes, Models, and Versions of Hardware, Software, and Services:** DHS' initial assessment and methodology may be used in follow-on analysis to identify elements of ICT hardware, software, and services, including analyzing specific products and services to understand the potential vulnerabilities they introduce and the potential consequences they pose.
- **Identify and Evaluate Entities that Manufacture or Provide Critical ICT Elements:** DHS may identify the key suppliers and manufacturers of critical ICT elements, and work with the Office of the Director of

not support military operations. Future analysis is planned to identify specific elements whose compromise would have potentially more significant consequences based on system deployment use cases.

<sup>vi</sup> Manageably Critical elements are still critical. There could still be significant national security consequences if key mitigations are not in place—such as vendor diversity, element redundancy, and encryption.

<sup>vii</sup> The list of ICT element criticality assessments, while “final,” is not a permanent list, but will be dynamic and updated periodically to reflect current data on supply, demand, concentration of production, innovation in ICT sectors, new vulnerability considerations, and new mitigation considerations. This final list will serve as the Department of Commerce's initial focus as it develops its report to comply with Executive Order 13873.

<sup>viii</sup> Small cells and micro cells are miniature cellular towers that transmit short-range radio signals.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

TLP: WHITE

National Intelligence (ODNI) to incorporate threat analysis into its ICT supply chain analyses. Additionally, DHS reviewed the ODNI EO 13873 response before finalizing this report and found that the two products are complementary for meaningful subsequent analysis.

- **Identify the Most Critical Users of Critical ICT Elements:** DHS may identify entities within the United States whose use of compromised ICT Elements could result in the greatest consequences.
- **Identify or Assess Technology Serving Primarily Physical Purposes:** DHS may expand its list of elements to include Operations Technology (OT), such as programmable logical controllers (PLCs), and Internet of Things (IoT) technology, such as networked thermostats and telematics equipment, which serve primarily physical purposes.<sup>ix</sup>
- **Compare the Consequences of Data Theft with the Consequences of System Damage or Disruption:** It is likely that the set of entities identified as having high potential consequences from data theft will be different from the set of entities identified as having high potential consequences from damage or disruption.
- **Evaluate the Potential Impacts from Mitigation Activities:** DHS may evaluate the potential impacts to U.S. entities from various mitigation activities. This could include evaluating how identified threats might respond to mitigation actions taken by U.S. entities, including the Federal Government, and what the possible consequences of those responses would be for national security. DHS' written assessment may be used in follow-on analysis to analyze potential threat countermeasures and their possible consequences.
- **Analyze ICT Elements Throughout the ICT Supply Chain Phases:** DHS may evaluate elements and assess risk throughout each phase of the supply chain:<sup>2</sup>
  - Phase 1: Design
  - Phase 2: Development and Production
  - Phase 3: Distribution
  - Phase 4: Acquisition and Deployment
  - Phase 5: Maintenance
  - Phase 6: Disposal

---

<sup>ix</sup> DHS defines IoT as "the connection of systems and devices with primarily physical purposes (e.g., sensing, heating and cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems."

TLP: WHITE



TLP: WHITE

## APPENDIX A: NATIONAL CRITICAL FUNCTIONS

NCFs are those functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof. This assessment focuses on the *Connect* theme of the National Critical Functions list as it covers the backbone of national connectivity that enables cross-country and global operations. Please see table 2 below:

TABLE 2—NATIONAL CRITICAL FUNCTIONS

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
<ul style="list-style-type: none"> <li>Operate Core Network</li> <li>Provide Cable Access Network Services</li> <li>Provide Internet Based Content, Information, and Communication Services</li> <li>Provide Internet Routing, Access, and Connection Services</li> <li>Provide Positioning, Navigation, and Timing Services</li> <li>Provide Radio Broadcast Access Network Services</li> <li>Provide Satellite Access Network Services</li> <li>Provide Wireless Access Network Services</li> <li>Provide Wireline Access Network Services</li> </ul>	<ul style="list-style-type: none"> <li>Distribute Electricity</li> <li>Maintain Supply Chains</li> <li>Transmit Electricity</li> <li>Transport Cargo and Passengers by Air</li> <li>Transport Cargo and Passengers by Rail</li> <li>Transport Cargo and Passengers by Road</li> <li>Transport Cargo and Passengers by Vessel</li> <li>Transport Materials by Pipeline</li> <li>Transport Passengers by Mass Transit</li> </ul>	<ul style="list-style-type: none"> <li>Conduct Elections</li> <li>Develop and Maintain Public Works and Services</li> <li>Educate and Train</li> <li>Enforce Law</li> <li>Maintain Access to Medical Records</li> <li>Manage Hazardous Materials</li> <li>Manage Wastewater</li> <li>Operate Government</li> <li>Perform Cyber Incident Management Capabilities</li> <li>Prepare for and Manage Emergencies</li> <li>Preserve Constitutional Rights</li> <li>Protect Sensitive Information</li> <li>Provide and Maintain Infrastructure</li> <li>Provide Capital Markets and Investment Activities</li> <li>Provide Consumer and Commercial Banking Services</li> <li>Provide Funding and Liquidity Services</li> <li>Provide Identity Management and Associated Trust Support Services</li> <li>Provide Insurance Services</li> <li>Provide Medical Care</li> <li>Provide Payment, Clearing, and Settlement Services</li> <li>Provide Public Safety</li> <li>Provide Wholesale Funding</li> <li>Store Fuel and Maintain Reserves</li> <li>Support Community Health</li> </ul>	<ul style="list-style-type: none"> <li>Exploration and Extraction of Fuels</li> <li>Fuel Refining and Processing Fuels</li> <li>Generate Electricity</li> <li>Manufacture Equipment</li> <li>Produce and Provide Agricultural Products and Services</li> <li>Produce and Provide Human and Animal Food Products and Services</li> <li>Produce Chemicals</li> <li>Provide Metals and Materials</li> <li>Provide Housing</li> <li>Provide Information Technology Products and Services</li> <li>Provide Materiel and Operational Support to Defense</li> <li>Research and Development</li> <li>Supply Water</li> </ul>
<p><b>National Critical Functions:</b> The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.</p>			

TLP: WHITE



**TLP: WHITE**

DHS' assessment specifically addresses the following National Critical Functions (NCFs) within the *Connect* theme:

- Operate Core Network
- Provide Cable Access Network Services
- Provide Internet Routing, Access, and Connection Services
- Provide Radio Broadcast Access Network Services
- Provide Satellite Access Network Services
- Provide Wireless Access Network Services
- Provide Wireline Access Network Services

To narrow the scope of the required EO assessment to a manageable, but meaningful initial response, DHS focused on the NCFs most closely aligned to the Communications sector and the portions of the Information Technology sector that the Communications sector depends on. The focus on NCFs within these sectors was due to the extensive dependence of these NCFs on ICT elements, their criticality to other NCFs, and the criticality to national security of not just U.S. interconnectivity, but global interconnectivity. These NCFs enable all forms of communications in the United States, without which, all U.S. operations would be impacted with potentially catastrophic consequences.

**TLP: WHITE**

## APPENDIX B: GLOSSARY

**Broadcast Networks:** Identified as a sub-role in the ICT Framework. Networks consisting of free and subscription-based, over-the-air radio and television (TV) stations that offer analog and digital audio and video programming services and data services.

**Cable Access Points:** Identified as a sub-role in the ICT Framework. Systems offering access to analog and digital video programming services, digital telephone service, and high-speed broadband services. Utilizes a mixture of fiber and coaxial cable commonly referred to as a hybrid fiber/coaxial (HFC) network to provide bi-directional signal paths to the customer.

**Connect Theme (of National Critical Functions):** The NCF *Connect* theme contains nine critical functions, including: Operate Core Network; Provide Cable Access Network Services; Provide Internet Routing, Access, and Connection Services; Provide Radio Broadcast Access Network Services; Provide Position, Navigation, and Timing Services; Provide Internet-Based Content, Information, and Communication Services; Provide Satellite Access Network Services; Provide Wireless Access Network Services; and Provide Wireline Access Network Services.

**Core Networking Systems:** Identified as a sub-role in the ICT Framework. Core networking systems (also known as “backbone” systems when used to describe internet networks) facilitate the exchange of information among various sub-networks.

**Critical:** This is a criticality determination made by the National Risk Management Center. Compromise of the element could create an unacceptable amount of risk to the national security of the United States. There would likely be significant regional or national impacts, including affecting operations and the confidentiality, integrity, or availability of data or the system, and the ability to effectively mitigate these risks is uncertain or unsatisfactory.

**Criticality Criteria:** Criticality criteria considers important factors that will have the greatest impact on consequences.

**End User Equipment and Edge Networking Equipment:** Identified as a sub-role in the ICT Framework. End user equipment is any device used by an end-user to communicate, while edge networking equipment provide an entry point for end user equipment to connect into core networking systems. Examples include cellular phones, desktop and laptop computers, and tablets; related local area network infrastructure; and related software.

**ICT Element:** An ICT element is a type of hardware, software, or service.

**ICT Element Core Factors:** Core factors are the low-level functional operations performed by individual ICT elements that collectively contribute to determining overall criticality of the element.

**ICT Framework:** The ICT Framework is comprised of generic representation of ICT systems, which will serve as an organizing principle for binning ICT elements and drawing basic judgements about criticality.

**Independent Mitigation:** Non-element functions obviate concerns. This is one criticality criterion used by the National Risk Management Center to make criticality determinations.

**Local User Access:** One of five determined ICT Framework roles. Systems facilitating individual or group user access, via devices, to telecommunications and internet resources.

**Long Haul and Short Haul Networks:** Identified as a sub-role in the ICT Framework. Communication networks spanning both long and short distances.

**Manageably Critical:** This is a criticality determination made by the National Risk Management Center. Compromise of the element could potentially have significant regional or national impacts, including affecting

the confidentiality, integrity, or availability of data or the system, but risks can be mitigated with reliable and reasonable measures when properly implemented, such as using encryption or having redundant components supplied by multiple vendors and manufacturers.

**Mobile Networks:** Identified as a sub-role in the ICT Framework. Also known as “cellular networks.” A communication network where the last link is wireless. The network is distributed over land areas called cells, each served by at least one fixed-location transceiver. When joined together, these cells provide radio coverage over a wide geographic area.

**National Critical Functions (NCFs):** NCFs are those functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof.

**Not Critical:** This is a criticality determination made by the National Risk Management Center. Compromise of the element is unlikely to have significant regional or national impacts.

**Processing:** One of five determined ICT Framework roles. Systems supporting the creation and manipulation of data or information for a variety of purposes.

**Roles:** Roles are represented as the five top-level headings of the ICT Element Framework (local user access, transmission, storage, processing, and system management). ICT roles group ICT elements into broad categories of ICT operations they facilitate.

**Satellite Access Points:** Identified as a sub-role in the ICT Framework. Systems offering access to platforms launched into orbit to relay voice, video, or data signals as part of a telecommunications network.

**Security and Operations:** Identified as a sub-role in the ICT Framework. Devices, services, and software that provide security and operational functions within a network.

**Security Features:** Hardware, software, and services that are integrated into ICT systems to provide protection from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide (i.e., anti-virus/anti-malware, IDS/IPS, encryption, authentication, etc.).

**Sensitive:** An element is designated as sensitive if it resides within a network or system that contains classified or sensitive data such that, if the data’s confidentiality, integrity, or availability were to be compromised, there could be severe consequences. Examples of such networks include federal, military, and certain critical infrastructure networks.

**Sub-Roles:** Sub-Roles further group ICT elements into narrower operational roles under each of the five ICT roles. ICT elements are decomposed under the sub-roles they support.

**Storage:** One of five determined ICT Framework roles. Systems supporting retention of data generated by computers and other devices generated either locally or remotely.

**Storage and Cloud Based Delivery:** Identified as a sub-role in the ICT Framework. Computer data storage and delivery, either on a local server, or (in the case of cloud-based) on multiple servers across multiple locations.

**System:** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.<sup>3</sup>

**System Management:** One of five determined ICT Framework roles. Devices, services, and software serving functions required for system operation, security, and maintenance.

**TLP: WHITE**

**Transmission:** One of five determined ICT Framework roles. Systems supporting the process of sending data over a communication medium to one or more computing, network, transit network, communication or electronic devices in a point-to-point, point-to-multipoint, or multipoint-to-multipoint environment.

**Wireless Local Area Networks:** Identified as a sub-role in the ICT Framework. Systems offering access to telecommunication in which electromagnetic waves (rather than wire) carry the signal over part of or the entire communication path.<sup>x</sup>

**Wireline Access Points:** Identified as a sub-role in the ICT Framework. Circuit- and packet-switched networks via copper, fiber, and coaxial transport media.

---

<sup>x</sup> Wireless technologies consist of cellular phones, wireless hot spots (WiFi), personal communication services, high-frequency radio, unlicensed wireless, and other commercial and private radio services to provide communication services.

**TLP: WHITE**

TLP: WHITE

---

<sup>1</sup> President of the United States. Executive Order 13873—Securing the Information and Communications Technology and Services Supply Chain. May 15, 2019. <https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain>. Accessed on January 16, 2020.

<sup>2</sup> DHS/CISA/NRMC. December 2018. Supply Chain Risks for Information and Communication Technology. [https://www.cisa.gov/sites/default/files/publications/19\\_0424\\_cisa\\_nrmc\\_supply-chain-risks-for-information-and-communication-technology.pdf](https://www.cisa.gov/sites/default/files/publications/19_0424_cisa_nrmc_supply-chain-risks-for-information-and-communication-technology.pdf). Accessed on January 16, 2020.

<sup>3</sup> NIST. Computer Security Resource Center. "System." 2019. <https://csrc.nist.gov/glossary/term/system>. Accessed on January 16, 2020.

## DHS POINT OF CONTACT

National Risk Management Center  
Cybersecurity and Infrastructure Security Agency  
U.S. Department of Homeland Security  
[NRMC@cisa.dhs.gov](mailto:NRMC@cisa.dhs.gov)

For more information about NRMC, visit [www.cisa.gov/national-risk-management](http://www.cisa.gov/national-risk-management).

PDM19058

TLP: WHITE



# EXHIBIT 22



# United States Strategic Approach to the People's Republic of China

## Introduction

Since the United States and the People's Republic of China (PRC) established diplomatic relations in 1979, United States policy toward the PRC was largely premised on a hope that deepening engagement would spur fundamental economic and political opening in the PRC and lead to its emergence as a constructive and responsible global stakeholder, with a more open society. More than 40 years later, it has become evident that this approach underestimated the will of the Chinese Communist Party (CCP) to constrain the scope of economic and political reform in China. Over the past two decades, reforms have slowed, stalled, or reversed. The PRC's rapid economic development and increased engagement with the world did not lead to convergence with the citizen-centric, free and open order as the United States had hoped. The CCP has chosen instead to exploit the free and open rules-based order and attempt to reshape the international system in its favor. Beijing openly acknowledges that it seeks to transform the international order to align with CCP interests and ideology. The CCP's expanding use of economic, political, and military power to compel acquiescence from nation states harms vital American interests and undermines the sovereignty and dignity of countries and individuals around the world.

To respond to Beijing's challenge, the Administration has adopted a competitive approach to the PRC, based on a clear-eyed assessment of the CCP's intentions and actions, a reappraisal of the United States' many strategic advantages and shortfalls, and a tolerance of greater bilateral friction. Our approach is not premised on determining a particular end state for China. Rather, our goal is to protect United States vital national interests, as articulated in the four pillars of the 2017 *National Security Strategy of the United States of America* (NSS). We aim to: (1) protect the American people, homeland, and way of life; (2) promote American prosperity; (3) preserve peace through strength; and (4) advance American influence.

Our competitive approach to the PRC has two objectives: first, to improve the resiliency of our institutions, alliances, and partnerships to prevail against the challenges the PRC presents; and second, to compel Beijing to cease or reduce actions harmful to the United States' vital, national interests and those of our allies and partners. Even as we compete with the PRC, we welcome cooperation where our interests align. Competition need not lead to confrontation or conflict. The United States has a deep and abiding respect for the Chinese people and enjoys longstanding ties to the country. We do not seek to contain China's development, nor do we wish to disengage from the Chinese people. The United States expects to engage in fair competition with the PRC, whereby both of our nations, businesses, and individuals can enjoy security and prosperity.

Prevailing in strategic competition with the PRC requires cooperative engagement with multiple stakeholders, and the Administration is committed to building partnerships to

protect our shared interests and values. Vital partners of this Administration include the Congress, state and local governments, the private sector, civil society, and academia. The Congress has been speaking out through hearings, statements, and reports that shed light on the CCP's malign behavior. The Congress also provides legal authorities and resources for the United States Government to take the actions to achieve our strategic objectives. The Administration also recognizes the steps allies and partners have taken to develop more clear-eyed and robust approaches toward the PRC, including the European Union's publication in March 2019 of *EU-China: A Strategic Outlook*, among others.

The United States is also building cooperative partnerships and developing positive alternatives with foreign allies, partners, and international organizations to support the shared principles of a free and open order. Specific to the Indo-Pacific region, many of these initiatives are described in documents such as the Department of Defense June 2019 *Indo-Pacific Strategy Report* and the Department of State November 2019 report on *A Free and Open Indo-Pacific: Advancing a Shared Vision*. The United States is working in concert with mutually aligned visions and approaches such as the Association of Southeast Asian Nation's *Outlook on the Indo-Pacific*, Japan's free and open Indo-Pacific vision, India's Security and Growth for All in the Region policy, Australia's Indo-Pacific concept, the Republic of Korea's New Southern Policy, and Taiwan's New Southbound Policy.

This report does not attempt to detail the comprehensive range of actions and policy initiatives the Administration is carrying out across the globe as part of our strategic competition. Rather, this report focuses on the implementation of the NSS as it applies most directly to the PRC.

## Challenges

The PRC today poses numerous challenges to United States national interests.

### 1. Economic Challenges

Beijing's poor record of following through on economic reform commitments and its extensive use of state-driven protectionist policies and practices harm United States companies and workers, distort global markets, violate international norms, and pollute the environment. When the PRC acceded to the World Trade Organization (WTO) in 2001, Beijing agreed to embrace the WTO's open market-oriented approach and embed these principles in its trading system and institutions. WTO members expected China to continue on its path of economic reform and transform itself into a market-oriented economy and trade regime.

These hopes were not realized. Beijing did not internalize the norms and practices of competition-based trade and investment, and instead exploited the benefits of WTO membership to become the world's largest exporter, while systematically protecting its domestic markets. Beijing's economic policies have led to massive industrial overcapacity that distorts global prices and allows China to expand global market share at the expense of

competitors operating without the unfair advantages that Beijing provides to its firms. The PRC retains its non-market economic structure and state-led, mercantilist approach to trade and investment. Political reforms have likewise atrophied and gone into reverse, and distinctions between the government and the party are eroding. General Secretary Xi's decision to remove presidential term limits, effectively extending his tenure indefinitely, epitomized these trends.

In his 2018 *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974*, the United States Trade Representative (USTR) determined that numerous acts, policies, and practices of the PRC government were unreasonable or discriminatory, and burden or restrict United States commerce. Based on a rigorous investigation, USTR found that the PRC: (1) requires or pressures United States companies to transfer their technology to Chinese entities; (2) places substantial restrictions on United States companies' ability to license their technology on market terms; (3) directs and unfairly facilitates acquisition of United States companies and assets by domestic firms to obtain cutting edge technologies; and (4) conducts and supports unauthorized cyber intrusions into United States companies' networks to access sensitive information and trade secrets.

The list of Beijing's commitments to cease its predatory economic practices is littered with broken and empty promises. In 2015, Beijing promised that it would stop government-directed cyber-enabled theft of trade secrets for commercial gain, reiterating that same promise in 2017 and 2018. Later in 2018, the United States and a dozen other countries attributed global computer intrusion campaigns, targeting intellectual property and confidential business information, to operators affiliated with the PRC's Ministry of State Security – a contravention of Beijing's 2015 commitment. Since the 1980s, Beijing has signed multiple international agreements to protect intellectual property. Despite this, more than 63 percent of the world's counterfeits originate in China, inflicting hundreds of billions of dollars of damage on legitimate businesses around the world.

While Beijing acknowledges that China is now a "mature economy," the PRC continues to argue in its dealings with international bodies, including the WTO, that it is still a "developing country." Despite being the top importer of high technology products and ranking second only to the United States in terms of gross domestic product, defense spending, and outward investment, China self-designates as a developing country to justify policies and practices that systematically distort multiple sectors globally, harming the United States and other countries.

One Belt One Road (OBOR) is Beijing's umbrella term to describe a variety of initiatives, many of which appear designed to reshape international norms, standards, and networks to advance Beijing's global interests and vision, while also serving China's domestic economic requirements. Through OBOR and other initiatives, the PRC is expanding the use of Chinese industrial standards in key technology sectors, part of an effort to strengthen its own companies' position in the global marketplace at the expense of non-Chinese firms. Projects that Beijing has labeled OBOR include: transportation, information and communications technology and energy infrastructure; industrial parks; media collaboration; science and

technology exchanges; programs on culture and religion; and even military and security cooperation. Beijing is also seeking to arbitrate OBOR-related commercial disputes through its own specialized courts, which answer to the CCP. The United States welcomes contributions by China to sustainable, high-quality development that accords with international best practices, but OBOR projects frequently operate well outside of these standards and are characterized by poor quality, corruption, environmental degradation, a lack of public oversight or community involvement, opaque loans, and contracts generating or exacerbating governance and fiscal problems in host nations.

Given Beijing's increasing use of economic leverage to extract political concessions from or exact retribution against other countries, the United States judges that Beijing will attempt to convert OBOR projects into undue political influence and military access. Beijing uses a combination of threat and inducement to pressure governments, elites, corporations, think tanks, and others – often in an opaque manner – to toe the CCP line and censor free expression. Beijing has restricted trade and tourism with Australia, Canada, South Korea, Japan, Norway, the Philippines, and others, and has detained Canadian citizens, in an effort to interfere in these countries' internal political and judicial processes. After the Dalai Lama visited Mongolia in 2016, the PRC government imposed new tariffs on land-locked Mongolia's mineral exports passing through China, temporarily paralyzing Mongolia's economy.

Beijing seeks global recognition for its environmental efforts and claims to promote “green development.” China, however, has been the world's largest greenhouse gas emitter by a wide margin for more than a decade. Beijing has put forward vague and unenforceable emissions reduction commitments that allow China's emissions to keep growing until “around 2030.” China's planned growing emissions will outweigh the reductions from the rest of the world combined. Chinese firms also export polluting coal-fired power plants to developing countries by the hundreds. The PRC is also the world's largest source of marine plastic pollution, discharging over 3.5 million metric tons into the ocean each year. The PRC ranks first in the world for illegal, unreported, and unregulated fishing in coastal nations' waters around the world, threatening local economies and harming the marine environment. Chinese leaders' unwillingness to rein in these globally harmful practices does not match their rhetorical promises of environmental stewardship.

## 2. Challenges to Our Values

The CCP promotes globally a value proposition that challenges the bedrock American belief in the unalienable right of every person to life, liberty, and the pursuit of happiness. Under the current generation of leadership, the CCP has accelerated its efforts to portray its governance system as functioning better than those of what it refers to as “developed, western countries.” Beijing is clear that it sees itself as engaged in an ideological competition with the West. In 2013, General Secretary Xi called on the CCP to prepare for a “long-term period of cooperation and conflict” between two competing systems and declared that “capitalism is bound to die out and socialism is bound to win.”



The CCP aims to make China a “global leader in terms of comprehensive national power and international influence,” as General Secretary Xi expressed in 2017, by strengthening what it refers to as “the system of socialism with Chinese characteristics.” This system is rooted in Beijing’s interpretation of Marxist-Leninist ideology and combines a nationalistic, single-party dictatorship; a state-directed economy; deployment of science and technology in the service of the state; and the subordination of individual rights to serve CCP ends. This runs counter to principles shared by the United States and many likeminded countries of representative government, free enterprise, and the inherent dignity and worth of every individual.

Internationally, the CCP promotes General Secretary Xi’s vision for global governance under the banner of “building a community of common destiny for mankind.” Beijing’s efforts to compel ideological conformity at home, however, present an unsettling picture of what a CCP-led “community” looks like in practice: (1) an anticorruption campaign that has purged political opposition; (2) unjust prosecutions of bloggers, activists, and lawyers; (3) algorithmically determined arrests of ethnic and religious minorities; (4) stringent controls over and censorship of information, media, universities, businesses, and non-governmental organizations; (5) surveillance and social credit scoring of citizens, corporations, and organizations; and (6) and arbitrary detention, torture, and abuse of people perceived to be dissidents. In a stark example of domestic conformity, local officials publicized a book burning event at a community library to demonstrate their ideological alignment to “Xi Jinping Thought.”

One disastrous outgrowth of such an approach to governance is Beijing’s policies in Xinjiang, where since 2017, authorities have detained more than a million Uighurs and members of other ethnic and religious minority groups in indoctrination camps, where many endure forced labor, ideological indoctrination, and physical and psychological abuse. Outside these camps, the regime has instituted a police state employing emerging technologies such as artificial intelligence and biogenetics to monitor ethnic minorities’ activities to ensure allegiance to the CCP. Widespread religious persecution – of Christians, Tibetan Buddhists, Muslims, and members of Falun Gong – includes the demolition and desecration of places of worship, arrests of peaceful believers, forced renunciations of faith, and prohibitions on raising children in traditions of faith.

The CCP’s campaign to compel ideological conformity does not stop at China’s borders. In recent years, Beijing has intervened in sovereign nations’ internal affairs to engineer consent for its policies. PRC authorities have attempted to extend CCP influence over discourse and behavior around the world, with recent examples including companies and sports teams in the United States and the United Kingdom and politicians in Australia and Europe. PRC actors are exporting the tools of the CCP’s techno-authoritarian model to countries around the world, enabling authoritarian states to exert control over their citizens and surveil opposition, training foreign partners in propaganda and censorship techniques, and using bulk data collection to shape public sentiment.

China’s party-state controls the world’s most heavily resourced set of propaganda tools. Beijing communicates its narrative through state-run television, print, radio, and online

organizations whose presence is proliferating in the United States and around the world. The CCP often conceals its investments in foreign media entities. In 2015, China Radio International was revealed to control 33 radio stations in 14 countries via shell entities, and to subsidize multiple intermediaries through providing free, pro-Beijing content.

Beyond the media, the CCP uses a range of actors to advance its interests in the United States and other open democracies. CCP United Front organizations and agents target businesses, universities, think tanks, scholars, journalists, and local, state, and Federal officials in the United States and around the world, attempting to influence discourse and restrict external influence inside the PRC.

Beijing regularly attempts to compel or persuade Chinese nationals and others to undertake a range of malign behaviors that threaten United States national and economic security, and undermine academic freedom and the integrity of the United States research and development enterprise. These behaviors include misappropriation of technology and intellectual property, failure to appropriately disclose relationships with foreign government sponsored entities, breaches of contract and confidentiality, and manipulation of processes for fair and merit-based allocation of Federal research and development funding. Beijing also attempts to compel Chinese nationals to report on and threaten fellow Chinese students, protest against events that run counter to Beijing's political narrative, and otherwise restrict the academic freedom that is the hallmark and strength of the American education system.

PRC media entities, journalists, academics, and diplomats are free to operate in the United States, but Beijing denies reciprocal access to American counterpart institutions and officials. The PRC government routinely denies United States officials, including the United States Ambassador to the PRC, access to Department of State-funded American Cultural Centers, which are hosted in Chinese universities to share American culture with the Chinese people. Foreign reporters working in the PRC often face harassment and intimidation.

### 3. Security Challenges

As China has grown in strength, so has the willingness and capacity of the CCP to employ intimidation and coercion in its attempts to eliminate perceived threats to its interests and advance its strategic objectives globally. Beijing's actions belie Chinese leaders' proclamations that they oppose the threat or use of force, do not intervene in other countries' internal affairs, or are committed to resolving disputes through peaceful dialogue. Beijing contradicts its rhetoric and flouts its commitments to its neighbors by engaging in provocative and coercive military and paramilitary activities in the Yellow Sea, the East and South China Seas, the Taiwan Strait, and Sino-Indian border areas.

In May 2019, the Department of Defense issued its annual report to the Congress, *Military and Security Developments Involving the PRC*, assessing current and future trajectories of China's military-technological development, security and military strategies, and People's Liberation Army (PLA) organizational and operational concepts. In July 2019, the PRC

Minister of Defense publicly acknowledged that OBOR is linked to the PRC's aspirational expansion of PLA presence overseas, including locations such as the Pacific Islands and the Caribbean.

Beijing's military buildup threatens United States and allied national security interests and poses complex challenges for global commerce and supply chains. Beijing's Military-Civil Fusion (MCF) strategy gives the PLA unfettered access into civil entities developing and acquiring advanced technologies, including state-owned and private firms, universities, and research programs. Through non-transparent MCF linkages, United States and other foreign companies are unwittingly feeding dual-use technologies into PRC military research and development programs, strengthening the CCP's coercive ability to suppress domestic opposition and threaten foreign countries, including United States allies and partners.

The PRC's attempts to dominate the global information and communications technology industry through unfair practices is reflected in discriminatory regulations like the PRC National Cyber Security Law, which requires companies to comply with Chinese data localization measures that enable CCP access to foreign data. Other PRC laws compel companies like Huawei and ZTE to cooperate with Chinese security services, even when they do business abroad, creating security vulnerabilities for foreign countries and enterprises utilizing Chinese vendors' equipment and services.

Beijing refuses to honor its commitment to provide travel documents for Chinese citizens with orders of removal from the United States in a timely and consistent manner, effectively blocking their removals from our country and creating security risks for American communities. In addition, the PRC's violations of our bilateral consular treaty puts United States citizens at risk in China, with many Americans detrimentally affected by the PRC government's coercive exit bans and wrongful detentions.

## Approach

The NSS demands that the United States "rethink the policies of the past two decades – policies based on the assumption that engagement with rivals and their inclusion in international institutions and global commerce would turn them into benign actors and trustworthy partners. For the most part, this premise turned out to be false. Rival actors use propaganda and other means to try to discredit democracy. They advance anti-Western views and spread false information to create divisions among ourselves, our allies, and our partners."

Guided by a return to principled realism, the United States is responding to the CCP's direct challenge by acknowledging that we are in a strategic competition and protecting our interests appropriately. The principles of the United States' approach to China are articulated both in the NSS and our vision for the Indo-Pacific region – sovereignty, freedom, openness, rule of law, fairness, and reciprocity. United States-China relations do not determine our Indo-Pacific strategy, but rather fall within that strategy and the overarching

NSS. By the same token, our vision of a free and open Indo-Pacific region does not exclude China.

The United States holds the PRC government to the same standards and principles that apply to all nations. We believe this is the treatment that the people of China want and deserve from their own government and from the international community. Given the strategic choices China's leadership is making, the United States now acknowledges and accepts the relationship with the PRC as the CCP has always framed it internally: one of great power competition.

United States policies are not premised on an attempt to change the PRC's domestic governance model, nor do they make concessions to the CCP's narratives of exceptionalism and victimhood. Rather, United States policies are designed to protect our interests and empower our institutions to withstand the CCP's malign behavior and collateral damage from the PRC's internal governance problems. Whether the PRC eventually converges with the principles of the free and open order can only be determined by the Chinese people themselves. We recognize that Beijing, not Washington, has agency over and responsibility for the PRC government's actions.

The United States rejects CCP attempts at false equivalency between rule of law and rule by law; between counterterrorism and oppression; between representative governance and autocracy; and between market-based competition and state-directed mercantilism. The United States will continue to challenge Beijing's propaganda and false narratives that distort the truth and attempt to demean American values and ideals.

Similarly, the United States does not and will not accommodate Beijing's actions that weaken a free, open, and rules-based international order. We will continue to refute the CCP's narrative that the United States is in strategic retreat or will shirk our international security commitments. The United States will work with our robust network of allies and like-minded partners to resist attacks on our shared norms and values, within our own governance institutions, around the world, and in international organizations.

The American people's generous contributions to China's development are a matter of historical record – just as the Chinese people's remarkable accomplishments in the era of Reform and Opening are undeniable. However, the negative trend lines of Beijing's policies and practices threaten the legacy of the Chinese people and their future position in the world.

Beijing has repeatedly demonstrated that it does not offer compromises in response to American displays of goodwill, and that its actions are not constrained by its prior commitments to respect our interests. As such, the United States responds to the PRC's actions rather than its stated commitments. Moreover, we do not cater to Beijing's demands to create a proper "atmosphere" or "conditions" for dialogue.

Likewise, the United States sees no value in engaging with Beijing for symbolism and pageantry; we instead demand tangible results and constructive outcomes. We acknowledge and respond in kind to Beijing's transactional approach with timely incentives and costs, or

credible threats thereof. When quiet diplomacy proves futile, the United States will increase public pressure on the PRC government and take action to protect United States interests by leveraging proportional costs when necessary.

The PRC government has fallen short of its commitments in many areas including: trade and investment; freedoms of expression and belief; political interference; freedoms of navigation and overflight; cyber and other types of espionage and theft; weapons proliferation; environmental protection; and global health. Agreements with Beijing must include stringent verification and enforcement mechanisms.

We speak candidly with the Chinese people and expect honesty from PRC leaders. In matters of diplomacy, the United States responds appropriately to the CCP's insincere or vague threats, and stands up alongside our allies and partners to resist coercion. Through our continuous and frank engagement, the United States welcomes cooperation by China to expand and work toward shared objectives in ways that benefit the peace, stability, and prosperity of the world. Our approach does not exclude the PRC. The United States stands ready to welcome China's positive contributions.

As the above tenets of our approach imply, competition necessarily includes engagement with the PRC, but our engagements are selective and results-oriented, with each advancing our national interests. We engage with the PRC to negotiate and enforce commitments to ensure fairness and reciprocity; clarify Beijing's intentions to avoid misunderstanding; and resolve disputes to prevent escalation. The United States is committed to maintaining open channels of communication with the PRC to reduce risks and manage crises. We expect the PRC to also keep these channels open and responsive.

## **Implementation**

In accordance with the President's NSS, the political, economic, and security policies outlined in this report seek to protect the American people and homeland, promote American prosperity, preserve peace through strength, and advance a free and open vision abroad. During the first 3 years of the Administration, the United States has taken significant steps in implementing this strategy as it applies to China.

### **1. Protect the American People, the Homeland, and the American Way of Life**

The United States Department of Justice (DOJ)'s China Initiative and Federal Bureau of Investigation are directing resources to identify and prosecute trade secrets theft, hacking, and economic espionage; and increasing efforts to protect against malign foreign investment in United States infrastructure, supply chain threats, and foreign agents seeking to influence American policy. For example, DOJ informed PRC state media company CGTN-America of its obligation to register as a foreign agent as specified under the Foreign Agents Registration Act (FARA), which obligates registrants to disclose their activities to Federal authorities and



appropriately label information materials they distribute. CGTN-America subsequently registered under FARA.

The Administration is also responding to CCP propaganda in the United States by highlighting malign behavior, countering false narratives, and compelling transparency. United States officials, including those from the White House and the Departments of State, Defense, and Justice, are leading efforts to educate the American public about the PRC government's exploitation of our free and open society to push a CCP agenda inimical to United States interests and values. In an effort to achieve reciprocity of access, the Department of State has implemented a policy requiring Chinese diplomats to notify the United States Government before meeting with state and local government officials and academic institutions.

The Administration is raising awareness of and actively combatting Beijing's co-optation and coercion of its own citizens and others in United States academic institutions, beyond traditional espionage and influence efforts. We are working with universities to protect the rights of Chinese students on American campuses, provide information to counter CCP propaganda and disinformation, and ensure an understanding of ethical codes of conduct in an American academic environment.

Chinese students represent the largest cohort of foreign students in the United States today. The United States values the contributions of Chinese students and researchers. As of 2019, the number of Chinese students and researchers in the United States has reached an all-time high, while the number of student visa denials to Chinese applicants has steadily declined. The United States strongly supports the principles of open academic discourse and welcomes international students and researchers conducting legitimate academic pursuits; we are improving processes to screen out the small minority of Chinese applicants who attempt to enter the United States under false pretenses or with malign intent.

In the United States research community, Federal agencies such as the National Institutes of Health and the Department of Energy have updated or clarified regulations and procedures to ensure compliance with applicable standards of conduct and reporting, in order to improve transparency and prevent conflicts of interest. The National Science and Technology Council's Joint Committee on the Research Environment is developing standards for Federally-funded research, and best practices for United States research institutions. The Department of Defense is working to ensure grantees do not also have contracts with China's talent recruitment programs, while also continuing to welcome foreign researchers.

To prevent foreign malign actors from gaining access to United States information networks, the President issued the "Executive Order on Securing the Information and Communications Technology and Services Supply Chain" and the "Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector." The implementation of these Executive Orders will prevent certain companies associated with or answering to the intelligence and security apparatus of foreign adversaries from, for example, readily accessing the private and sensitive information of the United States Government, the United States private sector, and

individual Americans. To ensure protection of our information worldwide, including sensitive military and intelligence data, the United States is actively engaging with our allies and partners, including in multilateral fora, to promote a set of common standards for secure, resilient, and trusted communications platforms that underpin the global information economy. To compel Beijing to adhere to norms of responsible state behavior, the United States is working with allies and like-minded partners to attribute and otherwise deter malicious cyber activities.

The Administration is implementing the Foreign Investment Risk Review Modernization Act to update and strengthen the capacity of the Committee on Foreign Investment in the United States (CFIUS) to address growing national security concerns over foreign exploitation of investment structures, which previously fell outside CFIUS jurisdiction. This includes preventing Chinese companies from exploiting access to United States innovation through minority investments in order to modernize the Chinese military. The United States has updated its export control regulations, particularly in light of Beijing's whole-of-society MCF strategy and its efforts to acquire advanced technologies related to hypersonics, quantum computing, artificial intelligence, biotechnology, and other emerging and foundational technologies. We are also engaging allies and partners to develop their own foreign investment screening mechanisms, and to update and implement export controls collaboratively through multilateral regimes and other forums.

The United States Government is also taking concrete actions to protect the American consumer from counterfeit and substandard products. Between 2017 and 2018, the United States Department of Homeland Security seized more than 59,000 shipments of counterfeit goods, produced in the PRC, valued at more than \$2.1 billion. This represents five times the total shipments and value seized from all other foreign countries combined.

In addition to falsely branded apparel, footwear, handbags, and watches, United States Customs and Border Protection intercepted three shipments containing 53,000 illegal Chinese gun parts and electronics that could have compromised the security and privacy of American businesses and consumers. United States law enforcement agencies are also targeting counterfeit pharmaceuticals and cosmetics originating from China, which have been found to contain high levels of contaminants, including bacteria and animal waste that pose a danger to American consumers.

The United States is working with Chinese authorities to stem the deadly flow of illicit Chinese fentanyl from the PRC to the United States. In December 2018, the President secured a commitment from his Chinese counterpart to control all forms of fentanyl in the PRC. With the Chinese regulatory regime in place since May 2019, United States and PRC law enforcement agencies are sharing intelligence and coordinating to set conditions for enforcement actions that will deter Chinese drug producers and traffickers. The United States is also working with China's postal agencies to improve tracking of small parcels for law enforcement purposes.

## 2. Promote American Prosperity

In response to the PRC's documented unfair and abusive trade practices and industrial policies, the Administration is taking strong actions to protect American businesses, workers, and farmers, and to put an end to Beijing's practices that have contributed to a hollowing-out of the United States manufacturing base. The United States is committed to rebalancing the United States-China economic relationship. Our whole-of-government approach supports fair trade and advances United States competitiveness, promotes United States exports, and breaks down unjust barriers to United States trade and investment. Having failed since 2003 to persuade Beijing to adhere to its economic commitments through regular, high-level dialogues, the United States is confronting China's market-distorting forced technology transfer and intellectual property practices by imposing costs in the form of tariffs levied on Chinese goods coming into the United States. Those tariffs will remain in place until a fair Phase Two trade deal is agreed to by the United States and the PRC.

In response to Beijing's repeated failure to reduce or eliminate its market-distorting subsidies and overcapacity, the United States imposed tariffs to protect our strategically important steel and aluminum industries. For those unfair Chinese trade practices that are subject to dispute settlement at the WTO, the United States continues to pursue and win multiple cases. Finally, to crack down on China's dumping and subsidies across a broad range of industries, the Department of Commerce is making greater utility of United States antidumping and countervailing duties laws than in past administrations.

In January 2020, the United States and the PRC signed Phase One of an economic and trade agreement that requires structural reforms and other changes to China's economic and trade regime, addressing several longstanding United States concerns. The agreement prohibits the PRC from forcing or pressuring foreign companies to transfer their technology as a condition for doing business in China; strengthens protection and enforcement of intellectual property in China in all key areas; creates new market opportunities in China for United States agriculture and financial services by addressing policy barriers; and addresses longstanding, unfair currency practices. The agreement also establishes a strong dispute resolution mechanism that ensures prompt and effective implementation and enforcement. By addressing structural barriers to trade and making the commitments fully enforceable, the Phase One agreement will expand United States exports to China. As part of this agreement, the PRC committed over the next 2 years to increase imports of United States goods and services by no less than \$200 billion in four broad categories: manufactured goods, agriculture, energy, and services. This agreement marks critical progress toward a more balanced trade relationship and a more level playing field for American workers and companies.

Domestically, the Administration is taking steps to strengthen the United States economy and promote economic sectors of the future, such as 5G technology, through tax reforms and a robust deregulatory agenda. The President's "Executive Order on Maintaining American Leadership in Artificial Intelligence" is an example of a United States Government initiative

to promote investment and collaboration to ensure the United States continues to lead in innovation and setting standards for a growing industry.

Together with other likeminded nations, the United States promotes an economic vision based on principles of sovereignty, free markets, and sustainable development. Alongside the European Union and Japan, the United States is engaged in a robust trilateral process to develop disciplines for state-owned enterprises, industrial subsidies, and forced technology transfers. We will also continue to work with our allies and partners to ensure that discriminatory industrial standards do not become global standards. As the world's most valuable consumer market, largest source of foreign direct investment, and leading wellspring of global technological innovation, the United States engages extensively with allies and partners to evaluate shared challenges and coordinate effective responses to ensure continued peace and prosperity. We work closely with United States companies to build their competitiveness at home and abroad while fostering sustainable development through programs such as Prosper Africa, *America Crece* in Latin America and the Caribbean, and Enhancing Development and Growth through Energy in the Indo-Pacific region.

### 3. Preserve Peace through Strength

The 2018 National Defense Strategy (NDS) prioritizes long-term competition with China and emphasizes modernization and partnerships to counter the PLA's technological advancements, force development, and growing international presence and assertiveness. As described in the Nuclear Posture Review, the Administration is prioritizing the modernization of the nuclear triad, including the development of supplementary capabilities designed to deter Beijing from using its weapons of mass destruction or conducting other strategic attacks. Meanwhile, the United States continues to urge China's leaders to come to the table and begin arms control and strategic risk reduction discussions as a nuclear power with a modern and growing nuclear arsenal and the world's largest collection of intermediate range delivery systems. The United States believes it is in the interest of all nations to improve Beijing's transparency, prevent miscalculations, and avoid costly arms buildups.

The Department of Defense is moving quickly to deploy hypersonic platforms, increasing investments in cyber and space capabilities, and developing more lethal fires based on resilient, adaptive, and cost-effective platforms. Together, these capabilities are intended to deter and counter Beijing's growing ambitions and the PLA's drive toward technological parity and superiority.

As part of our worldwide freedom of navigation operations program, the United States is pushing back on Beijing's hegemonic assertions and excessive claims. The United States military will continue to exercise the right to navigate and operate wherever international law allows, including in the South China Sea. We are speaking up for regional allies and partners, and providing security assistance to help them build capacity to withstand Beijing's attempts to use its military, paramilitary, and law enforcement forces to coerce and prevail in disputes. In 2018, the United States military withdrew the invitation for the PLA to

participate in the biennial Rim of the Pacific exercise due to Beijing's deployment of advanced missile systems onto manmade features in the South China Sea.

Stronger alliances and partnerships are a cornerstone of the NDS. The United States is building partner capacity and deepening interoperability to develop a combat-credible forward operating presence, fully integrated with allies and partners to deter and deny PRC aggression. The Administration's Conventional Arms Transfer policy aims to promote United States arms sales and accelerate the transformation of partner military capabilities in a strategic and complementary manner. In June 2019, the Department of Defense released its first *Indo-Pacific Strategy Report*, articulating the Department's implementation of the NDS and our whole-of-government strategy for the Indo-Pacific region.

The United States will continue to maintain strong unofficial relations with Taiwan in accordance with our "One China" policy, based on the Taiwan Relations Act and the three United States-PRC Joint Communiques. The United States maintains that any resolution of cross-Straits differences must be peaceful and according to the will of the people on both sides, without resorting to threat or coercion. Beijing's failure to honor its commitments under the communiques, as demonstrated by its massive military buildup, compels the United States to continue to assist the Taiwan military in maintaining a credible self-defense, which deters aggression and helps to ensure peace and stability in the region. In a 1982 memorandum, President Ronald Reagan insisted "that the quantity and quality of the arms provided Taiwan be conditioned entirely on the threat posed by the PRC." In 2019, the United States approved more than \$10 billion of arms sales to Taiwan.

The United States remains committed to maintaining a constructive, results-oriented relationship with the PRC. The United States conducts defense contacts and exchanges with the PRC to communicate strategic intent; prevent and manage crises; reduce the risks of miscalculation and misunderstanding that could escalate into conflict; and cooperate in areas of shared interest. The United States military engages with the PLA to develop effective crisis communication mechanisms, including responsive channels for de-escalation in unplanned scenarios.

#### 4. Advance American Influence

For the past seven decades, the free and open international order has provided the stability to allow sovereign, independent states to flourish and contribute to unprecedented global economic growth. As a large, developed country and a major beneficiary of this order, the PRC should help guarantee freedom and openness for other nations around the globe. When Beijing instead promotes or abets authoritarianism, self-censorship, corruption, mercantilist economics, and intolerance of ethnic and religious diversity, the United States leads international efforts to resist and counter these malign activities.

In 2018 and 2019, the Secretary of State hosted the first two gatherings of the Ministerial to Advance Religious Freedom. Along with the President's unprecedented Global Call to Protect Religious Freedom during the United Nations General Assembly (UNGA) in September 2019, these events brought together global leaders to address religious persecution around the



world. During both ministerials, the United States and partner countries released joint statements calling on the PRC government to respect the rights of Uighur and other Turkic Muslims, Tibetan Buddhists, Christians, and Falun Gong adherents, all of whom face repression and persecution in China. In February 2020, the Department of State launched the first ever International Religious Freedom Alliance with 25 likeminded partners to defend the right of every person to worship without fear. The President met with Chinese dissidents and survivors on the margins of the 2019 Ministerial, and he shared the stage during UNGA with victims of religious persecution from China. The United States also continues to support human rights defenders and independent civil society working in or on China.

In October 2019 at the United Nations in New York, the United States joined likeminded nations in condemning Beijing's ongoing human rights violations and other repressive policies in Xinjiang that threaten international peace and security. The latter event followed United States Government actions to stop United States exports to select Chinese government agencies and surveillance technology companies complicit in the Xinjiang human rights abuses and to deny United States visas for Chinese officials, and their family members, responsible for violating Beijing's international human rights commitments. The United States has also begun actions to block imports of Chinese goods produced using forced labor in Xinjiang.

The United States will continue to take a principled stand against the use of our technology to support China's military and its technology-enabled authoritarianism, working in conjunction with likeminded allies and partners. In doing so, we will implement policies that keep pace with rapid technological change and PRC efforts to blend civil and military uses and compel companies to support China's security and intelligence services.

These efforts demonstrate United States commitment to the fundamental values and norms that have served as the foundation of the international system since the end of the Second World War. While the United States has no desire to interfere in the PRC's internal affairs, Washington will continue to be candid when Beijing strays from its international commitments and responsible behavior, especially when United States interests are at stake. For example, the United States has significant interests in the future of Hong Kong. Approximately 85,000 United States citizens and more than 1,300 United States businesses reside in Hong Kong. The President, the Vice President, and the Secretary of State have repeatedly called on Beijing to honor the 1984 Sino-British Joint Declaration and preserve Hong Kong's high degree of autonomy, rule of law, and democratic freedoms, which enable Hong Kong to remain a successful hub of international business and finance.

The United States is expanding its role as an Indo-Pacific nation that promotes free enterprise and democratic governance. In November 2019, the United States, Japan, and Australia launched the Blue Dot Network to promote transparently-financed, high quality infrastructure through private sector-led development around the world, which will add to the nearly 1 trillion dollars of United States direct investment in the Indo-Pacific region alone. At the same time, the Department of State issued a detailed progress report on the

implementation of our whole-of-government strategy for the Indo-Pacific region:  
*A Free and Open Indo-Pacific: Advancing a Shared Vision.*

## Conclusion

The Administration's approach to the PRC reflects a fundamental reevaluation of how the United States understands and responds to the leaders of the world's most populous country and second largest national economy. The United States recognizes the long-term strategic competition between our two systems. Through a whole-of-government approach and guided by a return to principled realism, as articulated by the NSS, the United States Government will continue to protect American interests and advance American influence. At the same time, we remain open to constructive, results-oriented engagement and cooperation from China where our interests align. We continue to engage with PRC leaders in a respectful yet clear-eyed manner, challenging Beijing to uphold its commitments.

# EXHIBIT 23



---

# WE CHAT, THEY WATCH

How international users unwittingly build up WeChat's Chinese censorship apparatus

By Jeffrey Knockel, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert

MAY 7, 2020

RESEARCH REPORT #127

---



---

## Copyright

© The Citizen Lab



Licensed under the Creative Commons BY-SA 4.0 (Attribution-ShareAlike licence). Electronic version first published in 2020 by the Citizen Lab. This work can be accessed through <https://citizenlab.ca/2020/05/we-chat-they-watch/>.

Document Version: 1.0

The Creative Commons Attribution-ShareAlike 4.0 license under which this report is licensed lets you freely copy, distribute, remix, transform, and build on it, as long as you:

- give appropriate credit;
- indicate whether you made changes; and
- use and link to the same CC BY-SA 4.0 licence.

However, any rights in excerpts reproduced in this report remain with their respective authors; and any rights in brand and product names and associated logos remain with their respective owners. Uses of these that are protected by copyright or trademark rights require the rightsholder's prior written agreement.

---

## Suggested Citation

Jeffrey Knockel, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert "We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus," Citizen Lab Research Report No. 127, University of Toronto, May 2020.



---

## Acknowledgements

We would like to thank Abbas Razaghpanah for valuable peer review and Mari Zhou for graphics design. We would also like to thank Miles Kenyon, Masashi Crete-Nishihata for editing and comments.

This project was supported by Open Society Foundations.

---

## About the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

**The Citizen Lab** is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

---

# Contents

<b>Key Findings</b>	<b>5</b>
<b>Introduction</b>	<b>5</b>
<b>2.1 Background</b>	<b>11</b>
<b>2.2 Statistical Experiment</b>	<b>12</b>
2.2.1 Methodology	12
2.2.2 Experimental Setup	17
2.2.3 Results	18
<b>2.3 Collision Experiment</b>	<b>19</b>
2.3.1 Methodology	19
2.3.2 Experimental Setup	21
2.3.3 Results	21
<b>2.4 Retention Experiment</b>	<b>21</b>
2.4.1 Methodology	22
2.4.2 Experimental setup	22
2.4.3 Results	22
<b>2.5 Summary</b>	<b>23</b>
<b>Part 3 - Policy Assessment</b>	<b>24</b>
<b>3.1 Methodology</b>	<b>25</b>
3.1.1 Obtaining Relevant Public-Facing Policies	25
3.1.2 Structured Question Set	26
3.1.3 Communication with Data Protection Office	28
<b>3.2 Results</b>	<b>28</b>
3.2.1 General Policy Questions	28
3.2.2 Engaging with Company Through Questions or Complaints	30
3.2.3 Capture of Personal Information	31
3.2.4 Disclosures of Information	33
3.2.5 Behaviours of Hashing and Blocking User-Generated Content	35
3.2.6 Data Protection Office Non-Response	36
<b>3.3 Discussion</b>	<b>37</b>
3.3.1 Enabling Content Surveillance	38
3.3.2 Enabling Content or Metadata Disclosure	40
<b>Part 4. Data Access Request Assessment</b>	<b>41</b>
<b>4.1 Methodology</b>	<b>42</b>
4.1.1 Round One Data Access Request	43
4.1.2 Round Two Data Access Request	43
<b>4.2 Data</b>	<b>44</b>
<b>4.3 Discussion</b>	<b>46</b>
<b>Part 5 - Conclusion</b>	<b>47</b>
<b>Appendix</b>	<b>50</b>
<b>A. Letter to WeChat Data Protection Office</b>	<b>50</b>
<b>B. PIPEDA Data Request to Shenzhen Tencent Computer Systems Company Limited</b>	<b>54</b>
<b>C. PIPEDA Data Request to Tencent International Service Pte. Ltd., #1</b>	<b>56</b>
<b>D. PIPEDA Data Request to Tencent International Service Pte. Ltd., #2</b>	<b>59</b>

---

## Key Findings

- We present results from technical experiments which reveal that WeChat communications conducted entirely among non-China-registered accounts are subject to pervasive content surveillance that was previously thought to be exclusively reserved for China-registered accounts.
- Documents and images transmitted entirely among non-China-registered accounts undergo content surveillance wherein these files are analyzed for content that is politically sensitive in China.
- Upon analysis, files deemed politically sensitive are used to invisibly train and build up WeChat's Chinese political censorship system.
- From public information, it is unclear how Tencent uses non-Chinese-registered users' data to enable content blocking or which policy rationale permits the sharing of data used for blocking between international and China regions of WeChat.
- Tencent's responses to data access requests failed to clarify how data from international users is used to enable political censorship of the platform in China.

## Introduction

A significant body of research over the past decade has shown how online platforms in China are routinely censored to comply with government regulations. As Chinese companies grow into markets beyond China, their activities are also coming under scrutiny. For example, TikTok, a video-based social media company, has been accused of censoring content on its platform that would be sensitive in China.<sup>1</sup> Grindr, a Chinese-owned online dating platform for gay, bi, trans, and queer people,

1 Greg Roumeliotis, Yingzhi Yang, Echo Wang and Alexandra Alper, (2019), "US opens national security investigation into TikTok," *CNBC* (November 1, 2019) <<https://www.cnn.com/2019/11/01/us-to-investigate-tiktok-over-national-security-concerns-sources-say.html>>; Raymond Zhong, (2019), "TikTok's Chief Is on a Mission to Prove It's Not a Menace," *New York Times* (November 18, 2019) <<https://www.nytimes.com/2019/11/18/technology/tiktok-alex-zhu-interview.html>>; William Feuer, (2019), "TikTok says it doesn't censor content, but a user was just locked out after a viral post criticizing China," *CNBC* (November 26, 2019) <<https://www.cnn.com/2019/11/26/tiktok-says-it-doesnt-censor-but-a-user-who-criticized-china-was-locked-out.html>>; Drew Harwell and Tony Romm, (2019), "Inside TikTok: A culture clash where U.S. views about censorship often were overridden by the Chinese bosses," *Washington Post* (November 5, 2019) <<https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/>>.



fell under suspicion that it could be used to monitor, track, or otherwise endanger American users.<sup>2</sup>

WeChat is the most popular social media platform in China and third in the world.<sup>3</sup> While the platform dominates the market in China, it also has made efforts to internationalize and attract users globally. Like any other Internet platform operating in China, WeChat is expected to follow rules and regulations from Chinese authorities around prohibited content. Previous Citizen Lab research shows the balancing act WeChat must maintain as it attempts to keep within government red lines in China and attract users internationally. WeChat implements censorship for users with accounts registered to mainland China phone numbers. This censorship is done without notification to users and is dynamically updated, often in response to current events.<sup>4</sup>

In previous work, there was no evidence that these censorship features affected users with accounts that are not registered to China-based phone numbers. These users could send and receive messages that users with China-registered accounts could not. In this report, we show that documents and images shared among non-China-registered accounts are subject to content surveillance and are used to build up the database WeChat uses to censor China-registered accounts.<sup>5</sup> By engaging in analysis of WeChat privacy agreements and policy documents, we find that the company provides no clear reference or explanation of the content surveillance features and therefore absent performing their own technical experiments, users cannot determine if, and why, content surveillance was being applied. Consequently, non-China-based users who send sensitive content over WeChat may be unwittingly contributing to political censorship in China.

2 Georgia Well and Kate O’Keeffe, (2019), “U.S. Orders Chinese Firm to Sell Dating App Grindr Over Blackmail Risk,” *Wall Street Journal* (March 27, 2019) <<https://www.wsj.com/articles/u-s-orders-chinese-company-to-sell-grindr-app-11553717942>>; Jacob Rosenberg, (2019), “The Trump Administration Apparently Considers Grindr a National Security Threat. What Is Going On?,” *Mother Jones* (April 4, 2019) <<https://www.motherjones.com/politics/2019/04/the-trump-administration-apparently-considers-grindr-a-national-security-threat-what-is-going-on/>>.

3 Bucher, Birg, (2020), “WhatsApp, WeChat and Facebook Messenger Apps – Global Messenger Usage, Penetration and Statistics,” *Messenger People* <<https://www.messengerpeople.com/global-messenger-usage-statistics/>>.

4 Lotus Ruan, Jeffrey Knockel, Jason Q. Ng, and Masashi Crete-Nishihata. (2016) One App, Two Systems: “One App, Two Systems: How WeChat uses one censorship policy in China and another internationally,” *Citizen Lab*, <<https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/>>.

5 We define surveillance as the focused, systematic and routine attention to personal details for the purposes of influence, management, protection or direction. See: David Lyon (2007), *Surveillance Studies: An Overview*. (Polity Press: 2007) at 14.

The report proceeds as follows:

### **Part 1: Background**

Provides background on WeChat and an overview of previous research on surveillance and censorship on the platform.

### **Part 2: Technical Assessment**

Presents our technical experiments, including the side-channel methods which were used to uncover the surveillance to which non-China-registered accounts are subjected, as well as the findings and discussion emergent from the analysis.

### **Part 3: Policy Assessment**

Presents results from policy analysis, which involved interrogating Tencent's public-facing policy documents and directly contacting the company about how it treated international users' communications content.

### **Part 4: Data Access Request Assessment**

Recounts what we did, and did not, learn from issuing a data access request for our WeChat data, and shows that this method failed to reveal content surveillance on the platform.

### **Part 5: Conclusion**

Provides a brief conclusion, discusses the broad significance of our findings, and provides avenues for future research.

## **Part 1 - Background**

WeChat (*Weixin* 微信 in Chinese) is one of the most popular social media apps in China, with 1.15 billion monthly active users in China and overseas as of late 2019.<sup>6</sup> The application is owned and operated by Tencent, one of China's largest technology companies, and was launched in 2011 as a mobile instant messaging app. Since then, Tencent's WeChat/Weixin Group<sup>7</sup> has developed a variety of communication functionalities in WeChat including instant messaging (e.g., one-to-one private chat, group chat), WeChat Moments (i.e., a functionality that resembles Facebook's Timeline where users can share text-based updates, upload images, and share short videos or articles with their friends), and the Public Account platform

6 Tencent (2019), "Tencent Announces 2019 Third Quarter Results," *Tencent*, <<https://cdc.tencent.com-1258344706.image.myqcloud.com/uploads/2019/11/13/8b98062831f2f28d9c-b4616222a4d3c3.pdf>>.

7 Tencent Holdings Limited has six business groups that oversee different products and aspects of the company. The Weixin Group (WXG) is the one that develops and operates WeChat and related services. Tencent (n.d.), "Get To Know Tencent," *Tencent*, <<https://join.qq.com/business.php>>.



(i.e., a blogging-like platform that allows individual writers as well as businesses to write for general audiences). Forty-five billion messages are reportedly sent using WeChat on a daily basis.<sup>8</sup>

The Chinese market presents unique challenges for Internet platform providers due to laws and regulations that hold companies accountable for the content published or transmitted on their platforms. Companies are expected to invest in human resources and technologies to moderate content and comply with government regulations on content controls. Companies which do not undertake such moderation and compliance activities can be fined or have their business licenses revoked. Meanwhile, China's laws and regulations on content controls are broadly defined, with prohibited topics ranging from "disrupting social order and stability" or "damaging state honor and interests," to crossing "the bottom line of socialism."<sup>9</sup> Previous research has shown that these vaguely defined guidelines often lead companies and individuals alike to engage in self-censorship.<sup>10</sup>

Previous work shows that WeChat conducts pervasive political censorship for users whose accounts operate under WeChat China's terms of service; we refer to these accounts, generally, as China-registered accounts.<sup>11</sup> Accounts which were originally registered to mainland China phone numbers fall under these terms of service, and they remain under them even if the user later links their account to a non-Chinese phone number. Files and communications which are sent to, or from, China-registered accounts are assessed for political sensitivity among other content categories. If the content of the communications is found to be sensitive, it is censored for all China-registered accounts on the platform.

8 Yicai News (2019), "Here Comes WeChat's Big Data [in Chinese]," *Yicai*, <<https://www.yicai.com/news/100095261.html>>.

9 Cyberspace Administration of China (2014), "The Interim Provisions on the Administration of the Development of the Public Information Services of Instant Messaging Tools," *Cyberspace Administration of China* <[https://www.cac.gov.cn/2014-08/07/c\\_1111983456.htm](https://www.cac.gov.cn/2014-08/07/c_1111983456.htm)>.

10 Perry Link (2002), "China: The Anaconda in the Chandelier," *China File* <<http://www.chinafile.com/library/nyrb-china-archive/china-anaconda-chandelier>>.

11 We use the terms WeChat China and WeChat International to distinguish WeChat's China-based and internationally-based operations. We follow Tencent's definition of the scope of its China-based services. That is, WeChat China's technical and policy infrastructures apply to users who "register by binding a mobile number that is made available to you in the People's Republic of China (except for Taiwan, Hong Kong or Macau) (i.e., a contact number that uses international dialing code +86)." WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>.

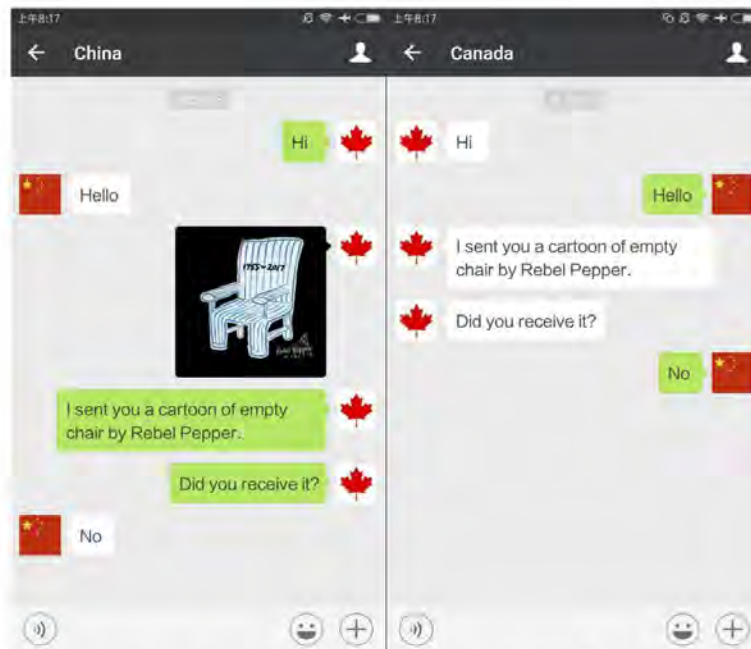


Figure 1: Evidence of image censorship in WeChat's one-to-one chat feature from Citizen Lab testing conducted in July 2017.<sup>12</sup>

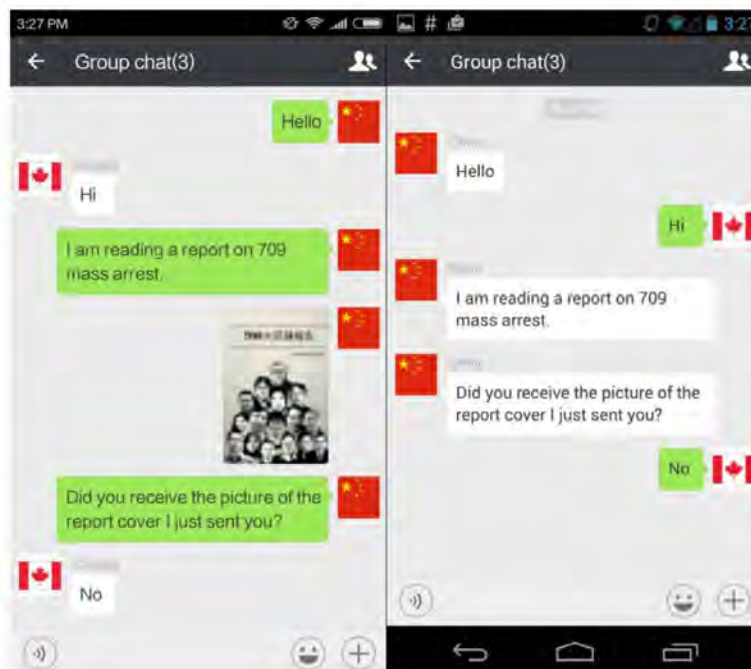


Figure 2: Evidence of image censorship in a WeChat group Chat from Citizen Lab testing conducted in January 2017.<sup>13</sup> A user with a China account (on the left) attempted to send a sensitive image, which was censored.

- 12 Crete-Nishihata, Masashi, Jeffrey Knockel, Blake Miller, Jason Q. Ng, Lotus Ruan, Lokman Tsui, and Ruohan Xiong (2017), "Remembering Liu Xiaobo: Analyzing Censorship of the Death of Liu Xiaobo on WeChat and Weibo," *Citizen Lab* <<https://citizenlab.ca/2017/07/analyzing-censorship-of-the-death-of-liu-xiaobo-on-wechat-and-weibo/>>.
- 13 Ruan, Lotus, Jeffrey Knockel, and Masashi Crete-Nishihata (2017), "We (can't)Chat: "709 Crack-down" Discussions Blocked on Weibo and WeChat," *Citizen Lab* <<https://citizenlab.ca/2017/04/we-cant-chat-709-crackdown-discussions-blocked-on-weibo-and-wechat/>>.



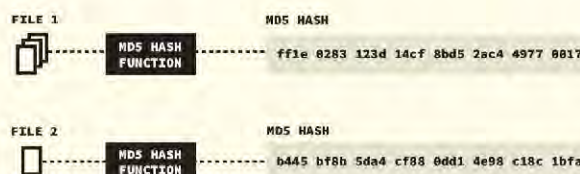
Previous work has found that WeChat placed images which are sent by China-registered accounts under two different kinds of surveillance.<sup>14</sup> Due to the computationally expensive and time-consuming methods required to analyze an image for sensitivity, these methods are not easily adapted to run in real-time. As a result, WeChat first subjects these images to *file hash surveillance* to assess whether the image has previously been categorized as sensitive, which is determined by checking to see if the file's hash is present in a *hash index* of known sensitive file hashes. This hash index check is performed in real time. If the image's file hash is in the hash index, it is censored in real time. Images that are not in the hash index of known sensitive files undergo *content surveillance*. Such surveillance involves the image being analyzed for whether it is visually similar to that of any blacklisted image. Further, text that is in the image is extracted and analyzed to determine if any of the text is blacklisted. If the image is found to be sensitive, then its file hash is added to the hash index to enable future real-time censorship. Of note, previous testing found that content surveillance was never performed in real time and that the first time that a sensitive image file is transmitted it was not censored.

In this report, we revisit how WeChat implements image surveillance. For the first time, we examine how WeChat conducts surveillance and censorship of documents sent over the platform. Moreover, we examine whether images and documents communicated entirely among non-China-registered accounts are subject to the same surveillance practices which were previously found to apply to communication to, or from, China-registered accounts.

### What is an MD5 hash?

Hash functions are designed to map a data input, such as a message or a file, into a short, fixed-size output called a hash. The MD5 hash function is a cryptographic hash function, which is a hash function with special cryptographic properties. Cryptographic hash functions have many additional properties over ordinary hash functions, but one such property is that it should be infeasible to find two different inputs such that the hash function maps them to the same output. That is, it should be infeasible to find two different inputs with the same hash. MD5 is an older cryptographic hash function designed in 1991.

The diagram below illustrates the process of mapping a file (e.g., a document or an image) to an MD5 hash. In this example, two different images are inputted to a cryptographic hash function resulting in two unique MD5 hashes.



<sup>14</sup> Knockel, Jeffrey and Ruohan Xiong (2019), "(Can't) Picture This 2: An Analysis of WeChat's Real-time Image Filtering in Chats," *Citizen Lab* (July 15, 2019)

## Part 2 - Technical Assessment

Measuring communications surveillance can be challenging due to its inherently invisible nature. In the absence of censorship, which restricts communication in a way that has a measurable effect (e.g., a message fails to be delivered), surveillance can be difficult to detect. To detect the communications surveillance of non-China-registered accounts, we developed and ran two side-channel experiments. In both experiments, we employ two channels, one communicating entirely among non-China-registered accounts and a second communicating with a China-registered account. By utilizing the hash index that censors China-registered WeChat accounts as a side channel, we were able to infer that content surveillance was occurring in the first channel by measuring for censorship in the second. We develop and performed a third experiment testing whether recalling a message containing a file removes that file's hash from the hash index.

In short, while we did not detect censorship in communications among non-China-registered accounts, we did demonstrate that such accounts are nevertheless subject to content surveillance. Such surveillance was discovered by confirming that politically sensitive content which was sent exclusively between non-China-registered accounts was identified as politically sensitive and subsequently censored when transmitted between China-registered accounts, without having previously been sent to, or between, China-registered accounts. In the remainder of this section, we explain our pre-experiment analysis, our experimental designs, and we present our experiment's results.

### 2.1 Background

Before designing our side-channel experiments, we first explored whether sensitive documents sent to, or from, China-registered accounts were surveilled and censored using a hash index. By sending sensitive documents to a China-registered account, we could observe which files were censored. We found that documents such as UTF8-encoded plain text (\*.txt), Microsoft Word (\*.docx), and Portable Document Format (\*.pdf) documents which contained certain sensitive keyword combinations such as “法輪功 [+] 法輪大法” (Falun Gong + Falun Dafa) were censored. As part of our investigation, we sent multiple documents across multiple days. Of particular note, we sent over 50 during November 25–26, which was immediately before our experiment, as well as over 50 during December 3–5, which was during our experiment. We found that all sent documents were subject



to surveillance and censored in the same way as images had been found to be surveilled and censored in previous work.<sup>15</sup> Namely, we confirmed that documents underwent file hash surveillance and that such files were not censored in real time until they had undergone non-real time content surveillance and their file hash had been added to the hash index.

We also sought to confirm whether images were still subject to surveillance and censored as described in previous work.<sup>16</sup> We found that, unlike in previous work where content surveillance of images was not performed in real time, images were now sometimes censored in real time even if they had never been sent over the platform before. Because of this new capability of WeChat's censorship implementation, we designed our experiment to send a large number of images such that we expected, with high probability, that at least one would not be censored in real time.

## 2.2 Statistical Experiment

In this section, we present our first side-channel experiment which tests for content surveillance of sensitive documents and images transmitted over WeChat. We call this experiment the *statistical experiment* because of this experiment's use of statistical analysis.

### 2.2.1 Methodology

In this experiment, we use two WeChat group chat conversations to serve as our two communication channels:

- 1) **Non-China group chat.** This group chat contains three non-China-registered WeChat accounts which were registered to Canadian phone numbers. In this group chat, a non-China-registered account sends content entirely among other non-China-registered accounts.
- 2) **China group chat.** This group chat contains two non-China-registered WeChat accounts which were registered to Canadian phone numbers and one WeChat account that was registered to a mainland China

15 Knockel, Jeffrey and Ruohan Xiong (2019), "(Can't) Picture This 2: An Analysis of WeChat's Realtime Image Filtering in Chats," *Citizen Lab* (July 15, 2019) <<https://citizenlab.ca/2019/07/cant-picture-this-2-an-analysis-of-wechats-realtime-image-filtering-in-chats/>>

16 Knockel, Jeffrey and Ruohan Xiong (2019), "(Can't) Picture This 2: An Analysis of WeChat's Realtime Image Filtering in Chats," *Citizen Lab* (July 15, 2019) <<https://citizenlab.ca/2019/07/cant-picture-this-2-an-analysis-of-wechats-realtime-image-filtering-in-chats/>>



phone number. In this group chat, a non-China-registered account simultaneously sends content to both a non-China-registered and a China-registered account. In this group chat, we are interested in whether the China-registered account receives the content or if the content is instead censored.

Our experiments rely on testing for the presence of a file's hash in WeChat's censorship hash index. By sending a file in the **China group chat** and measuring whether that file is censored in real time, we can test whether its hash is already in the hash index. However, as a consequence of this test, we introduce the hash into the hash index if it was not already present. Thus, it is important that, whenever we perform a new test, we send a unique file with a hash that has never been sent over WeChat before. We call such a file a *novel* file, since its hash is novel to the WeChat platform.

In the remainder of this section, we explain the design of our side-channel experiment to test for content surveillance of document and image files when sent entirely among non-China-registered accounts.



Figure 3: In the case of no content surveillance, the hash index is not updated when non-China-registered accounts send a novel, sensitive document to other non-China-registered accounts (top). Thus, when the same document is sent to China-registered accounts, the document is not censored (bottom).

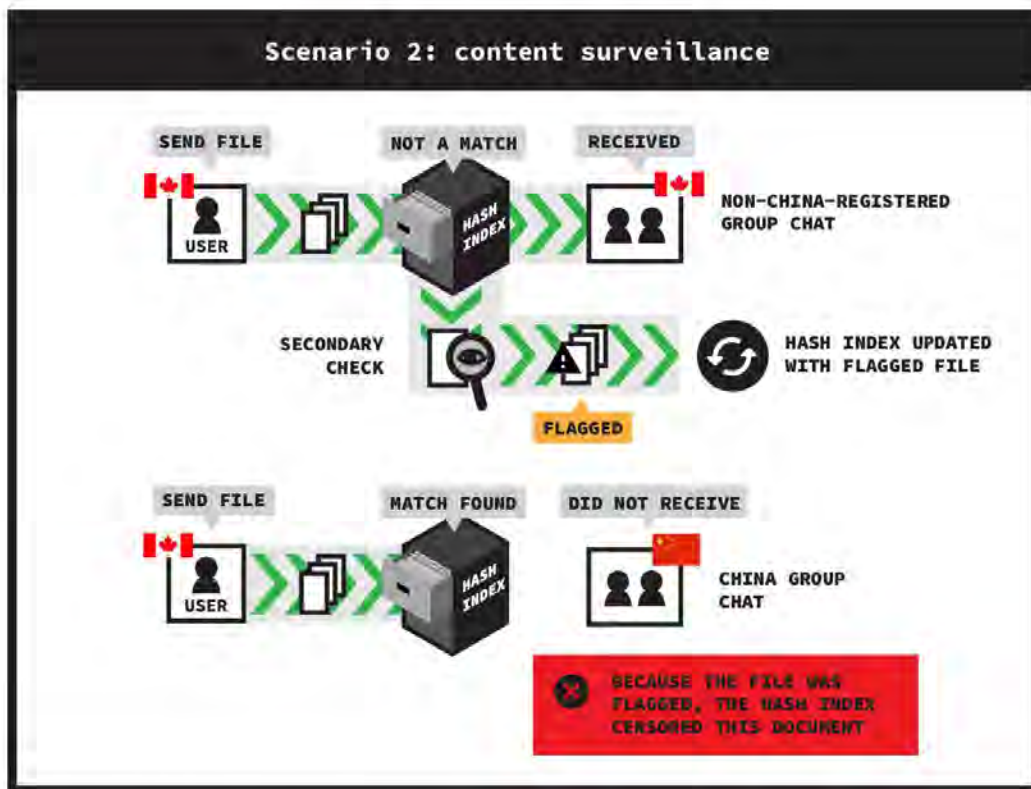


Figure 4: In the case of content surveillance, the hash index is updated when non-China-registered accounts send a novel, sensitive document to other non-China-registered accounts (top). Thus, when the same document is sent to China-registered accounts, the document is censored (bottom).

We performed the following test to evaluate whether document content surveillance takes place among non-China-registered accounts:

- **Document side-channel test.** We first send a novel, sensitive document in the **non-China group chat** and then send the same document in the **China group chat**. If the document is censored in real time when sent to the China-registered account, then we conclude there was surveillance of the sensitive document during the communication among the **non-China group chat**.

In this document side-channel test, the hash index serves as a side-channel by leaking information about whether the **non-China group chat** is under content surveillance by measuring for censorship in the **China group chat**. This method is sufficient for testing for the existence of document surveillance because, at the time of testing, WeChat did not censor documents in real time. Thus, whenever we observe real-time document censorship, we can conclude that the document had previously been subject to surveillance.

In the case of image files, we observed that sometimes WeChat censors them in real time even if they have not previously undergone content surveillance on the



platform. To accommodate this behaviour, we send a sufficiently large number of images such that, if images sent entirely among non-China-registered accounts undergo content surveillance, then we will still be able to distinguish the effect this surveillance has on real-time censorship even if real-time censorship sometimes happens in the absence of content surveillance. Specifically, we first conduct the following test:

- 1) **Image side-channel test.** We first send  $n$  novel, sensitive images in the **non-China group chat** and then send the same images in the **China group chat** one minute later. We count how many images were not received by the China-registered account.

We then compare the number of censored images from the previous test to that of the following test:

- 1) **Image control test.** We send  $n$  novel, sensitive images in the **China group chat**. We count how many were not received by the China-registered account.

The difference between these two tests is that in the **image side-channel test**, we first send an image among the non-China-registered accounts before sending it to a China-registered account, whereas in the **image control test**, we send the image to a China-registered account without sending it to non-China-registered accounts first. If there is a significantly larger number of images censored in the **image side-channel test**, then we can conclude that sending images among non-China-registered accounts is facilitating real-time Chinese censorship.

We use statistical hypothesis testing to determine whether there is a statistically significant increase in the number of images censored in the **image side-channel test** than in the **image control test**. Namely, we perform a chi-squared test<sup>17</sup> under the null hypothesis that sending images from non-China-registered accounts to non-China-registered accounts does not affect the probability that they will be censored in real-time when they are later sent to a China-registered account. If, according to the chi-squared test, we may reject the null hypothesis, then we can conclude that images sent entirely among non-China-registered accounts are under content surveillance and are contributing to WeChat's Chinese censorship system.

<sup>17</sup> Wikipedia (2020), "Chi-squared test," *Wikipedia* (Last updated February 14, 2020) <[https://en.wikipedia.org/wiki/Chi-squared\\_test](https://en.wikipedia.org/wiki/Chi-squared_test)>.

For each image test, we send  $n$  novel images. Our desire is to choose an  $n$  high enough that our statistical test has sufficient power to determine whether content surveillance between non-China-registered accounts exists. However, we also want  $n$  to be sufficiently low to minimize the risk of WeChat taking adverse action against our testing accounts (e.g., WeChat has been known to suspend or ban accounts in response to censorship testing<sup>18</sup>). In our experiment, we will evaluate choosing  $n = 60$ .

For both document and image testing, each test requires that we send novel, sensitive documents or images that have not previously been sent over the platform to ensure that the sensitive files' hashes are not already in the hash index. In principle, we could use entirely different sensitive documents and images. However, this approach would limit us to only performing as many file transmissions as we have known sensitive files. Thus, to facilitate testing, we generate novel, sensitive files by performing subtle modifications to a single sensitive document and a single sensitive image; we call each of these *seed* files. These modifications are designed to change these files' hashes without changing their ability to be recognized as sensitive and, thus, let us generate an indefinite number of sensitive documents and images. In the remainder of this section, we explain, for both documents and images, which seed file we use and how we generate novel copies of a seed file such that the derivative files remain sensitive.

Lorem ipsum  
 法輪大法  
 法輪大法  
 法輪功  
 法輪功  
 Lorem ipsum

*Figure 5: The text of the sensitive seed document.*

For documents, we use as our seed document a \*.docx file which contains the characters for Falun Dafa and Falun Gong in both simplified and traditional Chinese, as well as some filler text (see Figure 5). To create a novel, still-sensitive copy of it, we then append 64 alphanumeric characters chosen uniformly at random.

18 Xiong, Ruohan and Jeffrey Knockel (2019). "An Efficient Method to Determine which Combination of Keywords Triggered Automatic Filtering of a Message," *FOCI 2019* <[https://www.usenix.org/system/files/foci19-paper\\_xiong.pdf](https://www.usenix.org/system/files/foci19-paper_xiong.pdf)>.





Figure 6: Our sensitive seed image, a cartoon memorializing the passing of Nobel Peace Prize awardee Liu Xiaobo.

For images, we use as our seed file a cartoon of Liu Xiaobo (see Figure 6) that was found to be censored on WeChat in previous work.<sup>19</sup> To create a novel, still-sensitive copy of it, we append 24 KiB of random bytes to it. Since the seed file we used was a JPEG-encoded image, all data past the JPEG end-of-file marker is ignored when rendering the image; however, the appended data still causes the file to hash to a different value.

### 2.2.2 Experimental Setup

We ran our experiment to test for document and image file surveillance across three separate days: November 27, December 2, and December 6, 2019. We spread the experiment across three days to ensure that the behaviour we observed was consistent across time and to reduce the risk of adverse action taken against our test accounts. All measurements were performed from a University of Toronto network in Toronto, Canada. For each test, on each day, we transmitted novel, sensitive documents or images which had never previously been communicated

19. Knockel, Jeffrey and Ruohan Xiong (2019), “(Can’t) Picture This 2: An Analysis of WeChat’s Realtime Image Filtering in Chats,” *Citizen Lab* (July 15, 2019) <<https://citizenlab.ca/2019/07/cant-picture-this-2-an-analysis-of-wechats-realtime-image-filtering-in-chats/>>



over the platform. In the remainder of this section, we present the results of these experiments.

### 2.2.3 Results

Test	Nov. 25-26	Nov. 27	Dec. 2	Dec. 3-5	Dec. 6	Total
<b>Document side-channel</b>		1/1	1/1		1/1	3/3
<b>Document control</b>	0/≥50			0/≥50		0/≥100
<b>Image side-channel</b>		20/20	20/20		20/20	60/60
<b>Image control</b>		17/20	14/20		18/20	49/60

Table 1: For each test, the number of files which were censored on each date.

Table 1 shows the results of our experiment testing for document and image surveillance on each of the three days it was conducted. Although our experimental design did not explicitly contain a **document control test**, we reference one to be consistent with our presentation of the image test results. Specifically, this test refers to our implicit results from investigating how document censorship worked on WeChat, which confirmed that WeChat lacked the capability to censor documents in real time (see Section 2.1).

Our results show that on each day of testing, if a sensitive document is first sent from a non-China-registered account to non-China-registered accounts, before sending it to a China-registered account, they are censored in real time when sent to a China-registered account. This finding shows that documents sent even entirely among non-China-registered accounts undergo content surveillance and that these documents are used to build-up the censorship system to which China-registered accounts are subjected.

Unlike with documents, we observed that WeChat can sometimes censor images in real time.<sup>20</sup> Out of 60 images sent across three days, 49 images were censored in real time when only sending them to China-registered accounts. However, if we first sent them from a non-China-registered account to other non-China-registered accounts, then all 60 out of 60 images were censored in real-time when sent to a China-registered account. To confirm that the difference in these two results are

<sup>20</sup> As of now, it is unclear why certain images are censored in real time while others are not.

statistically significant, we performed a chi-squared test under the null hypothesis that sending images from non-China-registered accounts to non-China-registered accounts does not affect the probability that they will be censored in real time when they are later sent to a China-registered account. We reject the null hypothesis because we found that there is only a  $p = 0.00078$  probability of observing at least as large of a difference by chance. This result shows that, in addition to documents, images sent even entirely among non-China-registered accounts also undergo content surveillance, and that images sent among non-China-registered accounts are also used to build-up the censorship system to which China-registered accounts are subjected.

Finally, for our image testing, we evaluate our choice of sending  $n = 60$  images across each image test. At no point during testing were any of our test accounts banned for sending this number of images. Moreover, choosing this number yielded highly significant results. These findings show that sending 60 images across three different days is powerful enough to result in statistically significant results and suggests that an even smaller value of  $n$  could be used in future experiments to further minimize risk of account closure.

## 2.3 Collision Experiment

In Section 2.2, we presented a side-channel experiment that confirmed that documents and images which are communicated entirely among non-China-registered accounts undergo content surveillance. Unlike documents, novel images were sometimes censored in real time when sent over WeChat for the first time. Consequently, we used statistical methods to show that such images were increasingly censored when previously exposed to surveillance. In this section, we present an alternative experiment that does not require statistical analysis and which further confirms the findings of the past experiment. The method of our follow-up experiment, the *collision experiment*, takes advantage of the fact that WeChat uses MD5 as its file hash algorithm and that this hash function has known vulnerabilities relating to hash collisions.

### 2.3.1 Methodology

Our method in the collision experiment is similar to the statistical experiment described in Section 2.2, but with one significant difference. In this experiment, we never send a sensitive image in the **China group chat**. Instead, we send a non-sensitive image that has been specially crafted to have the same MD5 hash as that



of a novel, sensitive image. As we have demonstrated in previous work<sup>21</sup>, due to a vulnerability<sup>22</sup> in the MD5 hash algorithm, given any two images, we can modify the images' metadata such that they have the same MD5 hash.



Table 2: The sensitive (left) and non-sensitive (right) seed images used in our experiment. Examples of MD5 hash collisions are here<sup>23</sup> (left) and here<sup>24</sup> (right).

Specifically, we conduct the following two tests:

- 1) **Collision side-channel test.** We first generate 20 novel, sensitive images with the same MD5 hashes as 20 non-sensitive images. We send the 20 sensitive images in the **non-China group chat** and then send the 20 non-sensitive images in the **China group chat** one minute later. We count how many of the non-sensitive images were not received by the China-registered account.

We then compare the number of censored images from the image collision side-channel test to that of the following test:

- 2) **Collision control test.** We first generate 20 novel, sensitive images with the same MD5 hashes as 20 non-sensitive images. We send the 20 non-

21 Knockel, Jeffrey and Ruohan Xiong (2019), “(Can’t) Picture This 2: An Analysis of WeChat’s Realtime Image Filtering in Chats,” *Citizen Lab* (July 15, 2019) <<https://citizenlab.ca/2019/07/cant-picture-this-2-an-analysis-of-wechats-realtime-image-filtering-in-chats/>>

22 Albertini, Ange and Marc Stevens (2019), “Hash collisions and their exploitations,” <<https://github.com/corkami/collisions>>

23 n.d.. <<https://raw.githubusercontent.com/citizenlab/chat-censorship/master/md5-collision-example/lxb-afa92a14854d6ac92d8a8446145b4d1b.jpeg>>

24 n.d.. <<https://raw.githubusercontent.com/citizenlab/chat-censorship/master/md5-collision-example/citlab-afa92a14854d6ac92d8a8446145b4d1b.jpeg>>

sensitive images in the **China group chat**. We count how many were not received by the China-registered account.

Like in the image experiment performed in Section 2.2, if there is content surveillance of communications sent entirely among non-China accounts, then we would expect a larger number of images to be censored in the **collision side-channel test** than in the **collision control test**. In fact, in this experiment, since we only send benign images in the **non-China group chat** test, if there is surveillance, then we expect that all non-sensitive images should be censored in the **collision side-channel test** and that none of the non-sensitive images will be censored in the **collision control test**.

### 2.3.2 Experimental Setup

We performed this experiment on January 30, 2020, on a University of Toronto network in Toronto, Canada. Unlike with our statistical experiment, we performed the collision experiment on a single day because this experiment does not require measuring a large number of image transmissions.

### 2.3.3 Results

Test	Jan. 30, 2020
Collision side-channel	20/20
Collision control	0/20

Table 4: For each test, the number of non-sensitive images which were censored.

In the **collision side-channel test**, all 20 of the 20 non-sensitive images were censored, whereas in the **collision control test** none of the 20 non-sensitive images were censored. Without the use of statistics, these results demonstrate that images are under content surveillance even when sent entirely among non-China-registered accounts, and that they are used to invisibly build up WeChat’s censorship system.<sup>25</sup>

## 2.4 Retention Experiment

WeChat provides a feature to recall<sup>26</sup> a message which lets users delete a chat message that has been sent within the last two minutes to prevent users from viewing it if they have not viewed the message already. The international version

<sup>25</sup> As a secondary consequence, these results also show that WeChat still uses the MD5 hash function for hashing files for its hash index.

<sup>26</sup> WeChat (n.d.), “How do I recall a sent message?” WeChat <<https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?opcode=2&plat=2&lang=en&id=120813euEJVf1410236fl7RB&Channel=helpcenter>>.



of WeChat's privacy policy contains links to support documentation<sup>27</sup> that advises users based in the European Union to use the recall feature to remove personal information from chat messages. In this section, we design and perform an experiment to evaluate whether, after a chat message containing a file is recalled, WeChat still retains its hash in the hash index.

### 2.4.1 Methodology

To test whether WeChat retains a hash of a recalled file, we perform the following test:

- **Hash retention test.** We send a novel, sensitive document in the **non-China group chat** in a group chat and then immediately recall the document. One hour later, we send the same document in the **China group chat**. If the document is censored in real time when sent to the China-registered account, then recalling the document did not remove the hash from the file index.

For this test, we generate novel, sensitive documents as described in Section 2.2.1.

### 2.4.2 Experimental setup

We performed this experiment on January 7, 2020, on a University of Toronto network in Toronto, Canada. To test if the results would be different for European Union users, we repeated this experiment on January 9, 2020, using a WeChat account registered to a Belgian phone number and using a VPN server in Belgium. On each day of testing, we ran the test five times.

### 2.4.3 Results

Test	Jan. 7, 2020	Jan. 9, 2020
Hash retention	5/5	5/5

Table 4: The number of recalled images which were censored on each day.

For both days of testing, in all five tests, the recalled document was never received by the China-registered account. This result shows that recalling a document after it is sent does not remove that file's MD5 hash from WeChat's hash index, either for users outside or inside the European Union.

<sup>27</sup> WeChat (n.d.), "How do I manage my account including how to export my personal data or request my account to be deleted?" *WeChat* <<https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?opcode=2&lang=en&plat=ios&id=180323e2Ermm180323yqauAZ&Channel=help-center>>.



## 2.5 Summary

Our experiments reveal that content surveillance is applied to both China-registered accounts as well as to non-China-registered accounts. Content surveillance between users of non-China-registered accounts is functionally undetectable unless those users conduct their own side-channel research to detect whether the documents or images that they shared have both been hashed for censorship purposes and, also, that the hashed documents or images are actually being censored. Put another way, in cases where documents or images are hashed but the files themselves are not presently censored, it would not be possible to know which, if any, files had been analyzed and hashed for potential censorship activities using the experiments we performed.

While there is a system in place to monitor and generate hashes for the documents and images transmitted between non-China-registered accounts for content which raises social or political concerns in China, our research has not demonstrated that there is an equivalent application of a censorship system in place for the communications which take place between non-China-registered accounts. Put plainly, we have not witnessed censorship between non-China-registered accounts of materials which are censored among China-registered accounts. By conducting our side-channel experiment, we were nevertheless able to measure the existence of content surveillance for such materials transmitted among non-China-registered accounts.

Moreover, the experiments show that non-China-registered accounts cannot remove hashes of sensitive content which they have sent when communicating entirely with other international users as a side effect of recalling their content. Consequently, while it may appear to users that they can recall the content of their communications, at least some of the metadata associated with such communications—such as the hashes of sensitive files—are disassociated from the retraction system. It is unclear based on our technical findings whether such a hash register would be associated with individual accounts. Nevertheless, these hashes will be used to build-up WeChat's censorship system.

Finally, our experiments conducted on multiple days across November 2019 – January 2020 consistently show content surveillance of documents and images sent among non-China-registered users. However, our data cannot answer for how long non-China registered users' files have been subject to such surveillance, and we cannot distinguish between this surveillance behaviour being a recent addition

versus a long-standing behaviour. Although such surveillance was consistently observed on each day of testing, we cannot speak to whether such surveillance was consistently applied across days which were not tested.

## Part 3 - Policy Assessment

Before a company can make their application available on the Google Play store or Apple's App store, they must first develop and publish a privacy policy to accompany the given application. These public-facing documents are intended to inform users about how their data will be used and protected. Quite often, privacy policies and accompanying terms of service documents will include information such as what is, and is not, considered personal information or sensitive information, as well as detailed information concerning the kinds of activities a company may take towards a user's data.

For this report, we analyzed the international (i.e., Singapore) as well as the mainland China (i.e., Shenzhen) privacy policies and terms of service documents that were associated with WeChat. The analysis was meant to help us understand how the company asserts that it handles personal information and, through this analysis, better understand whether Tencent's international policy documentation suggests that international users' communication might be used to develop, enhance, or maintain the hash index which is used to censor communications between China-registered WeChat accounts. We also sent detailed questions to Tencent's international data protection office to seek clarity concerning the company's privacy policy and terms of service documentation. We also hoped that responses from the office would confirm the report's technical findings and disclose the rationales for which content transmitted between non-China-registered accounts was used to develop, enhance, or maintain the censorship system which is applied to China-registered accounts.

Overall, we found, first, that neither the China nor international public policy documents made clear to users that non-China accounts could have their content surveilled and the resulting hashes used to censor content for China-registered accounts. Second, we found it was plausible that the international policy documents could permit content surveillance of international users' communications, but the company did not respond to these questions. Third, we found that it was unclear on what basis the hashes of international users' communications could be shared with WeChat China, and the company did not respond to these questions.



## 3.1 Methodology

We undertook three related activities to assess Tencent's mainland China and international privacy policies and terms of service documents for WeChat<sup>28</sup>: downloading relevant policies (e.g., privacy policies and terms of service agreements); assessing the aforementioned policies using a pre-determined series of structured questions; and contacting the company's international data protection office with questions about whether content transmitted between non-China-registered accounts was ever used to develop, enhance, or maintain the censorship system applied to China-registered accounts.

### 3.1.1 Obtaining Relevant Public-Facing Policies

Relevant policies were downloaded from Tencent's websites in December 2019. We specifically downloaded the following policies which apply to China-registered WeChat accounts:

- Agreement on Software License and Services of Tencent Weixin (Simplified Chinese<sup>29</sup> and English<sup>30</sup> versions)
- Weixin Privacy Policy Protection Guidelines (Simplified Chinese<sup>31</sup> and English<sup>32</sup> versions)
- Standards of Weixin Account Usage (Simplified Chinese<sup>33</sup> and English<sup>34</sup> versions)

Each of these documents are available in several languages, including English, simplified Chinese, and traditional Chinese.

28 In this section we refer to policy documents applicable to WeChat's China-registered accounts as WeChat China documents and those to non-China-registered accounts as WeChat International documents.

29 Weixin (2019), "Weixin Privacy Protection Guidelines [in Chinese]," *Weixin* (September 30, 2019) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=zh\\_CN&t=weixin\\_agreement&s=privacy](https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy)> [<https://perma.cc/UG33-CYTP>]

30 Weixin (n.d.), "Agreement on Software License and Service of Tencent Weixin," *Weixin* (n.d.) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=default&c-c=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=default&c-c=CN)> [<https://perma.cc/DJB5-U7DD>]

31 [https://weixin.qq.com/cgi-bin/readtemplate?lang=zh\\_CN&t=weixin\\_agreement&s=privacy](https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy) [<https://perma.cc/UG33-CYTP>]. Our analysis is based on the Privacy Policy Protection Guidelines published on September 30, 2019. WeChat has updated the document on January 21, 2020, whose changes pertain to primarily a new functionality WeChat introduces to its platform.

32 Weixin (2019), "Weixin Privacy Protection Guidelines," *Weixin* (September 30, 2019) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=privacy&cc=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=privacy&cc=CN)> [<https://perma.cc/WD5C-J3ZR>]

33 [https://weixin.qq.com/cgi-bin/readtemplate?&t=page/agreement/personal\\_account&lang=zh\\_CN](https://weixin.qq.com/cgi-bin/readtemplate?&t=page/agreement/personal_account&lang=zh_CN)

34 Weixin (n.d.), "Standards of Weixin Account Usage," *Weixin* (n.d.) <[https://weixin.qq.com/cgi-bin/readtemplate?&t=page/agreement/personal\\_account&lang=en\\_US](https://weixin.qq.com/cgi-bin/readtemplate?&t=page/agreement/personal_account&lang=en_US)>.



We downloaded the following policies which applied to non-China WeChat accounts:

- WeChat Privacy Protection Summary<sup>35</sup>
- WeChat – Terms of Service<sup>36</sup>
- WeChat Acceptable Use Policy<sup>37</sup>

We primarily analyzed WeChat China's documents in English to facilitate comparing them directly with WeChat's international policies. We did, however, also examine the simplified Chinese version of WeChat China's documents to determine if there were significant differences between the Chinese and English; such discrepancies could potentially be notable because the Chinese version of the documents prevails over any versions of the documents in case of any inconsistency and discrepancy.<sup>38</sup>

### 3.1.2 Structured Question Set

We assessed the collected privacy policies, terms of service documents, and acceptable use policies using a structured question set. This question set is based on similar assessments that Citizen Lab researchers have conducted in the past of telecommunications companies, fitness tracker companies, online dating companies, and stalkerware companies.<sup>39</sup> Assessment categories were divided into specific questions pertaining to:

- **How Tencent presents and has developed its privacy policy:** e.g., "Is there

- 35 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 1, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)> [<https://perma.cc/3S76-6MCX>]
- 36 WeChat (2018), "WeChat -- Terms of Service," *WeChat* (March 21, 2018) <[https://www.wechat.com/en/service\\_terms.html](https://www.wechat.com/en/service_terms.html)> [<https://perma.cc/ZH6Y-GJWK>]
- 37 WeChat (2015), "WeChat -- Acceptable Use Policy," *WeChat* (November 13, 2015) <[https://www.wechat.com/en/acceptable\\_use\\_policy.html](https://www.wechat.com/en/acceptable_use_policy.html)> [<https://perma.cc/2FUB-7J94>]
- 38 Weixin (n.d.), "Agreement on Software License and Service of Tencent Weixin," *Weixin* (n.d.) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=default&c-CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=default&c-CN)> [<https://perma.cc/5KRJ-28NE>]. Section 12.6 of the Agreement on Software License and Service of Tencent Weixin reads, "In case of any inconsistency and discrepancy between the Chinese version and any version of other language, the Chinese version shall prevail."
- 39 Parsons, Christopher, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo, Ron Deibert (2019), "The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry," *Citizen Lab* <<https://citizenlab.ca/docs/stalkerware-holistic.pdf>>; Hilts, Andrew, Christopher Parsons, and Jeffrey Knockel (2016), "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security," *Open Effect* <[https://openeffect.ca/re-ports/Every\\_Step\\_You\\_Fake.pdf](https://openeffect.ca/re-ports/Every_Step_You_Fake.pdf)>; Parsons, Christopher, Andrew Hilts, and Masashi Crete-Nishihata (2017), "Approaching Access: A comparative analysis of company responses to data access requests in Canada," *Citizen Lab* <[https://citizenlab.ca/wp-content/uploads/2018/02/approaching\\_access.pdf](https://citizenlab.ca/wp-content/uploads/2018/02/approaching_access.pdf)>; Parsons, Christopher (2015), "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project* <<http://www.telecomtransparency.org/release-the-governance-of-telecommunications-surveillance/>>.

a link to a privacy policy on the company's webpage?," "Is there a reference to compliance with: national privacy laws, international guidelines, and/or self-regulatory instruments from associations?," "Is there a statement concerning which nation/court proceedings must go through?"

- **How Tencent addresses questions from its users of WeChat:** e.g., "Is there a contact to a privacy officer listed?" and "Is there a description/discussion of who you can complain to if you're unsatisfied with the information provided by the company?"
- **How Tencent captures personally identifiable information (PII):** e.g., "Is there specification about the kinds of PII (i.e., information about the 'users') collected? If so, what types of categories are listed?," "Is there any distinction made between sensitive and non-sensitive PII?," and "Are there specifications for where the information is stored?"
- **How, or under what conditions, Tencent might disclose collected data:** e.g., "Is there a specification on the kinds of organizations that users' information may be disclosed to?," Does the company use the term 'sharing' or 'selling' information to third parties?," and "Does the company reserve the right to share information with other parties in the case that they suspect a law has been violated or to exercise the company's own legal rights, or to remain compliant with the law?"
- **Are there rationales under which Tencent might 'hash' the content of international users' communications?**
- **Are there rationales under which Tencent might block or censor content?**

Combined, these questions were designed to help us understand the company's compliance with laws designed to protect persons' privacy, whether the company has processes in place to help individuals answer questions about their privacy or business practices, the kinds of data that the company asserts it does collect and disclose to other parties, and specifically whether the policies permit or justify Tencent's hashing of communications content transmitted between non-China-registered accounts.



### 3.1.3 Communication with Data Protection Office

We contacted Tencent's international data protection office to seek further clarity concerning the privacy policy and terms of use policies which applied to international users. We adopted this methodology to better understand how the company interpreted its policies as well as to seek confirmation or denial that it hashed the content of its international users' communications. The letter contained eight core questions; a copy of the letter is available in [Appendix A](#).

In addition to seeking clarity concerning the company's public policy documentation, we also sought to better understand the extent to which persons who were involved in Tencent's international policy work understood, or were made aware of, how WeChat functionally operated. Specifically, we contacted the company after completing our experiments that showed communications between non-China registered accounts were used to develop, enhance, or maintain the hash index that is used to censor content between China-registered account users. Additionally, we wanted to understand if the international data protection officer was aware of such surveillance of international users' communications content.

## 3.2 Results

The following sections present the most significant findings that emerged from our policy assessment.

### 3.2.1 General Policy Questions

WeChat China's and WeChat International's websites both provided links to their respective services' privacy policies or terms of service on the homepage of their respective websites. Links on WeChat China's homepage directed users to the Chinese versions of respective policies, and from there users could choose to view the policies in other languages.

WeChat China and WeChat International both included references to the national laws and regulations with which the respective entities comply. In the case of WeChat China, the policies included general references to "relevant laws and regulations" without specifying the specific ones the company complied with, with exception of policies concerning content moderation.<sup>40</sup> In the case of disputes, users

<sup>40</sup> Weixin (n.d.), "Agreement on Software License and Service of Tencent Weixin," *Weixin* (n.d.) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=default&c-](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=default&c-)

must submit them to the local people's court<sup>41</sup> in Nanshan District, Shenzhen City, Guangdong Province of the People's Republic of China.<sup>42</sup>

In contrast, WeChat International's policies made reference to the Digital Millennium Copyright Act (DMCA) (i.e., US copyright law) and broad references to European laws, though the policies did not explicitly cite the General Data Protection Regulation (GDPR). WeChat International's policies asserted that the governing jurisdiction for any disputes or claims, with the exception of those that pertained to US- and EU-based users, was the Hong Kong Special Administrative Region. The Hong Kong International Arbitration Centre was responsible for conducting any arbitration between users and WeChat International. However, in cases of US-based users, the governing law and dispute resolution would take place in the state or federal courts of California, with trial by jury and class action legal proceedings waived as a condition of using the service. For EU-based users, if the person was classified as a "consumer" (per EU Directive 83/2011/EU) then disputes were to be referred to, and resolved by, "the court of the person's place or residence of domicile."<sup>43</sup>

Both WeChat China's and WeChat International's privacy policies made partial references to their terms of services and other applicable documents, including the Standards of Weixin Account Usage for WeChat China users and the Acceptable Use Policy for WeChat International users. However, the entities did not always provide links to the relevant documents to which they referred. While WeChat China linked to its terms of services in its privacy policy, its privacy policy did not provide links to the terms of services. In the case of WeChat International, its terms of service included links to the privacy policy, and vice versa.

WeChat China noted when the last updated date and effective date were for its privacy policy but it did not do so for its terms of service. WeChat International provided information about when each of the respective documents was last

---

c=CN>; <https://perma.cc/5KRJ-28NE>. In the case of content regulation, WeChat China specified that users must not, among other things, "violate the basic principles established by the Constitution", or "contradict to *Interim Provisions on the Administration of the Development of Public Information Services of Instant Messaging Tools* and comply with the requirements of 'seven bottom lines' including laws and regulations, socialist systems, national interests, legitimate interests of citizens, public order, social morality and information authenticity." Italics in original.

41 The Supreme People's Court of the People's Republic of China (2009), "Constitute of the People's Republic of China," *China Court* <<http://en.chinacourt.gov.cn/public/detail.php?id=4446>>.

42 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>.

43 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>.



updated. Neither of the two entities provided access to historical versions of any of their policies.

### 3.2.2 Engaging with Company Through Questions or Complaints

We examined whether WeChat China and WeChat International provided specific contact information so that users could communicate with the company, which they may want to do in order to better understand how the platform captures, processes, or stores their personal information.

Both WeChat China and WeChat International had dedicated legal contact information, though neither identified a specific named privacy officer or point of contact. WeChat International explicitly noted that EU residents “have the right to lodge a complaint with [their] country’s data protection authority.”

While WeChat China and WeChat International promised to protect users’ rights to access, correct, and delete personal information, they both included caveats.<sup>44</sup> WeChat China provided a detailed operational guide in its privacy policy on how users can access, amend, or delete personal information and on how to withdraw permission within the application. In addition to data access, correction, and erasure, WeChat International outlined data portability features which were exclusively reserved for EU users.<sup>45</sup>

### 3.2.3 Capture of Personal Information

Many social media services are designed to collect vast quantities of personal information, some of which is intimately sensitive in nature. We examined whether WeChat China and WeChat International clearly indicated the types of information that they collected as well as whether they provided rationales for the collections. We also examined if there were specifications for where information was stored in these policies.

<sup>44</sup> WeChat (2018), “WeChat Privacy Protection Summary,” *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>. For specificity, WeChat International defined personal information as “any information, or combination of information, that relates to you, that can be used (directly or indirectly) to identify you.” Types of personal information WeChat International identified included “Registration Data and Log-in Data” (i.e., a user’s “name, user alias, mobile phone number, password, gender, and IP address”) and “user profile search data” (i.e., “record of search inquiries”).

<sup>45</sup> WeChat (n.d.), “How do I manage my account including how to export my personal data or request my account to be deleted?,” *WeChat* <<https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?opcode=2&lang=en&plat=ios&id=180323e2Ermm180323yqauAZ&Channel=help-center>>.



WeChat China and WeChat International policies distinguished between sensitive personal information and non-personal information. WeChat China's policy did not provide a definition of personal information but did indicate the types of information it collected and, from among those, which constituted sensitive information.<sup>46</sup> Notably, WeChat China asserted that in addition to the types of data it outlined in its policies, the company could collect and process relevant personal information without asking for users' content under various circumstances.<sup>47</sup> WeChat International defined personal information as "any information, or combination of information, that relates to you, that can be used (directly or indirectly) to identify you."<sup>48</sup> WeChat International further specified what types of information were regarded as "shared information" (i.e., "information about you or relating to you that is voluntarily shared by you on WeChat"). Of particular note, WeChat International recognized a difference between 'regular' personal information and 'sensitive' personal information. Sensitive personal information included that about "your race or ethnic origin, religious or philosophical views or personal health" and "is subject to stricter regulation than other types of Personal Information...Before communicating any Personal Information of a sensitive nature within WeChat, please consider whether it is appropriate to do so."<sup>49</sup> The WeChat International's definition of sensitive personal information is contrasted against that in WeChat China's, where sensitive information includes a user's mobile phone number, voice biometrics, location information, movement (e.g., number of steps), contact/friends information, and payment records.<sup>50</sup> Furthermore, whereas search

46 Weixin (2019), "Weixin Privacy Protection Guidelines," *Weixin* (September 30, 2019) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=privacy&cc=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=privacy&cc=CN)>;[https://weixin.qq.com/cgi-bin/readtemplate?lang=zh\\_CN&t=weixin\\_agreement&s=privacy](https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy). Types of sensitive information included mobile phone numbers, voice biometrics, location information, the number of steps users recorded in WeChat China's movement function, bank account information, and "recommended contacts/friends" information.

47 Weixin (2019), "Weixin Privacy Protection Guidelines," *Weixin* (September 30, 2019) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=privacy&cc=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=privacy&cc=CN)>;[https://weixin.qq.com/cgi-bin/readtemplate?lang=zh\\_CN&t=weixin\\_agreement&s=privacy](https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy). WeChat China broadly named 10 scenarios in which such instances might happen. For instance, "when it is directly related to national interests such as national security and national defense, or it is directly related to major public interests such as public safety, public health, and public knowledge."

48 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>. Types of personal information WeChat International identified included "Registration Data and Log-in Data" (i.e., a user's "name, user alias, mobile phone number, password, gender, and IP address") and "user profile search data" (i.e., "record of search inquiries").

49 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>.

50 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>; Weixin (2019), "Weixin Privacy Protection Guidelines," *Weixin* (September 30, 2019) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_)



data were explicitly defined as personal information in WeChat International's policies, WeChat China did not make an equivalent specification.

WeChat International stated that chat data, which constitutes "[c]ontent of communications between you and another user or group of users" is "stored on your device and the devices of the users that you have sent communications to. We do not permanently store this information on our servers and it only passes through our servers so that it can be distributed to users you have chosen to send communications to."<sup>51</sup> WeChat China's statement on the duration of data retention was relatively vague, noting that "in general, we will only keep your personal information for the time necessary to achieve a specific purpose."<sup>52</sup> Whereas WeChat International explained it only retained chat data for 120 hours,<sup>53</sup> WeChat China cited only two examples (i.e., "mobile phone number" and "information in Moments"<sup>54</sup>) to show how long it stored personal information. Specifically, users' mobile phone numbers are stored for as long as they use WeChat, and information in Moments is stored until a user deletes the corresponding information.

WeChat China noted that all personal information collected within the territory in China would be stored in China. For users of WeChat International, the personal information would be transferred to, stored, or processed in Ontario, Canada or in Hong Kong. The company provided justifications noted for the choice of each location.<sup>55</sup>

agreement&s=privacy&cc=CN>;[https://weixin.qq.com/cgi-bin/readtemplate?lang=zh\\_CN&t=weixin\\_agreement&s=privacy](https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy).

51 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>.

52 Weixin (2019), "Weixin Privacy Protection Guidelines," *Weixin* (September 30, 2019) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=privacy&cc=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=privacy&cc=CN)>;[https://weixin.qq.com/cgi-bin/readtemplate?lang=zh\\_CN&t=weixin\\_agreement&s=privacy](https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy) at Section 2.2.

53 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>.

54 Weixin (2019), "Weixin Privacy Protection Guidelines," *Weixin* (September 30, 2019) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=privacy&cc=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=privacy&cc=CN)>. WeChat China noted that it would store a user's phone number for as long as he or she uses WeChat services. As for information in WeChat Moments, information would be saved "to ensure your normal use of the Moments functions" and would be deleted if a user deletes corresponding information in Moments.

55 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>. WeChat International noted that Ontario Canada "was found to have an adequate level of protection for Personal Information under Commission Decision 2002/2/EC of 20 December 2001)." In the case of Hong Kong, WeChat International "rely on the European Commission's model contracts for the transfer of personal data to third countries



### 3.2.4 Disclosures of Information

One of the growing concerns over the global expansion of Chinese Internet companies which have operational entities in mainland China and overseas is whether user data collected outside of China is shared with members and affiliates of the company in China, China-based third-parties, or Chinese authorities.<sup>56</sup> The prospect of such sharing is particularly significant given that technical research, discussed in Section 2, revealed that non-China-registered accounts' information was being subject to content surveillance for the purpose of extending what was censored for China-registered accounts. As such, we examined WeChat China's and WeChat International's policies to determine the extent to which the companies asserted their rights to disclose collected information to third-parties and the conditions under which such disclosures were authorized.

We found that the clarification varied between the two entities with respect to the disclosure of information to third-parties and members or affiliates of Tencent. WeChat China made it clear that it would not share users' personal information with third-parties outside of Tencent.<sup>57</sup> However, it was left unclear how personal information would be shared among services owned by Tencent. We found the opposite in WeChat International's policies, where there were sometimes very clear specifications about which Tencent-related group companies the application could share personal information.<sup>58</sup> WeChat International acknowledged that it shared user data with certain third-party service providers, as well, without specifying with whom or what types of information were shared.

(i.e., the standard contractual clauses), pursuant to Decision 2001/497/EC (in the case of transfers to a controller) and Decision 2004/915/EC (in the case of transfers to a processor)."

56 See, for example, an ongoing class action lawsuit in the US against Chinese-owned TikTok that claims it transferred "vast quantities" of user data to China: BBC News (2019), "TikTok sent US user data to China, lawsuit claims," *BBC News* (December 3, 2019) <<https://www.bbc.com/news/business-50640110>>.

57 Weixin (2019), "Weixin Privacy Protection Guidelines," *Weixin* (September 30, 2019) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=privacy&cc=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=privacy&cc=CN)>; [https://weixin.qq.com/cgi-bin/readtemplate?lang=zh\\_CN&t=weixin\\_agreement&s=privacy](https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy). WeChat China stated that "at present, [Tencent] will not actively share or transfer [the user's] personal information to a third party outside of Tencent" and that if there was any disclosure, Tencent would "directly obtain or verify the third party has obtained [the user's] prior express consent to such share or transfer of [the user's] personal information."

58 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>. For Tencent-related group companies, WeChat International stated that it shared personal information "our group of companies, including Tencent International Service Europe BV (located in the Netherlands), Tencent International Service Pte. Ltd (located in Singapore), WeChat International Pte Ltd (located in Singapore) and Oriental Power Holdings Limited (located in Hong Kong) and WeChat International (Canada) Limited (located in Canada) that run the Hong Kong and Canadian Servers," Additionally, "in the event of an internal restructuring of our or our affiliates businesses, or the sale of WeChat or any of its assets to a third party, the entity that consequently operates WeChat may be a different entity to us and we will transfer your information accordingly so that your service can continue."



WeChat China and WeChat International acknowledged that they may share information with law enforcement organizations under certain conditions, though the level of specificity varies between the two companies. WeChat China strongly implied that it would disclose the user's personal information to law enforcement organizations without specifying whether such disclosure would be conducted under a court order or which organizations would potentially receive information (e.g., police department based in the signing place of WeChat China agreements versus police departments based in any part of China).<sup>59</sup> Moreover, the circumstances under which the company "may share, transfer, or publicly disclose personal information without prior consent of the subject of the personal information" were broadly defined.<sup>60</sup> Though the entity did not specify which jurisdictions it would not share information with, WeChat China did acknowledge that the governing jurisdiction was mainland China.

In contrast, WeChat International stated that any disclosure of information to "government, public, regulatory, judicial and law enforcement bodies or authorities" would be carried out where the company "[is] required to comply with applicable laws or regulation, a court order, subpoena or other legal process, or otherwise have a legal basis to respond to a request for data from such bodies, and the requesting entity has valid jurisdiction to obtain [the user's] personal information."<sup>61</sup> The company did not commit to informing users about such disclosures. Similar to WeChat China's policies, WeChat International did not specify any countries with whom data would not be shared.

### 3.2.5 Behaviours of Hashing and Blocking User-Generated Content

Social media companies operating in China are known to control sensitive information in compliance with local laws and regulations.<sup>62</sup> As of early 2020, there

59 Weixin (2019), "Weixin Privacy Protection Guidelines," *Weixin* (September 30, 2019) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=privacy&cc=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=privacy&cc=CN)>. For clarity, WeChat China stated that, "Except for the circumstances prescribed by laws and regulations, Tencent will not make public or disclose the user's personal information to any third party without permission of the users."

60 Weixin Privacy Protection Guidelines Section 5 noted at least six circumstances under which it may disclose personal information without seeking prior consent. Without citing specific laws and regulations, these circumstances included vaguely defined and potentially overarching terms such as "national security or national defense," and "public safety, public health, or major public interests."

61 WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>.

62 MacKinnon, Rebecca (2009), "China's Censorship 2.0: How companies censor bloggers," *First*

are increasing concerns about how Chinese-owned companies might exploit data generated outside mainland China or among their international users in the face of domestic political pressure, such as to block the availability of certain content, or conduct surveillance of particular persons or classes of communications. We examined whether there was any mention of, or justification for, performing hashing of communications content for the purpose of facilitating blocking access to content in either of WeChat China's or WeChat International's policies.

We found that both companies discussed the possibility of retaining and using content for several purposes. WeChat China acknowledged that it “may use information collected by certain features for [...] other services” and that such practices were justified on the basis of enabling performance and service optimization.<sup>63</sup> In addition to stating that WeChat International and its affiliate companies “are allowed to retain and continue to use Your Content after you stop using WeChat,” WeChat International wrote in its terms of services that:

**“you are giving us and our affiliate companies a perpetual, non-exclusive, transferable, sub-licensable, royalty-free, worldwide licence to use Your Content (with no fees or charges payable by us to you) for the purposes of providing, promoting, developing and trying to improve WeChat and our other services, including new services that we may provide in the future... As part of this licence, we and our affiliate companies may, subject to the our WeChat Privacy Policy, copy, reproduce, host, store, process, adapt, modify, translate, perform, distribute and publish Your Content worldwide in all media and by all distribution methods, including those that are developed in the future.”**

Further, WeChat International might justify its hashing of content on the basis that doing so constitutes services improvement and security protections. Specifically, the company's policies stated that WeChat “may be required to retain or disclose Your Content in order to enforce these Terms or to protect any rights, property or safety of ours, our affiliate companies or other users of WeChat.”<sup>64</sup>

---

Monday <<https://firstmonday.org/article/view/2378/2089>>.

63 Weixin (2019), “Weixin Privacy Protection Guidelines,” *Weixin* (September 30, 2019) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=wxin\\_agreement&s=privacy&cc=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=wxin_agreement&s=privacy&cc=CN)>. In particular, WeChat China stated that, “Tencent is granted to use the non-confidential contents uploaded or published by you (such as video published via Time Capsule, selfie stickers) for achieving the performance of the Software and Services, including without limited to storage, displaying to relevant users, granting and allowing other use.”

64 WeChat (2018), “WeChat -- Terms of Service,” *WeChat* (March 21, 2018) <[https://www.wechat.com/en/service\\_terms.html](https://www.wechat.com/en/service_terms.html)>.



In terms of blocking content, WeChat China asserted that Tencent would act in accordance with laws and regulations based on its “reasonable judgement” to “remove or obscure relevant contents at any time without notice, impose punishment on the violating account including but not limited to warning, restriction or prohibition of the use of some or all of the functions, account banning or cancellation, and announce the results of treatment.”<sup>65</sup> Similarly, WeChat International stated that it “may review (but make no commitment to review) content (including any content posted by WeChat users) or third party programs or services made available through WeChat to determine whether or not they comply with our policies, applicable laws and regulations or are otherwise objectionable. We may remove or refuse to make available or link to certain content or third party programs or services if they infringe intellectual property rights, are obscene, defamatory or abusive, violate any rights or pose any risk to the security or performance of WeChat.”

### 3.2.6 Data Protection Office Non-Response

We contacted WeChat’s international data protection office on January 20, 2020, using the contact email that was provided in the company’s international Privacy Policy.<sup>66</sup> We did not receive a response from the Office, including even an acknowledgment that they received our initial letter, by February 3, 2020. As a result, we sent a reminder email on February 3, 2020; as of writing, we have still not received any response from WeChat’s international data protection office to the questions posed to them.

## 3.3 Discussion

It was easy to identify and access the international and China-specific versions of the privacy policies, terms of service, and associated documents linked with the WeChat service. Both China-registered and non-China-registered accounts were presented with data access, correction, and deletion capabilities, indicating that the company was compliant with basic rights afforded under the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada’s data privacy legislation. Similar rights are extended to persons living in European countries which are subject to the GDPR, or countries with GDPR-like legislation.

<sup>65</sup> Weixin (n.d.), “Agreement on Software License and Service of Tencent Weixin,” *Weixin* (n.d.) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=default&c-CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=default&c-CN)> [<https://perma.cc/5KRJ-28NE>] at Section 8.5.1.

<sup>66</sup> The email address was: dataprotection[.]@wechat[.]com.

While it is clear from public information that content may be blocked for China-registered accounts, it is unclear how international data is used to enable content blocking or the policy rationale which permits the sharing of data used for blocking between international and China regions of WeChat. As per their policies, WeChat International does reserve the right to block content for its international users. Specifically the company:

“may review (but make no commitment to review) content (including any content posted by WeChat users) or third party programs or services made available through WeChat to determine whether or not they comply with our policies, applicable laws and regulations or are otherwise objectionable. We may remove or refuse to make available or link to certain content or third party programs or services if they infringe intellectual property rights, are obscene, defamatory or abusive, violate any rights or pose any risk to the security or performance of WeChat.”<sup>67</sup>

While WeChat China’s policy documents clearly permit a wide range of blocking and WeChat International’s policies appear to permit some sort of blocking, these policies at best explain the motivation for content surveillance of non-China-registered users but do not enable it. In the remainder of this section, we discuss whether according to policy documents WeChat International is permitted to analyze non-China-registered users’ data for political sensitivity and whether WeChat International is permitted to share users’ data or the results of this analysis to entities in China.

### 3.3.1 Enabling Content Surveillance

The international public-facing policy documents do include language that could permit communications content surveillance and, therefore, prospectively the hashing of the contents of communications for the purposes of developing or enhancing WeChat’s censorship system. Specifically, the international policy documentation reveals that WeChat might review content, which could be interpreted as permitting the company to assess content to derive hashes from it. The company, elsewhere, acknowledges that individuals may share “sensitive information” on WeChat, “such as information about your race or ethnic origin, religious or philosophical views or personal health” and that “content and information that you input to WeChat, such as photographs or information about your school or social activities, may reveal your sensitive Personal Information to

<sup>67</sup> WeChat (2018), “WeChat -- Terms of Service,” *WeChat* (March 21, 2018) <[https://www.wechat.com/en/service\\_terms.html](https://www.wechat.com/en/service_terms.html)>.



others.”<sup>68</sup> WeChat is not providing an exclusive listing of what constitutes sensitive information; even what is listed, however, might be inclusive of political speech where it is aligned with philosophical views. Further, sensitive information exists in multiple kinds of shared content and not just the text that is typed. As such, sensitive information—including communicating certain philosophical views—might be found in photos and, presumably, documents or other kinds of files.

Analysis of international users’ communications are also authorized in the privacy policy and terms of service documents that they agree to. WeChat International includes a standard, broadly encompassing, class of language which authorizes them to transmit users’ communications without running afoul of copyright claims. Specifically, the company’s public-facing documentation includes:

**“you are giving us and our affiliate companies a perpetual, non-exclusive, transferable, sub-licensable, royalty-free, worldwide licence to use Your Content (with no fees or charges payable by us to you) for the purposes of providing, promoting, developing and trying to improve WeChat and our other services, including new services that we may provide in the future... As part of this licence, we and our affiliate companies may, subject to the our WeChat Privacy Policy, copy, reproduce, host, store, process, adapt, modify, translate, perform, distribute and publish Your Content worldwide in all media and by all distribution methods, including those that are developed in the future.”<sup>69</sup>**

WeChat might further justify analyzing content based on the assertion that the company “may be required to retain or disclose Your Content in order to enforce these Terms or to protect any rights, property or safety of ours, our affiliate companies or other users of WeChat.”<sup>70</sup> Content might be retained per this language, as well as assessed, if it is found to infringe upon “any rights, property or safety of ours” or the company’s “affiliate companies or other users of WeChat.” Specifically, without a better understanding of the way(s) in which WeChat’s international and China operations are associated, such as whether they constitute affiliate companies or China-registered WeChat accounts are “other users of WeChat” per the international company’s terms of service and privacy policy, it is challenging to definitively know

68 WeChat (2018), “WeChat Privacy Protection Summary,” *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>. See “Sensitive Personal Information.”

69 WeChat (2018), “WeChat -- Terms of Service,” *WeChat* (March 21, 2018) <[https://www.wechat.com/en/service\\_terms.html](https://www.wechat.com/en/service_terms.html)>.

70 WeChat (2018), “WeChat -- Terms of Service,” *WeChat* (March 21, 2018) <[https://www.wechat.com/en/service\\_terms.html](https://www.wechat.com/en/service_terms.html)>.

if these elements of the company's international public policy documentation authorize the analysis the content of international users' communications for that which is 'sensitive' in China, or the hashing of such content of communications, or the sharing the results with the Shenzhen-domiciled element of the company.

In contrast, the terms of services and privacy policies WeChat enforces on its China-registered accounts include a clear statement that would authorize the company to conduct content surveillance for the purpose of content blocking. Specifically, WeChat China's terms of services state that:

**"If Tencent finds or receives any report or complaint from others against the user on violation to this Agreement, Tencent is entitled to remove or obscure relevant contents at any time without notice, impose punishment on the violating account including but not limited to warning, restriction or prohibition of the use of some or all of the functions, account banning or cancellation, and announce the results of treatment."**<sup>71</sup>

In line with WeChat International's documents which justify the analysis of international users' communications for security and performance improvement reasons, the language used in the policy documents pertaining to WeChat's China-registered accounts allows Tencent to read and analyze users' communications.<sup>72</sup>

In conclusion, it remains highly plausible that WeChat could attempt to justify subjecting its international users' communications to content surveillance based on the contents of the company's public-facing policy document. Moreover, the company can clearly engage in content surveillance of the communications transmitted using China-registered accounts. To be entirely certain about the policy rationale undergirding content surveillance of international users' communications, however, the company's international data protection officer would have needed to reply to our letter. We have not received a response as of this report's publication date.

71 Weixin (n.d.), "Agreement on Software License and Service of Tencent Weixin," *Weixin* (n.d.) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=default&c-c=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=default&c-c=CN)> [<https://perma.cc/5KRJ-28NE>]

72 Weixin (n.d.), "Agreement on Software License and Service of Tencent Weixin," *Weixin* (n.d.) <[https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin\\_agreement&s=default&c-c=CN](https://weixin.qq.com/cgi-bin/readtemplate?lang=en&t=weixin_agreement&s=default&c-c=CN)> [<https://perma.cc/5KRJ-28NE>]. According to the Agreement of Software License and Service of Tencent Weixin, "to the extent permitted by laws, Tencent is granted to use the non-confidential contents uploaded or published by you (such as video published via Time Capsule, selfie stickers) for achieving the performance of the Software and Services, including without limited to storage, displaying to relevant users, granting and allowing other use."



### 3.3.2 Enabling Content or Metadata Disclosure

In specifically assessing the policies to ascertain whether they do, or do not, permit the disclosure of international users' communications content or metadata to parties in China, we found that the permissibility of such disclosures remained ambiguous. On the one hand, the international entity denoted a specific list of subsidiary international organizations with whom it might disclose information, and then more broadly identified classes of external organizations—such as those that enable SMS delivery or VoIP functionality—that might receive information about the user or their usage of WeChat. It is possible that these subsidiary or third-party organizations might, themselves, have disclosure policies that include sharing information about international users' communications with a China-based organization that ultimately routes data to WeChat's China-based entity. However, if this is the case, and presuming it is typical behaviour, then the failure to specify such practices would be misleading to someone who had read the privacy policy and terms of service with the intent of learning how the company typically handled users' communications. Should such disclosures be sufficiently irregular that they do not merit including information about them in the public-facing policy documents, then WeChat could and should notify individuals that data is being disclosed when it takes place, such as through in-app dialogues or automated chat sessions initiated by the company. Ultimately, then, while it is possible that the public-facing policy documents might authorize the sharing of international users' data with WeChat China, the prospect of this sharing is not clear or apparent from reading these policies.

Similarly ambiguous is how WeChat's China-based entity handles communications between its China and international users. The policy documents pertaining to WeChat's users with a China-registered account state that the company "may use information collected by certain features for our other services." Whereas these policy documents make it clear that Tencent does not share or transfer personal information to third parties outside of Tencent, it is left unclear how or whether information and contents of internationally-based users of Tencent-affiliated services are shared within the company.

In summary, it remains unclear on what basis the hashes of international users' communications might be disclosed to WeChat China. To be certain on what basis, if any, WeChat justifies the sharing of hashes between the international and China-specific iterations of WeChat, the company's international data protection officer would have had to reply to the letter we issued to them. As of publication, however, the company has failed to even acknowledge their receipt of the messages we have sent them, let alone respond to the questions we posed to the company.



## Part 4. Data Access Request Assessment

Tencent is subjected to the Personal Information Protection and Electronic Documents Act (PIPEDA) because it has a substantial commercial connection to Canada by merit of doing business with persons residing in Canada and because some of the company's data centres are located in Canada.<sup>73</sup> Principle 4.9 of PIPEDA outlines Canadians' access and correction rights; Canadians have a right to "be informed of the existence, use, and disclosure of their personal information and be given access to that information."<sup>74</sup> Individuals may have to prove their identity so that companies can retrieve their information. Organizations must provide some response to the requester within thirty days and may (as part of that response) inform requesters that the company is availing itself of an additional thirty days to prepare a response. Access should be provided at a minimum, or zero, cost.

In this section of the report, we discuss and assess the findings which emerged from filing a PIPEDA-based data access request upon Tencent's international business. Overall, while we found that there was a limited data export tool that employees were quick to help us use, the employees would not respond to questions about data not contained in the export tool, inclusive of how images were hashed, or whether such hashes were shared with WeChat China.

### 4.1 Methodology

One of the project researchers created a non-China-registered WeChat account. From this account, the researcher communicated with other accounts which our team created, all of which were registered internationally.<sup>75</sup> Specifically, the researcher transmitted unique and sensitive chat messages, documents, and images in a group chat which contained two other non-China-registered accounts. To confirm that the hashes of the documents and images were added to the hash index, a pair of experiments were conducted, as discussed in Section 2.

<sup>73</sup> WeChat (2018), "WeChat Privacy Protection Summary," *WeChat* (May 10, 2018) <[https://www.wechat.com/en/privacy\\_policy.html](https://www.wechat.com/en/privacy_policy.html)>. See "Where do we process your data"; see also: Office of the Privacy Commissioner of Canada (2017), "Commercial Activity," *Office of the Privacy Commissioner of Canada* (January 30, 2017) <[https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations\\_03\\_ca/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/)>.

<sup>74</sup> Office of the Privacy Commissioner of Canada (2013), "Access to Personal Information," *Office of the Privacy Commissioner of Canada* (May 16, 2013) <[https://www.priv.gc.ca/leg\\_c/interpretations\\_05\\_access\\_e.asp](https://www.priv.gc.ca/leg_c/interpretations_05_access_e.asp)>.

<sup>75</sup> The contents of these communications are detailed in Section 2.

We used PIPEDA-based data access requests to better understand the kinds of personal information that Tencent collects when an international user installs WeChat and uses the service. In particular, we explored whether such requests could be used to reveal to international users that the content of their communications were being used to develop the hash index which was used to censor the communications of China-registered accounts.

The researcher filed two rounds of personal information requests. The first round entailed two separate emails: one to Tencent's international data protection office, and the second to Tencent's China-based data protection office. The second round entailed a single follow-up email to Tencent's international data protection office.

#### **4.1.1 Round One Data Access Request**

The first request asked questions about the different kinds of data which might be collected in the course of using WeChat, inclusive of geolocation information, IP address logs, subscriber information, personally identifiable information, as well as any information pertaining to communications between users, any MD5 hashes of the content of communications exchanged using WeChat, or whether any communications sent using WeChat had been found to violate Tencent's terms of service and, if so, whether such violations pertained to violations associated with users who were located in China. The request also asked the company to disclose whether the content of any communications, or hashes derived from such communications, had been used to enable or optimize the detection of terms of service violations for users located in the People's Republic of China or any other jurisdiction. The request, finally, asked Tencent to disclose if any personal information, or information about the researcher's account or devices, had been shared with any other third-parties and, in the request made to Tencent Singapore, specifically whether it had been shared or disclosed with Shenzhen Tencent Computer Systems Company Limited. Shenzhen Tencent Computer Systems Company Limited is the portion of the company that is domiciled in the People's Republic of China and, thus, is required to comply with Chinese law that mandates the blocking of particular content that is communicated using WeChat. The letter cited PIPEDA and informed Tencent of its requirement to respond within thirty days and at a minimal cost.

Copies of this request as sent to the Tencent Shenzhen and Tencent Singapore data protection offices are available in Appendices B and C, respectively.



### 4.1.2 Round Two Data Access Request

After receiving an initial response—discussed in Section 4.2—another letter was sent which reiterated requests for the below data:

- Communications between the researcher and other users.
- The geographic location where data which the researcher contributed to the WeChat social network was stored and, more specifically, whether any of the data was stored in the People’s Republic of China.
- Social networking information, inclusive of MD5 hashes or other hashes computed upon the researcher’s chat messages, images, or files sent using the service.
- Results indicating whether any of the chat messages, images, or files sent using the service had been determined to violate the company’s terms of service and, if so, the basis for which these messages were categorized as violating the terms of service.

In cases where the data was not retained, the researcher asked that Tencent positively confirm that the data was not retained.

The follow-up letter also asked Tencent to disclose “whether (and, if so, which of) any of my chat messages, images, or files sent using your service, or any hashes computed upon these items, have been used for the purposes of detecting terms of service violations for users located in the People’s Republic of China or any other jurisdiction” as well as “whether (and, if so, which of) any of my chat messages, images, or files sent using your service, or any hashes computed upon these items, have been shared with, or disclosed to, Shenzhen Tencent Computer Systems Company Limited either by Tencent International Service Pte. Ltd. or a subsidiary, and to which other parties in China or outside China (inclusive of all subsidiaries) with whom this data has been shared.”

A copy of this letter is in [Appendix D](#).

## 4.2 Data

The first data access request (“PIPEDA request”) was sent on November 29, 2019, to the email address associated with the Tencent Shenzhen and Tencent Singapore data protection offices. Our interactions with Tencent Singapore took place according to the following timeline:

- December 2: Tencent provided instructions to access and use WeChat's "Export Personal Data" tool
- December 2: Researcher informed Tencent that, although they were using the latest version of the app, they could not find an "Export Personal Data" tool using the provided instructions
- December 5: Tencent responded that they can facilitate the data export but, to do so, the researcher had to verify their identity. Identity verification was based on providing eight different items for verification. Tencent requested that the researcher provide as many as possible
- December 5: Researcher provided Tencent with the eight items for verification
- December 16: Tencent responded by directing the researcher to paste a link<sup>76</sup> into a WeChat chat and to open the URL in WeChat to export the personal data
- December 18: The researcher followed the instructions. Using the export tool accessible from the link, the researcher was required to confirm their email address. After confirming their email address, the researcher was automatically emailed a link to a web page that provided a downloadable \*.zip file that contained information pertaining to the researcher's use of the application

The \*.zip included the following information:

- Personal account information: WeChat ID, Registration Region, Linked Accounts (i.e., email attached to the account), Registration Time, and Phone Number.
- Contact Data: Friends and Group Chat Contacts. No accounts were listed under the latter category.<sup>77</sup>
- Moments Data: My Moments, My Comments and Likes, Hide My Moments, and Hide User's Moments. No information was provided in this category, presumably because the researcher did not use these aspects of WeChat.
- Location and Login Information: Location Information and Login Devices. The latter identified the mobile device the researcher used while interacting with WeChat, whereas no information was presented for the former category.

Information which was requested in the initial letter but not provided in the response included:

<sup>76</sup> The URL we were provided was: <https://support.weixin.qq.com/security/readtemplate?t=exportdata/index>

<sup>77</sup> We did not explore how WeChat differentiated between Friends and Group Chat Contacts.



- IP address log information
- Information pertaining to whether and, if so, how the researcher's communications data was used to generate the censorship index for China-registered accounts
- Information of whether information about the researcher—inclusive of account information, communications content, or MD5 hashes of their content—had been shared with any third-parties

The second round of the data access request sent on December 18 reiterated that the researcher sought access to information discussed in Section 4.1.2. No subsequent communications have been received by Tencent Singapore as of the time of publication.

At no point did the researcher receive a response to the letter that they issued to Tencent Shenzhen.

### 4.3 Discussion

The data which Tencent Singapore provided to the researcher fell short of the information which had been requested. Most notably, it excluded information that was principally sought concerning the extent to which, and rationales upon which, derived elements of the researcher's communications might have been communicated to other parties such as Tencent Shenzhen. This failure took place despite the researcher's repeated engagements with Tencent Singapore employees; they were actively involved in communicating with the researcher to guide them to the Export Personal Data tool, but failed to provide substantive communications concerning the most pressing of the researcher's questions about the company's data handling practices.

Tencent Singapore's response, which directed users to a data export tool, parallels past experiences of researchers who have sought access to information retained by other companies, including fitness tracker companies and social media companies. Specifically, data export tools have been shown to not include all of the information that users provide to services, and companies routinely fail to answer questions about data collection, processing, and storage beyond what is presented through data export tools.<sup>78</sup> However, in the case of Tencent there is evidence—as denoted

<sup>78</sup> Parsons, Christopher, Andrew Hiltz, and Masashi Crete-Nishihata (2018), "Approaching Access: A comparative analysis of company responses to data access requests in Canada," *Citizen Lab* (February 12, 2018) <[https://citizenlab.ca/wp-content/uploads/2018/02/approaching\\_access.pdf](https://citizenlab.ca/wp-content/uploads/2018/02/approaching_access.pdf)>; Tsui, Lokman and Stuart Hargreaves (2019), "Who Decides What Is Personal Data? Testing

in Section 2—that either the Singapore or Shenzhen part(s) of the company are using non-China-registered users’ communications to develop a hash index that is subsequently applied to censor communications between a subset of Tencent’s user base: those who have registered their accounts in China.

Moreover, in cases where individuals are specifically asking about how their communications are treated—in this case, whether and why the contents of communications are subject to content surveillance and where the content of communications are stored—it is reasonable for a company to provide such information in a good faith effort to explain its data processing practices. The terms of service and privacy policy which applied to the service were ambiguous in how the company handled users’ data. Thus, the questions that were posed by our researcher constituted the sole remaining non-technical method that individuals might use to understand WeChat’s international data collection, processing, and storage activities.<sup>79</sup>

To explain the company’s handling of user data, it might have crafted a specific letter or other communication to a user. It might also have directed the user to a specific part of a company’s privacy policy or terms of service document to clarify how the company might interact with the contents of users’ communications. Tencent Singapore did not engage in either of these types of clarifying activities, preventing international users of the WeChat service from understanding how the company treats the contents of their communications, knowing who has access to or obtains the contents of their communications or derivations of them, or even where data is being stored.

## Part 5 - Conclusion

In this report, we present technical experiments which reveal that WeChat communications that are conducted entirely among non-China-registered accounts are subject to content surveillance. We found that documents and images that were transmitted entirely among non-China-registered accounts were analyzed for Chinese political sensitivity. Upon analysis, files deemed politically sensitive were

---

the Access Principle with Telecommunication Companies and Internet Providers in Hong Kong,” *International Journal of Communication* 13.

79 For details on how, and why, the terms of service and privacy policy were ambiguous on the issues of data collection, processing, and storage, see Section 3 of this report.



used to invisibly train and build up WeChat's Chinese political censorship system. We also conducted analysis of WeChat's public-facing policy documents, made data access requests, and engaged with Tencent data protection representatives to assess whether those methods could also explain, or uncover, the content surveillance carried out towards international users' communications. We found that none of the information WeChat makes available to users explains the rationales for such surveillance or the transmission of content hashes from WeChat International to WeChat China.

The failure of data protection officials to respond to our questions regarding WeChat's privacy policies is particularly notable given that Tencent staff were initially quick to assist our researchers in using an automated data-export tool associated with WeChat's commitment to facilitate access, modification, and removal of international users' content. Perhaps, however, the failure is less surprising given that the same staff were unwilling to provide any assistance or information above and beyond helping us use this tool: our more specific data access request questions were never acknowledged, let alone responded to.

Companies operating around the world staff their companies with privacy and data protection professionals to, in part, ensure that questions about companies' policies can be addressed. In the case of WeChat's international operations, however, it remains unclear to whom users can turn if they want to understand the company's policies. In the case of WeChat's failure to explain its content surveillance policies, as well as the apparent retention of hashes of content even after a user has recalled it, makes clear that the company must more meaningfully communicate with its users. However, as of today, individuals clearly cannot turn to the designated staff working at WeChat international and speak to individuals that users would rightly expect to be able to answer these kinds of questions.

Tencent has not only failed to explain to its international users how their communications content is being used to facilitate the censorship apparatus that is applied to China-registered WeChat accounts, but the company has also failed to explain, or clarify, whether international users' communications content are subject to surveillance that is not associated with the censorship of content that is deemed sensitive in China. Put another way, the content surveillance and hashing system we discuss in this report is at least part of the broader censorship system which has been fully deployed towards China-registered accounts. The infrastructure for hashing communications between internationally registered accounts exists and could, in theory, be (re)purposed to hash additional kinds of sensitive files (e.g.,



files associated with terrorism or child abuse imagery or leaked documents which governments do not want to have circulated about their operations). It is unclear how challenging it would be to repurpose the existing system(s) for determining what is, and is not, sensitive content, nor whether significant engineering efforts would be required to integrate the censorship system that is currently applied to China-registered accounts to internationally registered accounts.

Granted, social media surveillance and content moderations are not unique to WeChat. Surveillance constitutes a fundamental feature of all mainstream profit-oriented social media businesses.<sup>80</sup> As companies push to grow products internationally, they will inevitably experience pressures from governments to remove content or provide user data, as demonstrated by the requests documented in annual corporate transparency reports.<sup>81</sup> In the case of China, attention is typically centered on foreign companies that are attempting to enter the Chinese market and must decide whether and how to comply with the government's strict content regulations. Recent revelations of Google working on a search engine to enable geographically-based filtering features in an effort to re-enter China is but the latest example.<sup>82</sup>

While content surveillance and content moderation are ubiquitous across social media platforms, our research findings point to a worrying situation where globalized companies extend information controls beyond the borders of their home country and incorporate these practices into general product designs and business operations. There are at least three potential reasons why Tencent has designed its surveillance and censorship system in such a way. First, it may have been an intentional design decision for the purpose of complying with China's political and regulatory restrictions (e.g., only using communications among China-registered accounts to train their censorship system may be ineffective if those

80 Ronald Deibert (2019), "The Road to Digital Unfreedom: Three Painful Truths About Social Media," *Journal of Democracy* 30(1).

81 Parsons, Christopher (2016), "Transparency in Surveillance: Role of various intermediaries in facilitating state surveillance transparency," *Centre for Law and Democracy* <<http://responsible-tech.org/wp-content/uploads/2016/06/Parsons.pdf>>. Transparency reports may not, however, be particularly effective in genuinely expressing the regularity at which governments attempt to block, or have content taken down. For more, see Parsons, Christopher (2017), "The (In)effectiveness of Voluntarily Produced Transparency Reports," *Business & Society* <<http://journals.sagepub.com/doi/full/10.1177/0007650317717957>>.

82 McKune, Sarah, Ronald Deibert (2018), "Google's Dragonfly: A Bellwether for Human Rights in the Digital Age," *Just Society* <<https://www.justsecurity.org/59941/googles-dragonfly-bellwether-human-rights-digital-age/>>.

users are prevented from engaging in the very censored topics needed to train the system). Second, it may be a side effect of technical efficiency considerations (e.g., it may be simpler to engineer a platform that performs political content surveillance on all communication versus only on some). Finally, it may be a side effect of a content blocking system enabled for non-China-registered users which does not block Chinese political content but possibly does block other kinds (e.g., possibly terrorism content or pornography). In the case of our findings, there is no evidence attributing Tencent's surveillance behaviours enforced on international WeChat users to the direction of the Chinese government. We cannot conclusively determine which of these scenarios is true and it is possible there are other explanations that we have not considered. Regardless of the reasons, the implications of our research are clear: users of WeChat are not provided sufficient transparency into how their data is used to understand whether and how their data enables political censorship in other jurisdictions.

Building on the findings in this report, there are multiple avenues for future research. The technical experiments that we developed are capable of detecting content surveillance of documents and images on WeChat. However, our methodology, insofar as it relies on using WeChat's censorship hash index as a side channel, cannot be used to test whether there is surveillance of chat message text sent entirely among non-China-registered accounts. WeChat automatically censors chat message contents from or to China-registered accounts if they contain a blacklisted keyword combination, but it is currently an open question as to how WeChat generates or maintains these keyword combination blacklists. These keyword blacklists may be generated from users' communications similarly to how the hashes of users' images and documents populate WeChat's censorship hash index. Further research is required to explore if these keyword blacklists are built up from chat text sent among non-China-registered users in the same way as these users' communications contribute to the document and image hash index.

Furthermore, our report looked at one platform, Tencent's WeChat, and found that Tencent uses non-China-registered users' communications to build up its censorship system. Future work is required to understand if this behaviour is unique to Tencent or if it is common for internationally operating Chinese social media companies to use communications among their non-Chinese users to implement Chinese political censorship.



# Appendix

## A. Letter to WeChat Data Protection Office

Attn: Data Protection Officer  
Tencent International Service Pte. Ltd.  
10 Anson Road  
#21-07 International Plaza  
Singapore  
079903

Dear Tencent Data Protection Officer,

I am writing to you to learn more about how Tencent International handles and manages the data which is communicated by its users. Specifically, and in light of allegations concerning how competing services such as TikTok may be censoring certain classes of content, I want to better understand the division of the communications services provided to domestic Chinese users of WeChat versus the services provided to international users of WeChat's communications services.

I am particularly curious to know whether any of the communications content or metadata that WeChat's international users send to other international users is ever used to update, modify, or otherwise interact with the blocklists that Tencent is lawfully required to apply to communications between domestic Chinese WeChat users. In reading your company's international terms of service and privacy policy, it seemed like the respective policies might permit such activities. The specific questions that I have about Tencent International's communications service offerings follow.

- 1) In the discussion of "Types of Information We Process", Tencent International acknowledges that it collects log information such as metadata, which is "information related to items you have made available through WeChat, such as the date, time or location that a shared photograph or video was taken or posted." Would such metadata include a hash of the files or other contents shared using WeChat communications services? And, if so, could such hashes be used in the development or maintenance of the domestic blocklist system that

WeChat is lawfully obligated to apply to its domestic Chinese users?

- 2) In the discussion on how Tencent International processes its users' information, there is a section entitled "Pseudonymised and Aggregated Data", which notes that some activities are undertaken within the app to facilitate fraud detection and undertake account safety analysis. Does, or would, this section authorize Tencent International to process communications between its international users for the purpose of developing the domestic blocklist system that Tencent is lawfully obligated to apply to its domestic Chinese users?
- 3) In the WeChat Privacy Policy, Tencent International acknowledges that it may share information with government, public, regulatory, judicial and law enforcement bodies or authorities "where we are required to comply with applicable laws or regulations, a court order, subpoena or other legal process, or otherwise have a legal basis to respond to a request for data from such bodies, and the requesting entity has valid jurisdiction to obtain your personal information". Has Tencent International ever, or does Tencent International currently, disclose information pertaining to international WeChat users to such bodies in China, for the purposes of complying with legal requests directed at enhancing, developing, or maintaining the blocklists that Tencent is lawfully obliged to apply to its domestic Chinese users?
- 4) The WeChat Privacy Policy denotes a range of international Tencent subsidiaries with whom international WeChat users' information might be shared. Is it the case that no log data, non-personal data, personal information, or shared information is disclosed to Tencent's Shenzhen-operated domestic business? If information is shared between the Tencent international businesses which are involved in the operation of the communications service offered to international users, can you clarify which specific information is provided and how it is classified by the company (i.e., as log data, non-personal data, personal information, or shared information)?
- 5) The WeChat Terms of Service document indicates that Tencent International's business may "share Your Content with third parties that we work with to help provide, promote, develop and improve WeChat in accordance with the WeChat Privacy Policy". Can you confirm that



such sharing does not include the disclosure of log data, non-personal data, personal information, or shared information with Tencent's China-domiciled business operations? If some data is shared from the international business with the China-domiciled business operations, can you clarify what data is specifically shared and the purposes behind such sharing processes?

- 6) The WeChat Terms of Service document indicates that Tencent International "may be required to retain or disclose Your Content in order to enforce these Terms or to protect any rights, property or safety of ours, our affiliate companies or other users of WeChat." Can you clarify whether, under these terms, Tencent International would be permitted to share an international user's content with the China-domiciled elements of Tencent's business operations? And, if these terms would authorize such sharing, whether and under what conditions such sharing would take place?
- 7) The WeChat Terms of Service document denotes that Tencent International's international users provide the company and its affiliate companies "a perpetual, non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use Your Content (with no fees or charges payable by us to you) for the purposes of providing, promoting, developing and trying to improve WeChat and other services ... As part of this license, we and our affiliate companies may, subject to the WeChat Privacy Policy, copy, reproduce, host, store, process, adapt, modify, translate, perform, distribute and publish Your Content worldwide in all media and by all distribution methods[.]" Can you clarify whether, under these terms, Tencent International would be permitted to share an international user's content with the China-domiciled elements of Tencent's business operations? And, should these elements of the Terms of Service document authorize such sharing of an international user's data with the China-domiciled elements of Tencent's business operations, would such data ever be shared for the purposes of enhancing, developing, or maintaining the blocklists that Tencent is lawfully obliged to apply to its domestic Chinese users?
- 8) The aforementioned questions have, generally, sought to understand whether there are terms, conditions, or policies which would authorize



Tencent International's businesses to share international user's log data, non-personal information, personal information, shared information, or other classes of information to Tencent's China-domiciled businesses, or any other Tencent businesses operating within the People's Republic of China. Is it the case that such international users' information is never transmitted to the China-domiciled businesses, or any other Tencent businesses or affiliates operating within the People's Republic of China, for the purposes of enhancing, developing, or maintaining the blocklists that Tencent is lawfully obliged to apply to its domestic Chinese users?

Thank you for your attention to these questions, and in advance for the time that you may commit in responding to these questions. If you have any additional questions regarding this letter, please feel welcome to contact me at: [Researcher email address].

Best Regards,

[Name]

## **B. PIPEDA Data Request to Shenzhen Tencent Computer Systems Company Limited**

November 29 2019

Shenzhen Tencent Computer Systems Company Limited

Tencent Legal Department (Privacy & Data Protection Centre)

Tencent Building, Kejizhongyi Avenue, Hi-tech Park, Nanshan District, 518057  
Shenzhen, People's Republic of China

Re: Subject access request

Dear Sir or Madam,

I am a customer of WeChat, and I am interested in both learning more about your data management practices and the personal data you process about me. This is a request to access my personal data under Principle 4.9 of Schedule 1 and section

8 of Canada's federal privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA).

I am requesting a copy of all records which contain my personal information from your organization.

The following is a non-exclusive listing of all information that your organization may hold about me, including the following:

- **Mobile app data:** Information collected about me, or persons/devices associated with my account, using one of your company's mobile device applications
- **Geolocation data:** collected about me, my devices, and/or associated with my account (e.g. GPS information, cell tower information)
- **IP address logs:** associated with me, my devices, and/or my account (e.g. IP addresses assigned to my devices/router, IP addresses or domain names of sites I visit and the times, dates, and port numbers)
- **Subscriber information:** that you store about me, my devices, and/or my account
- **Personally identifying information:** that is unique to me, my devices, and/or my account, such as name, email addresses, phone numbers, responses to relationship questions, or device identifiers.
- **Any additional kinds of information:** that you have collected, retained, or derived from the mobile or website services you provide, including but not limited to:
  - a) communications between myself and other users;
  - b) social networking information, inclusive of MD5 hashes or other hashes computed upon my chat messages, images, or files sent using your service;
  - c) whether any of the chat messages, images, or files sent using your service have been determined to violate your terms of service and, if so, whether any such terms of service violations pertain to violations associated with users who are located in the People's Republic of China; and
  - d) whether any of my chat messages, images, or files sent using your service, or any hashes computed upon these items, have been used to enable/optimize detecting terms of service



violations for users located in the People's Republic of China or any other jurisdiction.

- **Disclosures to third parties:** Any information about disclosures of my personal information, or information about my account or devices, to other parties, including law enforcement and other state agencies. I am specifically interested in knowing whether and which of my information has been shared with, or disclosed to, Tencent International Service Pte. Ltd., and to which parties in China or outside China with whom my data has been shared.

If your organization has other information in addition to these items, I formally request access to that as well. If your service includes a data export tool, please direct me to it, and ensure that in your response to this letter, you provide all information associated with me that is not included in the output of this tool. Please ensure that you include all information that is directly associated with my name, phone number, e-mail, or account number, as well as any other account identifiers that your company may associate with my personal information. Finally, please provide this data, where possible, in a structured and non-proprietary digital format.

You are obligated to provide copies at a free or minimal cost within thirty (30) days of receipt of this message. If you choose to deny this request, you must provide a valid reason for doing so under Canada's PIPEDA. Ignoring a written request is the same as refusing access. See the guide from the Office of the Privacy Commissioner at: [http://www.priv.gc.ca/information/guide\\_e.asp#014](http://www.priv.gc.ca/information/guide_e.asp#014). The Commissioner is an independent oversight body that handles privacy complaints from the public.

Please let me know if your organization requires additional information from me before proceeding with my request.

Here is my information that may help you identify my records:

- First Name: [name]
- Last Name: [name]
- Email Address: [email address]
- Telephone Number: [phone number]

Sincerely,

[name]

## C. PIPEDA Data Request to Tencent International Service Pte. Ltd., #1

November 29 2019

Tencent International Service Pte. Ltd.

10 Anson Road, #21-07 International Plaza, Singapore 079903

Re: Subject access request

Dear Sir or Madam,

I am a customer of WeChat, and I am interested in both learning more about your data management practices and the personal data you process about me. This is a request to access my personal data under Principle 4.9 of Schedule 1 and section 8 of Canada's federal privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA).

I am requesting a copy of all records which contain my personal information from your organization.

The following is a non-exclusive listing of all information that your organization may hold about me, including the following:

- **Mobile app data:** Information collected about me, or persons/devices associated with my account, using one of your company's mobile device applications
- **Geolocation data:** collected about me, my devices, and/or associated with my account (e.g. GPS information, cell tower information)
- **IP address logs:** associated with me, my devices, and/or my account (e.g. IP addresses assigned to my devices/router, IP addresses or domain names of sites I visit and the times, dates, and port numbers)
- **Subscriber information:** that you store about me, my devices, and/or my account
- **Personally identifying information:** that is unique to me, my devices, and/or my account, such as name, email addresses, phone numbers, responses to relationship questions, or device identifiers.
- **Any additional kinds of information:** that you have collected, retained, or derived from the mobile or website services you provide, including but not limited to:



- e) communications between myself and other users;
  - f) social networking information, inclusive of MD5 hashes or other hashes computed upon my chat messages, images, or files sent using your service;
  - g) whether any of the chat messages, images, or files sent using your service have been determined to violate your terms of service and, if so, whether any such terms of service violations pertain to violations associated with users who are located in the People's Republic of China; and
  - h) whether any of my chat messages, images, or files sent using your service, or any hashes computed upon these items, have been used to enable/optimize detecting terms of service violations for users located in the People's Republic of China or any other jurisdiction.
- **Disclosures to third parties:** Any information about disclosures of my personal information, or information about my account or devices, to other parties, including law enforcement and other state agencies. I am specifically interested in knowing whether and which of my information has been shared with, or disclosed to, Shenzhen Tencent Computer Systems Company Limited, and to which other parties in China or outside China with whom my data has been shared.

If your organization has other information in addition to these items, I formally request access to that as well. If your service includes a data export tool, please direct me to it, and ensure that in your response to this letter, you provide all information associated with me that is not included in the output of this tool. Please ensure that you include all information that is directly associated with my name, phone number, e-mail, or account number, as well as any other account identifiers that your company may associate with my personal information. Finally, please provide this data, where possible, in a structured and non-proprietary digital format.

You are obligated to provide copies at a free or minimal cost within thirty (30) days of receipt of this message. If you choose to deny this request, you must provide a valid reason for doing so under Canada's PIPEDA. Ignoring a written request is the same as refusing access. See the guide from the Office of the Privacy Commissioner at: [http://www.priv.gc.ca/information/guide\\_e.asp#014](http://www.priv.gc.ca/information/guide_e.asp#014). The Commissioner is an independent oversight body that handles privacy complaints from the public.



Please let me know if your organization requires additional information from me before proceeding with my request.

Here is my information that may help you identify my records:

- First Name: [name]
- Last Name: [name]
- Email Address: [email address]
- Telephone Number: [phone number]

Sincerely,

[name]

## **D. PIPEDA Data Request to Tencent International Service Pte. Ltd., #2**

November 29 2019<sup>83</sup>

Tencent International Service Pte. Ltd.

10 Anson Road, #21-07 International Plaza, Singapore 079903

Dear Data Protection/Privacy Officer,

Thank you for providing me access to your data export tool. However, the data provided by this tool did not include all of the data that I requested.

For the following items, please provide a copy of all retained data:

- communications between myself and other users;
- where data which I contribute to the WeChat social network is stored and, more specifically, whether any of my data is stored in the People's Republic of China;
- social networking information, inclusive of MD5 hashes or other hashes computed upon my chat messages, images, or files sent using your service; and
- results indicating whether any of the chat messages, images, or files sent

<sup>83</sup> The second letter issued to Tencent Singapore was mistakenly dated November 29, 2019, but sent by email on December 18, 2019.

using your service have been determined to violate your terms of service and, if so, the basis for which these messages were categorized as violating the terms of service;

For any listed items for which you do not retain data, please explicitly indicate that you do not retain this data.

I am also interested in how my personal information is being used. Specifically, I wish to know whether (and, if so, which of) any of my chat messages, images, or files sent using your service, or any hashes computed upon these items, have been used for the purposes of detecting terms of service violations for users located in the People's Republic of China or any other jurisdiction. For any of these items not used for this purpose, please explicitly indicate that you do not use this data for this purpose.

Finally, I am interested in knowing how my personal information is being shared. I am specifically interested in knowing whether (and, if so, which of) any of my chat messages, images, or files sent using your service, or any hashes computed upon these items, have been shared with, or disclosed to, Shenzhen Tencent Computer Systems Company Limited either by Tencent International Service Pte. Ltd. or a subsidiary, and to which other parties in China or outside China (inclusive of all subsidiaries) with whom this data has been shared. For any of these items not shared with other parties, please explicitly indicate that you do not share this data with other parties.

For your convenience I have attached a copy of my original letter.

Sincerely,

[name]







# EXHIBIT 24

# Here are all the major US tech companies blocked behind China's 'Great Firewall'

BI [businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5](https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5)

Page Last Modified: 2019-10-10T16:23:00Z



A person protesting Chinese internet censorship in Germany.

Alexander Koerner/Getty Images

- The US has blacklisted a slew of Chinese companies this year, including major tech entities like Huawei, from doing business in the country.
- On the flip side, China has long blocked major US tech companies, including Facebook and Google, from operating in the country.
- Here are the major tech companies that are blocked in China behind the country's so-called "Great Firewall" of internet censorship.
- Visit Business Insider's homepage for more stories.

The tech Cold War between US and China is running hotter than ever since the US blacklisted dozens of Chinese tech companies, including Huawei, from doing business in its country.

Meanwhile, US tech companies have been largely banned from doing business in China for years. Communist-ruled China has long maintained strict regulations on which websites and social media platforms are accessible in the country — and which are blocked behind China's so-called "Great Firewall" of internet censorship.

That ban prevents companies like Facebook, Google, and Dropbox from reaching the country's over 800 million internet users. Just this week, Apple removed two apps from its App Store that are seen as potentially offensive to China. An app called HKMap Live, used by protesters in Hong Kong to track police activity, was removed after Apple said it was being used to "target and ambush police." Additionally, the US publication Quartz had its app removed from Apple's China App Store and blocked in mainland China.

Despite the ban, China still factors into the equation for US companies: Facebook, for example, saw an estimated \$5 billion in ad revenue from Chinese-based companies in 2018, making the country the company's second largest ad market, according to AdAge.

That "firewall" isn't impenetrable, either, as some Chinese citizens have found ways to circumvent blocks on websites by using virtual private networks (VPNs).

**Here are all the major US tech companies that are blocked from use in China, according to copyright tracker Great Fire:**



## Facebook

---

Facebook founder and CEO Mark Zuckerberg.  
Getty

**Includes:** Instagram, WhatsApp, Messenger

**When it was first blocked:** July 2009, in the wake of deadly riots in western China when the platform was used for communication among protesters. Instagram was blocked in September 2014 during pro-democracy protests in Hong Kong, and WhatsApp was blocked in September 2017.

## Google

---

Google CEO Sundar Pichai.  
Getty

**When it was first blocked:** YouTube was blocked on-and-off multiple times in the late 2000s, including in October 2007, March 2008 during riots in Tibet, and in March 2009 when it went down in the country for good.

Particular queries on Google, including those related to politics, have long been censored in China. Google.cn, the company's China-based search engine, was shut down in 2010 following disputes over censorship of search queries. Google's family of apps — including Gmail and Google Maps — have went offline multiple times, including in November 2012 and December 2014.

Reports emerged in 2018 that Google was working on a censored search engine for Chinese users called Project Dragonfly. The project was reportedly cancelled in December after facing outrage from Google employees and human rights groups, but some activists are not fully convinced Google has officially scrapped plans.

## Twitter

---

Twitter cofounder and CEO Jack Dorsey.  
Associated Press

**Includes:** Periscope

**When it was first blocked:** June 2009, shortly before the 20th anniversary of the Tiananmen Square protests in 1989, when the Chinese army killed hundreds of students demanding democracy.

Despite the ban, Twitter still has an estimated 10 million active users in China, who use VPNs to circumvent the ban.

## Snapchat

---

Snapchat cofounder & CEO Evan Spiegel.  
Matt Winkelmeyer/Getty Images

**When it was first blocked:** It's unclear when Snapchat was initially banned in China, but the social platform does have a small office in the country to work on Spectacles, Snap's camera-equipped smart sunglasses.

## Reddit

---

Reddit cofounder and CEO Steve Huffman.  
Guru Khalsa

**When it was first blocked:** August 2018, although many Redditors were more surprised the site hadn't been banned earlier.

## Tumblr

---

Ilya S. Savenok/Getty Images

**When it was first blocked:** May 2016, although pages containing political and pornographic content have been heavily censored in China before then.

## Pinterest

---

Pinterest cofounder and CEO Ben Silbermann.  
Hollis Johnson/Business Insider

**When it was first blocked:** March 2017, around the time when China was hosting its annual "Two Sessions" political gathering.

## Slack

---

Slack cofounder & CEO Stewart Butterfield.  
Getty

**When it was first blocked:** The timeline of when Slack was first blocked in China is not clear, but access to the messaging app has been "somewhat inconsistent" for years, according to the company itself.

## Twitch, an Amazon subsidiary

---

Twitch CEO Emmett Shear.

Getty/Steve Jennings

**When it was first blocked:** September 2018, after app downloads skyrocketed for those in China who wanted to catch e-sports matches at the 2018 Asian Games.

## Discord

---

Discord cofounder & CEO Jason Citron.

Kimberly White/Getty Images for TechCrunch.

**When it was first blocked:** Reports first surfaced in mid-2018 that users of the popular chat app for gamers were unable to access the service in China.

## Dropbox

---

Dropbox cofounder and CEO Drew Houston.

Ramsey Cardy/SPORTSFILE via Getty Images

**When it was first blocked:** May 2010. Access to Dropbox was temporarily restored in February 2014, but its website and apps were blocked again in China by that June.

## Quora

---

Quora cofounder and CEO Adam D'Angelo.

Digital First Media Group/Bay Area News via Getty Images

**When it was first blocked:** The popular Q&A site was first blocked in China in August 2018.

## Medium

---

Medium founder & CEO Evan Williams.

Diarmuid Greene/Web Summit via Sportsfile

**When it was first blocked:** The blogging site was unavailable in the country from April 2016.

## Wikipedia

---

Getty

**When it was first blocked:** Wikipedia's Chinese-language edition has been blocked for good since 2015, but China barred all language versions of Wikipedia more recently: this May.

## Vimeo

---

Sarah Jacobs/Business Insider

**When it was first blocked:** The video site went down in China pretty early, in October 2009.

## Flickr

---

Don MacAskill, CEO of Flickr parent company SmugMug.  
SmugMug/YouTube

**When it was first blocked:** The photo site went behind the "Great Firewall" in June 2007, just a few years after Yahoo bought it. Nowadays, SmugMug owns Flickr, but it doesn't appear like the site's situation in China has changed at all.

## SoundCloud

---

AP Photo/Mark Lennihan

**When it was first blocked:** The music-sharing service was first blocked in September 2013. Since then, it's been blocked in China intermittently, including in May 2015.

## DuckDuckGo

---

Washington Post via Getty Images

**When it was first blocked:** The privacy-focused search engine was blocked in September 2014.

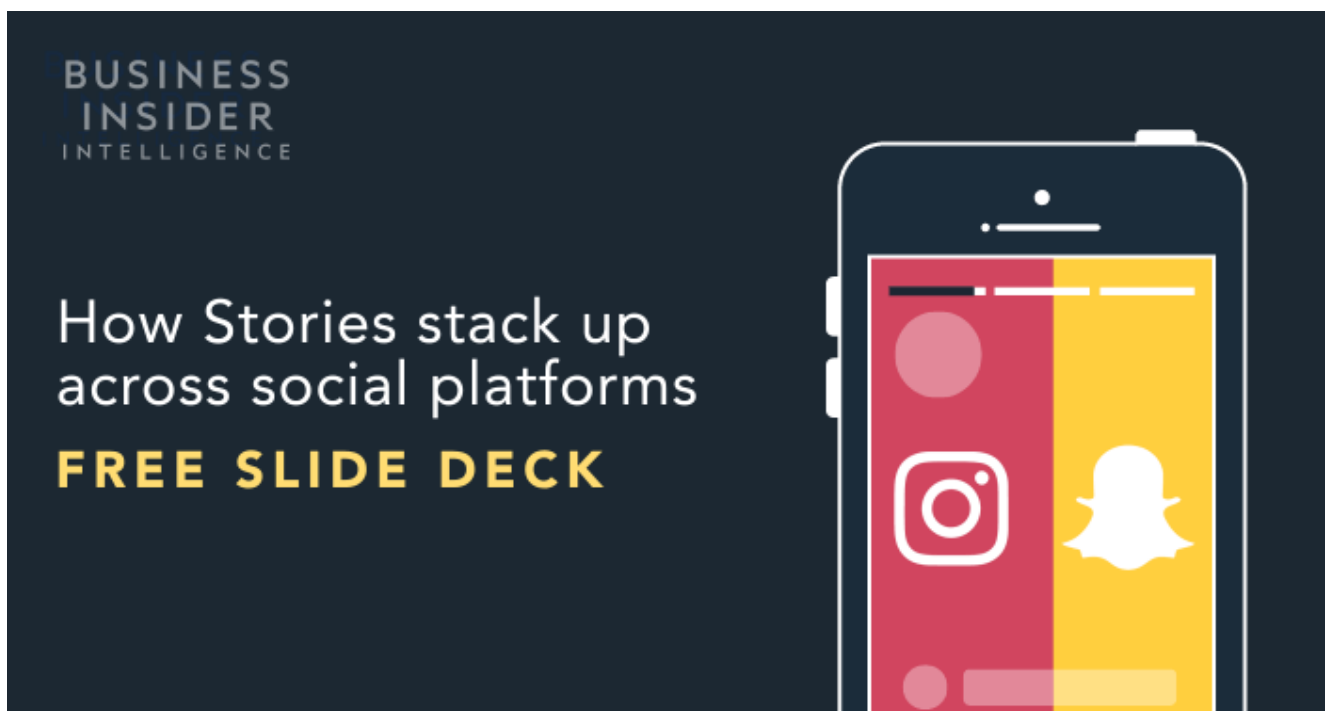
## Dailymotion

---

Dailymotion CEO Maxime Saada.  
Reuters/Jean-Paul Pelissier

**When it was first blocked:** Like several popular video-sharing sites, Dailymotion is blocked in China, although it's not clear when it went into effect.

Get the latest Google stock price here.



Get the latest Snap stock price [here](#).

Newsletter

Sign up now for Insider Today for regular insights and analysis from Henry Blodget & David Plotz.





By clicking 'Sign up', you agree to receive marketing emails from Business Insider as well as other partner offers and accept our [Terms of Service](#) and [Privacy Policy](#).



**SEE ALSO: Everything you need to know about Huawei, the Chinese tech giant accused of spying that the US just banned from doing business in America**

---

More: [Features](#) [Huawei](#) [Censorship](#) [China](#)

# EXHIBIT 25

# WECHAT – TERMS OF SERVICE

---

 [wechat.com/en/service/terms.htm](https://wechat.com/en/service/terms.htm)

## INTRODUCTION

---

Welcome to WeChat!

Your use of WeChat is subject to these Terms of Service (these "**Terms**"). Thank you for reviewing these Terms – we hope you enjoy using WeChat.

If you have any questions about, or if you wish to send us any notices in relation to, these Terms, please contact us by going to “Me” -> “Settings” -> “Help & Feedback” from within WeChat or by visiting [help.wechat.com](https://help.wechat.com).

### *Compliance with these Terms*

**These Terms apply to you if you are a user of WeChat anywhere in the world, except if you belong in any of the following categories: (a) a user of Weixin or WeChat in the People’s Republic of China; (b) a citizen of the People’s Republic of China using Weixin or WeChat anywhere in the world; or (c) a Chinese-incorporated company using Weixin or WeChat anywhere in the world. If you belong to any of these categories, please refer to the Terms of Service (PRC Users) for the terms that apply to you.**\*\* For the purposes of these Terms, a reference to “People’s Republic of China” does not include a reference to Taiwan, Hong Kong or Macau. If you are a user of Weixin or WeChat and are located in Taiwan, Hong Kong or Macau, and are not in categories (b) or (c) above, these Terms apply to you.

Please review these Terms and our policies and instructions to understand how you can and cannot use WeChat. You must comply with these Terms in your use of WeChat and only use WeChat as permitted by applicable laws and regulations, wherever you may be when you use them. In some countries, there are restrictions on your use of WeChat – it is your responsibility to ensure that you are legally allowed to use WeChat where you are located, and certain WeChat functionalities may not be available in some countries.

**By using WeChat, you agree to these Terms. If you do not agree to these Terms, you must not use WeChat.**

### *Other general terms in relation to these Terms*

If you are under the age of 13, you must not use WeChat. If you are between the ages of 13 and 18 (or the relevant age in your jurisdiction where you are considered a minor), your parent or guardian must agree to these Terms (both for themselves and on your behalf)

before you can use WeChat.

If you are using WeChat on behalf of a company, partnership, association, government or other organisation (your “**Organisation**”), you warrant that you are authorised to do so and that you are authorised to bind your Organisation to these Terms. In such circumstances, “you” will include your Organisation.

We may translate these Terms into multiple languages. If there is any difference between the English version and any other language version of these Terms, the English version will apply (to the extent permitted by applicable laws and regulations).

### *"WeChat"*

For the purposes of these Terms, any reference in these Terms to "WeChat" refers to WeChat and all WeChat-related services provided by or on behalf of us or our affiliate companies from time to time, including the following services:

- WeChat;
- WeChat Mini Programs Platform;
- WeChat Developers Platform;
- Official Account Admin Platform;
- WeChat Out; and
- WeChat Pay.

### *Contracting Entity*

By using WeChat, you are agreeing to be bound by these Terms between you and:

(i) if you are a user located within the European Economic Area or Switzerland (“**European Union**” or “**EU**”), **Tencent International Services Europe BV**, a Dutch company located at 26.04 on the 26th floor of Amstelplein 54, 1096 BC Amsterdam, the Netherlands; or

(ii) if you are a user located outside the EU, **Tencent International Service Pte. Ltd.**, a Singaporean company located at 10 Anson Road, #21-07 International Plaza, Singapore 079903,

(in each case, “**we**”, “**our**” and “**us**”).

We may specify in certain of our WeChat service-specific terms that you are contracting with one of our affiliate companies (instead of Tencent International Services Europe BV or Tencent International Service Pte. Ltd., as applicable) in relation to your use of the relevant WeChat service or feature to which the relevant service-specific terms apply. Where this is the case, the relevant contracting entity will be identified in the relevant WeChat service-specific terms, and these Terms (including those relevant service-specific terms) will apply between you and that identified contracting entity in relation to your use of the relevant WeChat service or feature.

## ADDITIONAL TERMS AND POLICIES

---

We offer a diverse range of services and features within WeChat, so there are additional terms and policies that may be applicable to your use of all or part of WeChat (the "**Additional Terms**"). We will notify you of the Additional Terms from time to time, including as set out in this section and otherwise from time to time within WeChat. These Additional Terms all form part of and are incorporated into these Terms.

### *WeChat policies*

The following policies are Additional Terms that you must comply with in using WeChat:

- *WeChat Privacy Policy* – which sets out how we collect, store and use your personal information, as well as our policy on the use of tracking technologies.
- *WeChat Acceptable Use Policy* – which sets out rules of good behaviour applicable to your use of WeChat.
- *Copyright Policy* – which sets out how we deal with intellectual property rights-related complaints in accordance with the DMCA.

### *Terms applicable to specific WeChat features*

Some of our services and features have Additional Terms specific to their use. You must comply with such Additional Terms (as well as these Terms) in your use of such services and features. Such service-specific Additional Terms include:

- *Sticker Licence Agreement* – governing your use of Stickers (as defined in such agreement) within WeChat.
- *WeChat Developers Platform Use Agreement* – governing your use of the WeChat Developers Platform.



- *WeChat e-Commerce Agreement and/or WeChat Official Account Admin Platform Merchant Function Agreement* – governing your use of WeChat's e-commerce services.
- *WeChat Official Account Admin Platform User Agreement* – governing your use of the WeChat Official Account Admin Platform.
- *WeChat Out Terms of Service* – governing your use of WeChat Out.
- *WeChat Pay System User Service Agreement* – governing your use of WeChat Pay.

#### *Additional country-specific terms*

If you are a citizen or a habitual resident of the following countries, the following country-specific Additional Terms will also apply to your use of WeChat:

- USA.
- Australia.
- European Union.

#### *Inconsistencies*

Subject to the next paragraph and except as otherwise expressly specified within these Terms or any Additional Terms – to the extent that any Additional Terms conflict with these Terms, the relevant Additional Terms will apply to the extent of the conflict.

## **CHANGES**

---

We may make changes to these Terms (and any applicable Additional Terms) over time (for example, to reflect technical improvements and changes to WeChat (for example, to address a security threat) or applicable laws and regulations (for example, to reflect applicable consumer rights)), so please come back and review these Terms regularly.

Where we consider that such changes are reasonably material, we will (where reasonably practicable) notify you (via <http://www.wechat.com>, direct communication to you, on this page or the relevant page for the relevant additional terms or policy, or other means), prior to such changes becoming effective. **By continuing to use WeChat after we make any changes to these Terms, you are agreeing to be bound by the revised Terms.**

## **CHANGES TO WECHAT**

---

As WeChat and user experiences are constantly evolving, we may from time to time:

- add, change or remove features or services from WeChat (including in relation to whether a feature or service is free of charge or not); and/or
- suspend, discontinue or terminate WeChat altogether.

You agree that we may take any such actions at any time. Where we consider that any changes to WeChat or any services or features accessible within WeChat are reasonably material, we will (where reasonably practicable) notify you (via <http://www.wechat.com>, direct communication to you, on this page or the relevant page for the relevant additional terms or policy, or other means), prior to such changes becoming effective.

## **YOUR ACCOUNT**

---

You need to create an account with us in order to access and use WeChat. Any account that you open with us is personal to you and you are prohibited from gifting, lending, transferring or otherwise permitting any other person to access or use your account. Your account name, user ID and other identifiers you adopt within WeChat remains our property and we can disable, reclaim and reuse these once your account is terminated or deactivated for whatever reason by either you or us.

You are responsible for: (a) safeguarding your account details, including any passwords used to access your account and WeChat, and (b) all use of WeChat under your account, including any purchases made and/or payment obligations arising under your account. You must promptly notify us by going to "Me" -> "Settings" -> "Help & Feedback" from within the WeChat app or by visiting <http://help.wechat.com> if you know or suspect that your password or account has been compromised. We will regard all use of your account on WeChat as being by you, except where we have received a valid and –properly received notification to us regarding your account or password being compromised.

We may allow you to register for and login to WeChat using sign-on functionalities provided by third party platforms, such as Facebook or Google. You agree to comply with the relevant third party platform's terms and conditions applicable to your use of such functionalities (in addition to these Terms).

## **PAYMENTS**

---

You may, from time to time, make payments to us or third parties as part of your use of WeChat (including for the provision of WeChat or provision of certain additional features within WeChat). We may set out further terms applying to such payments (including in relation to refunds (if any), billing arrangements and any consequences of failing to make timely payments). You must comply with all such terms in relation to your payments to us. You agree that you are solely responsible for all fees and taxes associated with any such payments. and that pricing and availability of Items and products are subject to change at any time.

We may from time to time make available payment methods to you for automatic, recurring or subscription-based charges. Where we do so, you agree that (subject to applicable laws and regulations):

- such purchases or payments are generally made by you on an advance basis. Unless the purchase was on a subscription basis, we will notify you prior to any automatic renewals;
- you authorise us to: (a) save your chosen payment method's information (e.g. credit card information) on our systems; and (b) bill your chosen payment method for the relevant time-periods as chosen by or notified to you;
- if any payment made via your chosen payment method is rejected, denied or returned unpaid for any reason: (a) we may not provide you with, or suspend our provision of, the relevant WeChat product or service until payment is properly processed; and (b) you are liable to us for any fees, costs, expenses or other amounts we incur arising from such rejection, denial or return (and we may automatically charge you for such amounts); and
- we will provide you with further instructions within WeChat regarding how you may update or cancel the relevant payment method.

We may change any fees that we charge for WeChat (or any parts of WeChat) at any time upon publication within WeChat. If you do not accept such change to the fees, we may be unable to provide WeChat (or the relevant part of WeChat) to you.

**SUBJECT TO MANDATORY APPLICABLE LAWS AND REGULATIONS OR AS OTHERWISE SPECIFIED BY US IN THESE TERMS OR FOR A PARTICULAR ITEM OR SERVICE WITHIN WECHAT, IN NO CIRCUMSTANCES WILL WE BE REQUIRED TO PROVIDE A REFUND FOR ANY PAYMENTS MADE BY YOU TO US IN RELATION TO ANY ITEMS OR SERVICE WITHIN WECHAT (WHETHER USED OR UNUSED).**

If you believe that we have charged you in error, and subject to applicable laws and regulations: (a) you must contact us within 30 days of the date of the relevant charge; and (b) no refunds will be given for any erroneous charges after such 30 days period. We may process payments from you in WeChat via a third party service, and we may provide your relevant Information to such third parties to process your payments. You agree to comply with that relevant third party's terms and conditions in relation to the payment processing service, as further set out in the "Third Party Content and Services" section below.

## **YOUR CONTENT**

---

When you submit, upload, transmit or display any data, information, media or other content in connection with your use of WeChat (“Your Content”), you understand and agree that:

- you will continue to own and be responsible for Your Content;
- we will not sell Your Content to any third party;
- you are giving us and our affiliate companies a perpetual, non-exclusive, transferable, sub-licensable, royalty-free, worldwide licence to use Your Content (with no fees or charges payable by us to you) for the purposes of providing, promoting, developing and trying to improve WeChat and our other services, including new services that we may provide in the future. All such use will, to the extent Your Content contains Personal Information, be in accordance with our WeChat Privacy Policy. As part of this licence, we and our affiliate companies may, subject to the our WeChat Privacy Policy, copy, reproduce, host, store, process, adapt, modify, translate, perform, distribute and publish Your Content worldwide in all media and by all distribution methods, including those that are developed in the future;
- you grant other WeChat users a non-exclusive licence to access and use Your Content within WeChat, in accordance with these Terms and WeChat's functionalities;
- we may share Your Content with third parties that we work with to help provide, promote, develop and improve WeChat in accordance with the WeChat Privacy Policy;
- we may use the name that you submit in connection with Your Content (whether that be your account name, real name or otherwise); and
- you will comply with these Terms, including our WeChat Acceptable Use Policy, in your submission of Your Content.

In addition, you agree that we and our affiliate companies (subject to these Terms, our WeChat Privacy Policy and applicable laws and regulations):

- are allowed to retain and continue to use Your Content after you stop using WeChat;
- may be required to retain or disclose Your Content: (a) in order to comply with applicable laws or regulations; (b) in order to comply with a court order, subpoena or other legal process; (c) in order to respond to a lawful request by a government authority, law enforcement agency or similar body (whether situated in your jurisdiction or elsewhere); or (d) where we believe it is reasonably necessary to comply with applicable laws or regulations, in each case whether such applicable law or regulation, legal process or government body is of your jurisdiction or elsewhere;

- may be required to retain or disclose Your Content in order to enforce these Terms or to protect any rights, property or safety of ours, our affiliate companies or other users of WeChat.

You understand that even if you seek to delete Your Content from WeChat, it may as a technical and administrative matter take some time or not be possible to achieve this – for example, we may not be able to prevent any third party from storing or using any of Your Content that you have made public via WeChat. Further information on your rights in relation to Your Content are set out in our [WeChat Privacy Policy](#).

We reserve the right to block or remove Your Content for any reason, including as is in our opinion appropriate, as required by applicable laws and regulations or in accordance with the Copyright Policy. We reserve the right to artificially manipulate the visibility, status, or rank of Your Content on WeChat.

### *Responsibility for Your Content*

You are solely responsible for Your Content. We are not responsible for maintaining a backup of Your Content - we recommend that you keep a back-up copy of it at all times.

You must at all times ensure that: (a) you have the rights required to copy, process, transmit, access, publish, display and use Your Content, and to grant us and other third parties the rights as set out in these Terms; and (b) Your Content (and our use of Your Content in accordance with these Terms) does not infringe or violate any applicable laws or regulations or the rights of any person.

## **INFRINGEMENT OF RIGHTS**

---

We comply with the provisions of the Digital Millennium Copyright Act applicable to Internet service providers (17 U.S.C. §512, as amended) (the "**DMCA**"). If you have an intellectual property rights-related complaint about any content posted in WeChat, please follow the instructions set out in our [Copyright Policy](#).

## **THIRD PARTY CONTENT AND SERVICES**

---

We are not responsible for and we do not endorse, support or guarantee the lawfulness, accuracy or reliability of any content submitted to, transmitted or displayed by or linked by WeChat, including content provided by users of WeChat or by our advertisers. You acknowledge and agree that by using WeChat, you may be exposed to content which is inaccurate, misleading, defamatory, offensive or unlawful. Any reliance on or use of any content on or accessible from WeChat by you is at your own risk. Your use of WeChat does not give you any rights in or to any content you may access or obtain in connection with your use of WeChat.



We also do not guarantee the quality, reliability or suitability of any third party services, programs (including any Mini Programs as made available on the WeChat Mini Programs Platform) or websites provided, made available, advertised or linked through WeChat (including any of WeChat's associated platforms or services) and we will bear no responsibility for your use of or relationship with any such third parties services, programs or websites, including any payment obligations or fees that you may incur in your use of such third party services or websites.

We may review (but make no commitment to review) content (including any content posted by WeChat users) or third party programs or services made available through WeChat to determine whether or not they comply with our policies, applicable laws and regulations or are otherwise objectionable. We may remove or refuse to make available or link to certain content or third party programs or services if they infringe intellectual property rights, are obscene, defamatory or abusive, violate any rights or pose any risk to the security or performance of WeChat.

There may be, from time to time, third party content, programs and/or services on WeChat that are subject to further terms from that third party – for examples, terms from the relevant third party that originally produced or created such content or service, terms in relation to promotional activities being held on WeChat, terms relating to your use of third party-provided WeChat login functionality or terms governing your use of any Mini Programs provided by a third party. You are solely responsible for reviewing and complying with any such third party terms and conditions.

We have the right to remove, at our sole discretion and without notice to you, any content, programs and/or services that are made available within WeChat (including any of WeChat's associated platforms or services), in accordance with these Terms.

## **ADVERTISING CONTENT ON WECHAT**

---

WeChat may include advertising or commercial content. You agree that: (a) we may integrate, display and otherwise communicate advertising or commercial content in WeChat and that (where reasonably practicable) we will identify such advertising or commercial content; and (b) as explained in more detail in our [WeChat Privacy Policy](#), we may use targeted advertising to try to make advertising more relevant and valuable to you.

## **OUR INTELLECTUAL PROPERTY RIGHTS**

---

All intellectual property rights in or to WeChat and any WeChat Software (including any future updates, upgrades and new versions to all such WeChat Software), will continue to belong to us and our licensors. Except as expressly provided in these Terms, you have no right to use our intellectual property rights, including our trade marks or product names (for example, “**Tencent**”, “**WeChat**” or “**QQ**”), logos, domain names or other distinctive

brand features, without our prior written consent. Any comments or suggestions you may provide regarding WeChat are entirely voluntary and we will be free to use these comments and suggestions at our discretion (including using such comments to improve existing services or create new services) without any payment or other obligation to you.

We grant you a limited, personal, on-exclusive, non-sublicensable, non-transferrable, royalty-free and revocable right to use WeChat and any software from us as part of or in relation to your use of WeChat (any such software being the "**WeChat Software**"), solely in accordance with these Terms and subject to any other instructions as provided by us to you in relation to your use of WeChat and/or the WeChat Software from time to time. Please note that these terms may be supplemented by terms and conditions applicable to WeChat Software (or specific features within WeChat Software).

You may not copy, modify, create derivative works, reverse compile, reverse engineer or extract source codes from WeChat Software, and you may not sell, distribute, redistribute or sublicense WeChat or the WeChat Software, except in each case to the extent that we may not prohibit you from doing so under applicable laws or regulations or you have our prior written consent to do so. Where applicable laws or regulations entitle you to reverse compile or extract source codes from WeChat Software, you will first contact us to request the information you need.

We may from time to time provide updates to WeChat Software. Such updates may occur automatically or manually. Please note that WeChat Software may not operate properly or at all if upgrades or new versions are not installed by you. We do not guarantee that we will provide any updates for any WeChat Software, or that such updates will continue to support your device or system. All updates to the WeChat Software are part of the WeChat Software and subject to these Terms, except as otherwise specified by us.

For the purposes of these Terms, "WeChat Software" includes any items, content or features (the "**Items**") within the WeChat Software – for example, Stickers, games or other downloadable items within WeChat, and any content accessed or used by you within WeChat. You must comply with any Additional Terms applicable to any such Items. We will notify you of any such additional terms and conditions within WeChat, within an Appendix to these Terms and/or in another manner. We may grant you a limited right to use these Items upon payment by you of "real world money" as applicable from time to time. You acknowledge that you do not own these Items and the amounts associated with such Items do not refer to any credit balance of real currency or the equivalent. We may eliminate these Items from WeChat at any time, and we have no liability to you in the event that we exercise these rights.

For the purpose of these Terms, "WeChat Software" also includes any APIs we make available to you for use in connection with WeChat or the WeChat Software. You must comply with any Additional Terms applicable to such APIs.

We may in our discretion provide technical support for WeChat (whether for free or for a fee). We provide technical support without any guarantee or warranty of any kind, and subject always to these Terms.

## OPEN SOURCE SOFTWARE

---

Certain WeChat Software may contain software that are subject to “open source” licences (the “**Open Source Software**”). Where we use such Open Source Software, please note that:

- there may be provisions in the Open Source Software's licence that expressly override these Terms, in which case such provisions shall prevail to the extent of any conflict with these Terms; and
- we will credit the relevant Open Source Software used in WeChat Software within an Appendix to these terms and/or within the relevant WeChat Software.

## USE OF YOUR DEVICE BY WECHAT

---

In order for us to provide WeChat to you, we may require virtual access to and/or use of your relevant device (e.g. mobile phone, tablet or desktop computer) that you use to access WeChat – for example, we may need to use your device's processor and storage to complete the relevant WeChat Software installation, or we may need to access your contact list to provide certain interactive functions within WeChat.

We will provide further information regarding how WeChat uses and accesses your device within WeChat or in another manner (e.g. via the relevant app store as part of the installation process for WeChat on your device). You agree to give us such access to and use of your device, and you acknowledge that if you do not provide us with such right of use or access, we may not be able to provide WeChat (or certain features within WeChat) to you.

Any Personal Information (as defined in the WeChat Privacy Policy) that we use or access within your device will be treated in accordance with these Terms, including our WeChat Privacy Policy.

You may need an adequate internet connection in order to authenticate your WeChat account or use WeChat. You may also be required to activate certain functionalities within WeChat in the manner described within WeChat. You may not be able to use certain functionalities within WeChat if you do not comply with such requirements.

Please note that we are not responsible for any third party charges you incur (including any charges from your internet and telecommunication services providers) in relation to or arising from your use of WeChat or WeChat Software.

## THIRD PARTY SOFTWARE AND CONNECTIVITY

---

You are solely responsible for any software (whether your own software or software supplied by third parties) used by you in connection with your use of WeChat, including any third party software or services made available to you through WeChat, such as Mini Programs made available on the WeChat Mini Programs Platform ("**Third Party Software**").

Please note that we are not responsible for and are not liable for any damages or losses arising from your use of the Third Party Software and we do not endorse, support or guarantee the quality, reliability or suitability of any Third Party Software. You must comply with any terms and conditions applicable to Third Party Software.

We do not provide any technical support for any Third Party Software. Please contact the relevant supplying third party for such technical support.

You will need an adequate internet connection in order to authenticate your WeChat account or use WeChat. You may also be required to activate certain functionalities within WeChat in the manner described within WeChat. You may not be able to use certain features within WeChat if you do not comply with such requirements.

Please note that we are not responsible for any third party charges you incur (including any charges from your internet and telecommunication services providers) in relation to or arising from your use of WeChat or WeChat Software.

## WARRANTY AND DISCLAIMER

---

We warrant to you that we will provide WeChat using reasonable care and skill.

APART FROM THIS WARRANTY, TO THE EXTENT PERMITTED BY APPLICABLE LAWS AND REGULATIONS, WECHAT (INCLUDING ANY WECHAT SOFTWARE) IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS AND NEITHER US NOR ANY OF OUR AFFILIATE COMPANIES MAKE ANY REPRESENTATION OR WARRANTY OR GIVE ANY UNDERTAKING IN RELATION TO WECHAT, ANY WECHAT SOFTWARE OR ANY DATA, MEDIA OR OTHER CONTENT SUBMITTED, TRANSMITTED OR DISPLAYED BY WECHAT, INCLUDING: (A) ANY REPRESENTATION, WARRANTY OR UNDERTAKING THAT WECHAT OR WECHAT SOFTWARE WILL BE UNINTERRUPTED, SECURE OR ERROR-FREE OR FREE FROM VIRUSES; (B) THAT WECHAT OR WECHAT SOFTWARE WILL BE COMPATIBLE WITH YOUR DEVICE; OR (C) THAT WECHAT OR WECHAT SOFTWARE WILL BE OF MERCHANTABLE QUALITY, FIT FOR A PARTICULAR PURPOSE OR NOT INFRINGE THE INTELLECTUAL PROPERTY RIGHTS OF ANY PERSON. TO THE EXTENT PERMITTED BY APPLICABLE LAWS AND REGULATIONS, YOU WAIVE ANY AND ALL IMPLIED REPRESENTATIONS, WARRANTIES AND UNDERTAKINGS.

## LIABILITY FOR WECHAT

---

TO THE EXTENT PERMITTED BY APPLICABLE LAWS AND REGULATIONS, THE TOTAL AGGREGATE LIABILITY OF US AND OUR AFFILIATE COMPANIES FOR ALL CLAIMS IN CONNECTION WITH THESE TERMS, OR WECHAT (INCLUDING ANY WECHAT SOFTWARE), ARISING OUT OF ANY CIRCUMSTANCES, WILL BE LIMITED TO THE GREATER OF THE FOLLOWING AMOUNTS: (A) THE AMOUNT THAT YOU HAVE PAID TO US FOR YOUR USE OF WECHAT OR WECHAT SOFTWARE TO WHICH THE CLAIM RELATES IN THE 6 MONTHS IMMEDIATELY PRECEDING THE DATE OF THE MOST RECENT CLAIM; AND (B) USD100 (ONE HUNDRED US DOLLARS). TO THE EXTENT PERMITTED BY APPLICABLE LAWS AND REGULATIONS, IN NO EVENT WILL WE OR ANY OF OUR AFFILIATE COMPANIES BE LIABLE FOR ANY OF THE FOLLOWING:

- IN CONNECTION WITH THESE TERMS OR WECHAT OR WECHAT SOFTWARE, FOR ANY DAMAGES OR LOSSES CAUSED BY: (A) ANY NATURAL DISASTER SUCH AS FLOODS, EARTHQUAKES OR EPIDEMICS; (B) ANY SOCIAL EVENT SUCH AS WARS, RIOTS OR GOVERNMENT ACTIONS; (C) ANY COMPUTER VIRUS, TROJAN HORSE OR OTHER DAMAGE CAUSED BY MALWARE OR HACKERS; (D) ANY MALFUNCTION OR FAILURE OF OUR OR YOUR SOFTWARE, SYSTEM, HARDWARE OR CONNECTIVITY; (E) IMPROPER OR UNAUTHORISED USE OF WECHAT OR WECHAT SOFTWARE; (F) YOUR USE OF WECHAT OR WECHAT SOFTWARE IN BREACH OF THESE TERMS; (G) ANY REASONS BEYOND OUR REASONABLE CONTROL OR PREDICTABILITY; OR (H) FAILURE TO SAVE OR BACK UP ANY DATA OR OTHER CONTENT;
- ANY LOSS ARISING FROM ANY CONTENT, PROGRAMS OR SERVICES PROVIDED BY ANY PARTY OTHER THAN US (OR OUR AFFILIATES);
- ANY LOSS OR DAMAGE WHICH ARE NOT FORESEEABLE, INDIRECT, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR LOSSES. FOR THE PURPOSES OF THIS CLAUSE, LOSS OR DAMAGE IS FORESEEABLE IF EITHER IT IS OBVIOUS THAT IT WILL HAPPEN OR IF, AT THE TIME THE CONTRACT WAS MADE, BOTH WE AND YOU KNEW IT MIGHT HAPPEN; AND/OR



- ANY:
  - LOSS OF USE;
  - LOSS OR INTERRUPTION OF BUSINESS;
  - LOSS OF REVENUES;
  - LOSS OF PROFITS;
  - LOSS OF GOODWILL;
  - LOSS OR DESTRUCTION OF CONTENT OR DATA.

Nothing in these Terms limits or excludes any of the following liabilities, except to the extent that such liabilities may be waived, limited or excluded under applicable laws and regulations:

- any liability for fraud;
- any liability for negligently caused death or personal injury;
- any liability for gross negligence or wilful misconduct; or
- any other liability to the extent that such other liability cannot be waived, limited or excluded under applicable laws and regulations.

NOTWITHSTANDING ANY OTHER PROVISIONS OF THESE TERMS, NOTHING IN THESE TERMS LIMITS OR EXCLUDES ANY OF YOUR STATUTORY RIGHTS IN YOUR JURISDICTION (INCLUDING ANY RIGHTS UNDER APPLICABLE CONSUMER PROTECTION REGULATION), TO THE EXTENT SUCH STATUTORY RIGHTS MAY NOT BE EXCLUDED OR WAIVED UNDER APPLICABLE LAWS AND REGULATIONS.

YOU AGREE THAT YOU (AND YOUR ORGANISATION, IF YOU ARE USING WECHAT OR WECHAT SOFTWARE ON BEHALF OF SUCH ORGANISATION) INDEMNIFY US AND OUR AFFILIATE COMPANIES FROM AND AGAINST ANY CLAIM, SUIT, ACTION, DEMAND, DAMAGE, DEBT, LOSS, COST, EXPENSE (INCLUDING LITIGATION COSTS AND ATTORNEYS' FEES) AND LIABILITY ARISING FROM: (A) YOUR USE OF WECHAT OR WECHAT SOFTWARE; OR (B) YOUR BREACH OF THESE TERMS.

## **NO LIABILITY FOR THIRD PARTIES**

---

As set out in the "Third Party Content and Services" and "Third Party Software" sections of these Terms, various third parties may provide certain content, services or software within WeChat.

THESE TERMS GOVERN THE RELATIONSHIP BETWEEN YOU AND US (AND, WHERE RELEVANT, OUR AFFILIATE COMPANIES). YOUR DEALINGS WITH ALL THIRD PARTIES (INCLUDING THOSE FOUND THROUGH, PROMOTED THROUGH, ACCESSED VIA HYPERLINK THROUGH OR OTHERWISE THROUGH WECHAT), ARE SOLELY BETWEEN YOU AND THE RELEVANT THIRD PARTY. SUBJECT TO MANDATORY APPLICABLE LAWS AND REGULATIONS, WE AND OUR AFFILIATE COMPANIES HAVE NO LIABILITY TO YOU IN RELATION TO ANY THIRD PARTIES (INCLUDING ANY CONTENT, SERVICES OR SOFTWARE PROVIDED BY SUCH THIRD PARTIES WITHIN WECHAT), NOTWITHSTANDING YOUR ENGAGEMENT WITH ANY SUCH THIRD PARTIES THROUGH WECHAT.

## **TERMINATION**

---

These Terms will apply to your use of WeChat until your access to WeChat is terminated by either you or us.

You may terminate your use of WeChat, or any of the services accessible therein, at any time (including if we have told you about an upcoming change to all or part of WeChat or these Terms which you do not agree to). If the terminated service is a paid service, we may deduct from any refund a reasonable proportion of such fee as compensation for the costs incurred by us in ending the relevant service.

We may suspend or terminate your access to your account or any or all of WeChat:

- if we undertake maintenance or support of WeChat;
- to make changes to WeChat as notified by us to you;
- if we reasonably believe that you have breached these Terms;
- if your use of WeChat creates risk for us or for other users of WeChat, gives rise to a threat of potential third party claims against us or is potentially damaging to our reputation;
- if you fail to use WeChat for a prolonged period;
- if such suspension or termination is required due to Applicable Laws; or
- to the extent permitted by applicable laws and regulations, for any other reason in our sole and absolute discretion,

and where reasonably practicable, we will give you advance notice of any suspension or termination.

If we suspend your access to any or all of WeChat then, to the extent permitted by applicable laws and regulations in your jurisdiction: (a) you remain responsible for all fees accrued through the date of suspension (including where the fees were incurred before suspension date but performance of the relevant obligations were after the suspension date); and (b) you remain responsible for any applicable fees for any part of WeChat to which you continue to have access.

If your access to WeChat is terminated (in whole or in part) by you or us, you agree that: (a) all of your rights under these Terms will terminate; (b) you remain responsible for all fees accrued through the date of termination (including where the fees were incurred before termination date but performance of the relevant obligations were after the termination date); and (c) you will immediately permanently delete all copies of WeChat Software to which the termination relates and you will immediately cease accessing and using any such WeChat Software.

### *Retention and back-up of Your Content*

Following termination of these Terms, we will only retain and use Your Content in accordance with these Terms and, to the extent Your Content includes Personal Information, the WeChat Privacy Policy. Subject to the WeChat Privacy Policy and applicable laws and regulations in your jurisdiction, where we suspend or terminate all or part of WeChat, or where your access to WeChat is terminated by you or us, we do not guarantee that we will be able to return any of Your Content back to you and we may permanently delete Your Content without notice to you at any time after termination. Please ensure that you regularly back up Your Content.

## **GENERAL**

---

Subject to the applicable laws and regulations in your jurisdiction, these Terms sets out the entire agreement between you and us in relation to WeChat – you agree that you will have no claim against us for any statement which is not explicitly set out in these Terms. The words "include" and "including" are to be construed without limitation. The invalidity of any provision of these Terms (or parts of any provision) will not affect the validity or enforceability of any other provision (or the remaining parts of that provision). If a court holds that we cannot enforce any part of these Terms as drafted, we may replace those terms with similar terms to the extent enforceable under applicable laws and regulations, without changing the remaining terms of these Terms. No delay in enforcing any provision of these Terms will be construed to be a waiver of any rights under that provision. Any rights and obligations under these Terms which by their nature should survive, including any obligations in relation to the liability of, or indemnities (if any) given by, the respective parties, will remain in effect after termination or expiration of these Terms.

No person other than you and us will have any right to enforce these Terms, whether pursuant to the Contracts (Rights of Third Parties) Ordinance or otherwise, and you may not delegate, assign or transfer these Terms or any rights or obligations under these Terms without our prior consent. We may freely assign or transfer these Terms or our rights and obligations under these Terms, in whole or in part, without your prior consent or prior notice to you. We may freely sub-contract any part of our performance of these Terms at any time, without your prior consent or prior notice to you.

## **GOVERNING LAW AND DISPUTE RESOLUTION**

---

Except to the extent that: (a) any applicable additional terms incorporated into these Terms provide differently, or (b) the applicable laws and regulations of your jurisdiction mandate otherwise (for example, you may have statutory rights in your jurisdiction in relation to bringing or defending claims in a local court (including small claims court)):

- these Terms and any dispute or claim arising out of or in connection with these Terms will be governed by the law of the Hong Kong Special Administrative Region; and
- any dispute, controversy or claim (whether in contract, tort or otherwise) arising out of, relating to, or in connection with these Terms, including their existence, validity, interpretation, performance, breach or termination, will be referred to and finally resolved by arbitration administered by the Hong Kong International Arbitration Centre under the Hong Kong International Arbitration Centre Administered Arbitration Rules in force when the Notice of Arbitration is submitted. The seat of the arbitration will be Hong Kong. There will be one arbitrator only. The arbitration proceedings will be conducted in English.

## **WECHAT TERMS OF SERVICE (USA-SPECIFIC TERMS)**

---

*If you are a user of WeChat in the United States of America, the below Additional Terms: (a) are incorporated into these Terms; (b) apply to your use of WeChat; and (c) override the head terms of these Terms to the extent of any inconsistency.*

If you are a user of WeChat in the United States of America, the following terms expressly replaces the above "Governing law and dispute resolution" section of these Terms.

If you live in (or, if a business, your principal place of business is in) the United States, the laws of the state where you live govern all claims, regardless of conflict of law principles, except that the Federal Arbitration Act governs all provisions relating to arbitration. You and we irrevocably consent to the exclusive jurisdiction and venue of the state or federal courts of California, for all disputes arising out of or relating to these Terms that are heard in court (excluding arbitration).

EACH OF THE PARTIES HERETO IRREVOCABLY WAIVES ANY AND ALL RIGHT TO TRIAL BY JURY OR TO PARTICIPATE IN A CLASS ACTION IN ANY LEGAL PROCEEDING ARISING OUT OF OR RELATING TO THESE TERMS OR THE TRANSACTIONS CONTEMPLATED HEREBY.

In the event of a dispute, you and we agree to try for sixty (60) days to resolve it informally. If you and we are unable to come to informal resolution within sixty (60) days, you and we agree to binding individual arbitration before the American Arbitration Association ("**AAA**") under the Federal Arbitration Act ("**FAA**") (with such arbitration to be conducted under the AAA's Commercial Arbitration Rules), and not to sue in court in front of a judge or jury. Instead, a neutral arbitrator will decide and the arbitrator's decision will be final except for a limited right of appeal under the FAA. Class action lawsuits, class-wide arbitrations, private attorney-general actions, and any other proceeding where someone acts in a representative capacity are not allowed, and nor is combining individual proceedings without the consent of all parties. These Terms govern to the extent they conflict with the AAA's Commercial Arbitration Rules or Consumer Arbitration Rules. You and we must file in arbitration any claim or dispute (except intellectual property disputes) within one year from when it first could be filed. If the class action waiver is found to be illegal or unenforceable as to all or some parts of a dispute, then those parts won't be arbitrated but will proceed in court, with the rest proceeding in arbitration. If any other provision of these provisions regarding arbitration is found to be illegal or unenforceable, that provision will be severed but the rest of these provisions regarding arbitration still apply.

If you are a California resident, then (except to the extent prohibited by applicable laws) you agree to waive California Civil Code Section 1542, and any similar provision in any other jurisdiction (if you are a resident of such other jurisdiction), which states: "A general release does not extend to claims which the creditor does not know or suspect to exist in his favour at the time of executing the release, which, if known by him must have materially affected his settlement with the debtor".

## **WECHAT TERMS OF SERVICE (AUSTRALIA-SPECIFIC TERMS)**

---

*If you are a user of WeChat in Australia, the below Additional Terms: (a) are incorporated into these Terms; (b) apply to your use of WeChat; and (c) override the head terms of these Terms to the extent of any inconsistency.*

All express or implied guarantees, warranties, representations, or other terms and conditions relating to these Terms or their subject matter, not contained in these Terms, are excluded from these Terms to the maximum extent permitted by applicable laws and regulations.



Nothing in these Terms excludes, restricts or modifies any guarantee, warranty, term or condition, right or remedy implied or imposed by any applicable laws and regulations which cannot lawfully be excluded, restricted or modified.

If any guarantee, condition, warranty or term is implied or imposed by any applicable laws and regulations and cannot be excluded (a “**Non-Excludable Provision**”), and we are able to limit your remedy for a breach of the Non-Excludable Provision, then our liability for breach of the Non-Excludable Provision is limited to one or more of the following at our option:

- in the case of goods, the replacement of the goods or the supply of equivalent goods, the repair of the goods, the payment of the cost of replacing the goods or of acquiring equivalent goods, or the payment of the cost of having the goods repaired; or
- in the case of services, the supplying of the services again, or the payment of the cost of having the services supplied again.

## **WECHAT TERMS OF SERVICE (EUROPEAN UNION-SPECIFIC TERMS)**

---

*If you are a user of WeChat and located in the European Union, the below Additional Terms: (a) are incorporated into these Terms; (b) apply to your use of WeChat; and (c) override the head terms of these Terms to the extent of any inconsistency.*

### *Refund of your purchases*

If you have purchased and paid for a WeChat product or service provided by us (and not by any third parties), you may receive a refund for such purchase if we receive a refund request from you within 14 days from the date you completed the relevant purchase. If you have already used a portion of the relevant product or service, you will receive a refund for the unused portion only. In the case of a download or streaming product, you acknowledge that by proceeding to download or stream such product, you will not be entitled to a refund of such purchase.

We set out further information within the relevant WeChat services and applicable Additional Terms in relation to how you can submit your refund request.

### *Dispute Resolution*

Notwithstanding the "Governing Law and Dispute Resolution" section of these Terms, if you are a "consumer" as defined under the EU Directive 83/2011/EU, any dispute, controversy or claim (whether in contract, tort or otherwise) between us and you, arising out of, relating to, or in connection with these Terms will be referred to and finally resolved

by the court of your place or residence or domicile. You can also file a complaint at the online platform for alternative dispute resolution (ODR-platform). You can find the ODR-platform through the following link: <https://ec.europa.eu/consumers/odr>.

### *Loss or damage*

If any WeChat services or features which we have supplied damages a device or digital content belonging to you and this is caused by our failure to use reasonable care and skill we will either repair the damage or pay you reasonable compensation for such damage. However, we will not be liable for damage which you could have avoided by following our advice to apply an update offered to you free of charge or for damage which was caused by you failing to correctly follow installation instructions or to have in place the minimum system requirements advised by us. We only supply WeChat and the services or features accessible via WeChat for domestic and private use. If you use WeChat or the services or features for any commercial or business purpose we will have no liability to you for any loss of profit, loss of business, business interruption, or loss of business opportunity.

Last modified: 2018-03-21