SECTION 2: CHINA'S CYBER ACTIVITIES

Introduction

Since the Commission's *2012 Annual Report to Congress*, strong evidence has emerged that the Chinese government is directing and executing a large-scale cyber espionage campaign against the United States. This section—based on discussions with cybersecurity experts and U.S. Department of Defense (DoD) officials and independent research *—provides an overview of this evidence, examines developments in Chinese cyber policy, and explores potential U.S. actions and policies to deter and mitigate future Chinese cyber theft and improve U.S. cyber policy development and implementation.†

Mounting Evidence of the Chinese Government's Active Role in Cyber Espionage

Detailed Technical Information Released on Chinese Cyber Activities

In February 2013, Mandiant, a private U.S. cybersecurity firm, published a report providing detailed technical information regarding the activities of a cyber threat group, which Mandiant refers to as Advanced Persistent Threat 1. According to the report, the group likely is the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's Third Department, also known as Unit 61398. Mandiant assesses Unit 61398 since 2006 has penetrated the networks of at least 141 organizations, including companies, international organizations, and foreign governments. These organizations are either located or have headquarters in 15 countries and represent 20 sectors, from information technology to financial services. Four of these sectors are among the seven strategic emerging industries the Chinese government prioritized for development in its 12th Five-Year Plan (2011 to 2015). 81 percent of the targeted organizations were either located in the United States or had U.S.-based headquarters. Through these intrusions, the group gained access to "broad categories of intellectual prop-

*In 2013 the Commission held a roundtable on U.S.-China cybersecurity issues on July 11 and sponsored a report on the economic and security implications of cloud computing development in China, which the Commission published on September 5. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013). *http://origin.www.uscc.gov/sites/default/files/Research/Red%20Cloud%20Rising_Cloud%20Computing%20in%20China.pdf*.

†For discussion of China's cyber strategy and actors, see U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2012), pp. 147–151; Bryan Krekel et al., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Falls Church, VA: Northrop Grumman Corporation for the U.S.-China Economic and Security Review Commission, March 2012). *http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf*.

erty, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and e-mails and contact lists from victim organizations' leadership." [1]

In its report, Mandiant states Unit 61398 is responsible for conducting computer network operations,* specifically the gathering of strategic and economic intelligence on targets in the United States and Canada, as well as targeting organizations whose primary language is English in other countries.[2] Aside from Unit 61398, the Third Department has another 11 operational bureaus, three research institutes, four operations centers, and 16 technical reconnaissance bureaus.† [3] Not all of these organizations are directing their actions against the United States, and there are no public reports available about their role in China's cyber espionage campaign.[4]

According to the *Wall Street Journal*, on the same day Mandiant published its report, the U.S. Department of Homeland Security and the U.S. Federal Bureau of Investigation shared hundreds of Internet Protocol (IP) addresses used by Unit 61398 with U.S. Internet service providers to help them defend their customers against cyber intrusions. Mandiant gave the U.S. government advance notice of the release of its report on Unit 61398; this may have been a factor in the timing of the government's sharing of the IP addresses.[5]

In April 2013, the Verizon RISK Team, a cybersecurity unit within private U.S. telecommunications company Verizon, published its annual *Data Breach Investigations Report*.[6] The report presents analysis of 621 cases of "confirmed data disclosure," which Verizon defines as "any event resulting in confirmed compromise (unauthorized viewing or accessing) of any non-public information," that occurred in 2012. Eighteen governmental and private organizations from the United States, Europe, Malaysia, and Australia provided the information about these cases. Verizon categorized 19 percent of the intrusions as espionage carried out by "state-affiliated actors." It identified 96 percent of the intrusions conducted by state-affiliated actors as originating in China.[7]

Chinese Cyber Espionage against U.S. Critical Infrastructure

In July 2013, a threat researcher at Trend Micro, a private Japanese cybersecurity firm, claimed he had detected a Chinese cyber intrusion, commencing in December 2012, of a honeypot.‡

---

* Computer network operations are "comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations." Bryan Krekel et al., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Falls Church, VA: Northrop Grumman Corporation for the U.S.-China Economic and Security Review Commission, March 2012), p. 115. *http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf*.

† Technical reconnaissance bureaus are administratively subordinate to the PLA General Staff Department's Third Department but are attached to the PLA's service arms and provide direct support to operational units through signals intelligence and computer network operations.

‡ A honeypot is part of a honeynet, which is a fake or diversionary computer network designed to draw in an adversary in order to identify the adversary or give the adversary false information. Honeynets can provide intelligence regarding adversaries' "tools, tactics, and motives." The

Chinese Cyber Espionage against U.S. Critical Infrastructure—*Continued*

He created the honeypot to resemble the industrial control system of a water plant in the United States. The researcher attributed the intrusion to Unit 61398, based on forensic analysis.[8] If true, this suggests Unit 61398 is collecting intelligence on critical infrastructure in addition to other targets. Such activities are consistent with PLA doctrine, which explains that one function of wartime computer network operations is to "disrupt and damage the networks of [an adversary's] infrastructure facilities, such as power systems, telecommunications systems, and educational systems."[9] Some PLA strategists also have suggested China should develop the capability to paralyze ports and airports by cyber or precision weapon attacks on critical infrastructure.[10]

U.S. Department of Defense for the First Time Attributes Cyber Espionage to China

In May 2013, DoD for the first time directly accused the Chinese government and military of cyber espionage against U.S. networks. DoD's 2013 *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* states: "In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military." The report then states, "China is using its computer network exploitation capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs."[11]

U.S. Secretary of Defense Chuck Hagel said addressing Chinese cyber espionage primarily requires dialogue between the U.S. and Chinese governments behind closed doors, but he added, "It has to be public as well."[12] Publicly attributing cyber intrusions to the Chinese government and military in the DoD report is a significant step for the U.S. government. Previous DoD documents and statements had acknowledged cyber espionage "emanated" or "originated" from China but stopped short of attributing those operations to the Chinese government and military. For example, DoD's 2012 report to Congress stated: "Computer networks and systems around the world continued to be targets of intrusions and data theft, many of which originated within China."[13] In a press briefing following the release of the 2012 report, then acting Deputy Assistant Secretary of Defense for East Asia David Helvey said, "We have concerns about a number of computer network operations and activities that appear to originate from China that affect DoD networks." When asked whether he was referring to the Chinese government, he said, "I didn't specify the attribution."[14]

Honeynet Project, "Short Video Explaining Honeypots." *http://old.honeynet.org/misc/files/HoneynetWeb.mov*.

Beijing Issues Routine Denials of the Allegations by Mandiant and DoD

When confronted with public accusations from the United States about its cyber espionage, Beijing attempted to refute the evidence, in part, by pointing to the anonymity of cyberspace and the lack of verifiable technical forensic data. The Chinese government's statements were similar to its responses to previous foreign allegations of cyber espionage.[15]

In a press conference on the day after Mandiant released its report, a spokesperson for China's Ministry of Foreign Affairs said, "Groundless speculation and accusations regarding hacker attacks, for various purposes, is both unprofessional and irresponsible and it is not helpful for solving the problem." He also emphasized cyber attacks are a serious problem for China.[16] In a press conference the next day, a spokesperson for China's Ministry of National Defense denied that the PLA supports hacking. He argued Mandiant's allegations are without merit, because, among other reasons, hackers frequently use third-party IP addresses to conduct cyber attacks.[17]

In response to the allegations regarding China's cyber espionage activities in DoD's 2013 report to Congress, a Ministry of Foreign Affairs spokesperson said China is "strongly against any form of hacking activities" and called the charges "baseless."[18]

Evidence of a Cyber Campaign against U.S. Press

There is growing evidence the Chinese government is conducting a cyber espionage campaign against U.S. media organizations. China likely seeks to use information acquired through these intrusions to (1) shape U.S. press coverage of China by intimidating U.S. journalists' sources in China, and (2) gain warning about negative media coverage of China before it is published.[19]

- In January 2013, the *New York Times* reported Chinese cyber actors had gained access to its computer network in September 2012 and had conducted activities inside the network for the next four months. The intrusions appeared to focus on the e-mail account of a reporter investigating the assets of family members of outgoing Chinese Premier Wen Jiabao. The *New York Times* hired Mandiant to investigate the intrusion, which Mandiant attributed to a China-based cyber threat group it refers to as Advanced Persistent Threat 12. The *New York Times* reported, "The attacks started from the same university computers used by the PLA to attack United States military contractors in the past."[20]
- The *New York Times* also reported Chinese cyber actors conducted an intrusion into computers at Bloomberg News in 2012 following Bloomberg's investigation of the assets of then Chinese Vice President Xi Jinping's relatives.[21]
- Following the *New York Times'* revelations, the *Wall Street Journal* and the *Washington Post* reported their networks also had been penetrated by hackers, with evidence in both cases implicating cyber actors based in China.[22] In the *Wall Street*

Journal intrusion, the hackers targeted personnel reporting on China.[23]

New Information Emerges about 2009 Intrusion into Google's Network

In May 2013, the *Washington Post* reported Chinese cyber actors in 2009 infiltrated a Google database containing information regarding Foreign Intelligence Surveillance Court orders Google had received.* The hackers seemed to be searching for names of Chinese intelligence operatives whom the U.S. government might be monitoring. Regarding this intrusion, a former U.S. government official said that were the Chinese government to become aware that its operatives were being monitored, it could "take steps to destroy information, get people out of the country," and perhaps intentionally transmit incorrect information to the U.S. government.[24] A former U.S. Department of Justice (DoJ) official said data breaches such as this one show "the overall security and effectiveness of lawful interception and undercover operations is dependent in large part on security standards in the private sector," which "clearly need strengthening."[25]

Defense Science Board Points to Widespread Hacking of U.S. Defense Designs

The Defense Science Board† warns in *Resilient Military Systems and the Advanced Cyber Threat*, an unclassified report published in October 2012, "The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War." The Defense Science Board then assesses DoD "is not prepared to defend against this threat."[26] In May 2013, the *Washington Post* published an article describing a classified version of the report, which lists more than 24 U.S. weapon system designs the board determined were accessed by cyber intruders. The *Washington Post* reported, "Senior military and industry officials with knowledge of the breaches said the vast majority were part of a widening Chinese campaign of espionage against U.S. defense contractors and government agencies." The list includes the Patriot Advanced Capability 3 air defense system, the Terminal High Altitude Area Defense system, the Aegis ballistic missile defense system, the F/A–18 fighter aircraft, the V–22 Osprey multirole combat aircraft, the Black Hawk helicopter, the Littoral Combat Ship, and the F–35 Joint Strike Fighter.[27]

---

*The intruders also reportedly accessed Google's source code. Source code is the set of instructions that compose computer software programs. In addition, they attempted to access the e-mail accounts of Chinese human rights activists. This intrusion was part of a broader campaign targeting over 30 companies that U.S. cybersecurity company McAfee called "Operation Aurora." Ellen Nakashima, "Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say," *Washington Post*, May 20, 2013. *http://articles.washingtonpost.com/2013-05-20/world/39385755_1_chinese-hackers-court-orders-fbi*; Andrew Jacobs and Miguel Helft, "Google, Citing Attack, Threatens to Exit China," *New York Times*, January 13, 2010. *http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?pagewanted=all&_r=0*; and Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," *Wired*, January 14, 2010. *http://www.wired.com/threatlevel/2010/01/operation-aurora/*.

†According to its charter, the Defense Science Board submits "independent advice and recommendations on science, technology, manufacturing, acquisition process, and other matters of special interest to the DoD" to the Secretary of Defense and other senior defense officials. Defense Science Board, "Charter." *http://www.acq.osd.mil/dsb/charter.htm*.

Update on U.S. Department of Justice Indictment of Chinese Company

In another high-profile example of a Chinese company allegedly targeting a U.S. company's intellectual property through cyber espionage, the DoJ in June 2013 filed charges against Sinovel Wind Group, a Chinese energy firm, alleging Sinovel stole intellectual property from Massachusetts-based company American Superconductor (AMSC). DoJ charged Sinovel, the deputy director of Sinovel's research and development department, a technology manager at Sinovel, and a former employee of a subsidiary of AMSC with theft of trade secrets and related charges.[28]

AMSC and Sinovel entered into a business relationship in 2005, with AMSC selling software, components, and electrical systems to Sinovel for use in its wind turbines. In the following years, Sinovel became AMSC's largest client. However, the Chinese firm in 2011 stopped paying for products that had arrived in China and cancelled existing orders after allegedly stealing source code from AMSC to reproduce AMSC's software.[29] Media reporting alleges Dejan Karabasevic, who was working as an engineer for AMSC Wintec GmbH in Austria at the time, remotely extracted the source code from a computer in Wisconsin and delivered it to Sinovel by e-mail.[30] According to the company's chief executive officer, without sales to Sinovel, AMSC's revenue declined dramatically, and 50 percent of its 900 employees lost their jobs.[31] In early 2012, the U.S. Federal Bureau of Investigation found software alleged to have been illegally copied from AMSC's software in a wind turbine the Massachusetts Water Resources Authority had purchased from Sinovel. This was a critical factor leading to Sinovel's indictment.[32] AMSC has sought compensation from Sinovel through lawsuits in China, an effort that is ongoing and has resulted in legal fees for AMSC exceeding $6 million.[33]

Chinese Cyber Policy Developments

United States and China Establish Cyber Working Group

In April 2013, U.S. Secretary of State John Kerry announced the U.S. and Chinese governments would establish a working group to discuss cybersecurity.[34] The Cyber Working Group convened for the first time in July immediately preceding the latest meeting of the U.S.-China Strategic and Economic Dialogue (S&ED). Christopher Painter, the U.S. Department of State's Coordinator for Cyber Issues, and Dai Bing, an official from China's Ministry of Foreign Affairs, were the senior representatives for their respective countries at the meeting.[35] At the conclusion of the S&ED, the two sides announced they had "decided to take practical measures to enhance dialogue on international norms and principles in order to guide action in cyber space and to strengthen CERT to CERT (Computer Emergency Response Team)* coordination and cooperation."[36] James Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies

*A CERT is an organization that is devoted to preventing and resolving cybersecurity problems and provides information regarding cyber threats and vulnerabilities to government agencies, companies, and other organizations. For an example of a CERT, see US–CERT, "About Us" (Washington, DC: U.S. Department of Homeland Security). *http://www.us-cert.gov/about-us*.

(CSIS), testified to the House Foreign Affairs Committee's Subcommittee on Asia and the Pacific that the July S&ED and Cyber Working Group meetings "are an important step that, if it succeeds, will make the situation in Asia more stable." He added, "We are looking at a long effort and the S&ED process will need to be sustained and reinforced." [37]

China Shifts on International Law and Cyberspace

In what appears to be a break with the past, China in June 2013 agreed in a United Nations (UN) report that international law, which includes the law of armed conflict,* extends to cyberspace. The report states, "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible [information and communication technology] environment." [38] In addition, China agreed that "states must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-state actors for unlawful use of [information and communication technologies]." [39] This statement is based on the contents of the UN's *Articles on Responsibility of States for Internationally Wrongful Acts*, also known as the law of state responsibility.[40] The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which includes China, the United States, Russia, and 12 other countries, agreed on the report's contents when the group convened in New York.[41]

James Mulvenon, vice president of Defense Group Inc.'s Intelligence Division, at the roundtable on U.S.-China cybersecurity issues held by the Commission on July 11, said, "The Chinese made a dramatic reversal on their view about how the laws of armed conflict did not apply to the cyber dimension, which was a showstopper for DoD about [the department] being involved in any confidence building measures [with China]." [42] While the Chinese government does not appear to have publicly asserted its stance on the applicability of the law of armed conflict and the law of state responsibility to cyberspace prior to the UN report, U.S. experts and media reports indicate that in the past Beijing has not agreed that these laws apply to activities in cyberspace.[43]

Impact of Snowden Leaks on U.S. Efforts to Stop Chinese Cyber Espionage

In June 2013, Edward Snowden, a former contractor for the U.S. National Security Agency (NSA) alleged NSA has conducted cyber operations against hundreds of Hong Kong and mainland Chinese targets.[44] Addressing Mr. Snowden's allegations, a

*The law of armed conflict, which is also known as international humanitarian law, includes principles such as distinction between military and civilian targets, proportionality, military necessity, and limitation. International Committee of the Red Cross, "The Law of Armed Conflict: Basic Knowledge," June 2002, pp. 12–14. *http://www.icrc.org/eng/assets/files/other/law1_final.pdf*.

Impact of Snowden Leaks on U.S. Efforts to Stop Chinese Cyber Espionage—*Continued*

spokesperson for China's Ministry of National Defense said, "To, on the one hand, abuse one's advantages in information technology for selfish ends, while on the other hand, making baseless accusations against other countries, shows double standards that will be of no help for peace and security in cyberspace."[45] Despite the Obama Administration's efforts to distinguish what it calls "cyber-enabled economic espionage" or "cyber-enabled theft of trade secrets" from government-to-government espionage,[46] some observers expect Mr. Snowden's allegations to set back U.S. efforts on U.S.-China cybersecurity issues by at least six months. Dr. Mulvenon said, "I don't really think we're going to make a lot of progress for a while. . . . I would say it's probably going to delay progress six to twelve months."[47] However, an official at the U.S. embassy in Beijing told the Commission Mr. Snowden's allegations had not affected private discussions with the Chinese government on cyber theft of intellectual property.

Developments Related to Chinese Information Technology Companies

An October 2012 report by the U.S. House Permanent Select Committee on Intelligence (HPSCI) characterized China's two largest telecommunication equipment companies, Huawei and ZTE, as a risk to U.S. national security because they could facilitate intelligence collection by the Chinese government. The report advised U.S. companies against using products or services provided by Huawei and ZTE.*[48] During an interview with the *Australian Financial Review* in July 2013, former director of the Central Intelligence Agency and NSA, General Michael Hayden (Retd.), confirmed and augmented the HPSCI's findings regarding Huawei. When asked to verify whether he believed "it is reasonable to assume that hard evidence exists that Huawei has engaged in espionage on behalf of the Chinese state," General Hayden said, "Yes, that's right." He then added, "At a minimum, Huawei would have shared with the Chinese state intimate and extensive knowledge of the foreign telecommunications systems it is involved with. I think that goes without saying."[49]

Huawei and ZTE continue to issue public assurances that they do not pose a security threat.[50] For example, Huawei's president Ren Zhengfei said during his first interview with a media organization in May 2013 that his company would not assist the Chinese government with collecting foreign intelligence if asked.[51]

Despite widespread concerns about the national security risks posed by Huawei and ZTE, Bloomberg reported in August 2013 that the U.S. General Services Administration (GSA) authorized U.S. government agencies to procure a videoconferencing system produced by ZTE and Prescient, a division within U.S. company CyberPoint International LLC, in November 2012. According to an

*For more details on the HPSCI report, see U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2012), p. 164.

executive at CyberPoint, Prescient produced hardware and software to enhance the security of the system, which was originally made by ZTE. He said, due to these alterations, it now was a "Made-in-America product."[52] However, in September 2013, U.S. Customs and Border Protection concluded the system should still be considered a Chinese product, because "the Chinese-origin Video Board and the Filter Board impart the essential character to the video teleconferencing server."[53] GSA subsequently took the system off the list of products agencies can buy. Even before the decision, no U.S. agencies had purchased this product.[54]

In a meeting in May 2013, Commissioners and DoD officials discussed DoD's interpretation of U.S. law regarding procurement sources. DoD officials indicated a stricter procurement evaluation standard that includes sourcing concerns could be applied only to items on the United States Munitions List. Items outside this list are judged by a different standard, which some officials believe might preclude concerns about the origin of products. For example, items procured for C4ISR* maintenance facilities are not subject to stricter scrutiny. Commissioners raised concerns that this interpretation of the law was limiting the department's ability to address potential risks arising from certain procurement sources. Commissioners urged DoD to expand the purview of the stricter standard to items beyond the munitions list.

DoD is currently moving in this direction. Section 806 of the National Defense Authorization Act (NDAA) for Fiscal Year 2011 is intended to address the problem, but it has yet to be fully implemented. Section 806 authorizes the Secretary of Defense and the secretaries of the Army, Navy, and Air Force to reject procurement sources for information technology on grounds of protecting supply chain security if they receive a recommendation to do so from DoD.[55] According to a DoD Congressional liaison, as of May, "DoD has proceeded to implement NDAA Section 806, beginning with a number of table-top exercises involving department procurement, legal, acquisition, engineering, and intelligence experts to expose any underlying issues with 806 implementation."[56] In addition, DoD wrote the Defense Federal Acquisition Regulation Supplement Rule implementing Section 806 and, as of May, the rule was in the process of interagency coordination.[57] These changes to DoD procurement ultimately may provide officials with the flexibility they need to protect all DoD systems. However, progress has been slow and the problem the Commissioners highlighted will remain until the new policy is implemented, potentially posing a threat to national security.

Security Implications of Cloud Computing in China

"Cloud computing, often referred to as simply 'the cloud,' is the delivery of on-demand computing resources—everything from applications to data centers—over the Internet and on a pay-for-use basis," according to IBM.[58] In *Red Cloud Rising: Cloud Computing in China*, a report for the Commission published in 2013, Defense

*C4ISR refers to command, control, communications, computers, intelligence, surveillance, and reconnaissance.

Group Inc. (DGI) describes several potential cybersecurity concerns related to China and cloud computing, including the following:

- Microsoft licensed 21Vianet, a Chinese data center services company, to provide Office 365 and Windows Azure, two cloud computing products, to customers in China. Microsoft currently plans to link 21Vianet's data centers in China to Microsoft's data centers in other parts of Asia, Europe, and North America. As a part of this plan, Windows Azure users outside China could choose to store their data in data centers in China, and Azure users in China could store their data in other countries. Domestic Chinese law authorizes the government to "inspect the electronic communication instruments and appliances and other similar equipment and installations" of organizations operating in China. If the Chinese government accesses 21Vianet's data centers, it might then potentially connect to foreign data centers through the network Microsoft is planning. DGI states, "This risk can be mitigated by designing the network with appropriate data segregation and limits on network administrator privileges." [59]
- China's Ministry of State Security (MSS), the country's main foreign intelligence collection agency, is closely connected with the Chongqing Special Cloud Computing Zone. In addition to being one of the central government agencies to authorize the establishment of the zone, the MSS has stated it is giving the zone "leading guidance and corresponding requirements." [60] The agency's connection to this cloud computing zone represents a potential espionage threat to foreign companies that might use cloud computing services provided from the zone or base operations there.[61]
- Since Chinese domain registrars and Internet service providers typically are not vigilant about users employing their services to carry out nefarious activities against computers outside China, DGI writes, "One can speculate that malicious use of Chinese cloud services may eventually take place at a higher rate than the cloud computing industry's global norm." [62]
- Given the widely acknowledged security weaknesses in networking hardware developed by Chinese companies and the shift toward use of this equipment in Chinese cloud infrastructure, "it logically follows that use of this equipment may constitute an additional vulnerability in some Chinese cloud infrastructure, beyond the standard 'baseline' level of vulnerability." [63]

In addition, cloud computing could improve the PLA's C4ISR capabilities. DGI writes that cloud computing "could enable more effective and flexible development and deployment of military equipment, while at the same time improving the survivability of the PLA's information systems by endowing them with greater redundancy (allowing a system's capabilities to survive the disabling or destruction of any individual node)." [64]

Deterring Chinese Cyber Theft against U.S. Companies

There are no indications the public exposure of Chinese cyber espionage in technical detail throughout 2013 has led China to change its attitude toward the use of cyber espionage to steal intellectual property and proprietary information. Mandiant's revelations merely led Unit 61398 to make changes to its cyber "tools and infrastructure," causing future intrusions to be harder to detect and attribute.[65] Richard Bejtlich, chief security officer at Mandiant, said Unit 61398 decreased its activity for about one month following the publishing of Mandiant's report in February.[66] Former and current U.S. officials said the U.S. government's sharing of IP addresses with Internet service providers contributed to this reduction in activity.[67] However, Mr. Bejtlich said Unit 61398 remains active but at lower levels compared to the period before Mandiant's report was released.[68]

It is clear naming and attempting to shame will not be sufficient to deter entities in China from engaging in cyber espionage against U.S companies. Mitigating the problem will require a long-term and multifaceted approach that centers on changing China's cost-benefit calculus.[69] Congress, the Obama Administration, and outside experts are discussing a number of potential U.S. actions and policies, including the following:

Link Chinese economic cyber espionage to trade restrictions. An example of such a measure is the *Deter Cyber Theft Act* (S. 884), a bipartisan bill introduced in the Senate in May 2013. The bill requires the U.S. intelligence community to identify goods it assesses to have been "manufactured or otherwise produced using technologies or proprietary information" that was "developed by United States persons" and acquired through cyber espionage. It calls on the President to block the import of these goods if the President deems it necessary for safeguarding intellectual property rights or the DoD supply chain.[70]

Prohibit Chinese firms using stolen U.S. intellectual property from accessing U.S. banks. In May 2013, the Commission on the Theft of American Intellectual Property (hereafter "the IP Commission"),* released a report that examines the pilfering of U.S. intellectual property and presents policy recommendations to address the problem. The IP Commission recommends the U.S. government "deny the use of the American banking system to foreign companies that repeatedly benefit from the misappropriation of American intellectual property."[71] Roy Kamphausen, senior advisor for political and security affairs at the National Bureau of Asian Research and the deputy executive director for the IP Commission, explained at the Commission's roundtable the U.S. government could determine whether or not a foreign company should be sanctioned based on a combination of information from commercial or government sources, and well-defined bench-

*The IP Commission was co-chaired by Dennis Blair, former U.S. director of national intelligence, and Jon Huntsman, former U.S. ambassador to China.

Deterring Chinese Cyber Theft against U.S. Companies—*Continued*

marks, such as the results of legal cases in the past involving the company.[72]

Ban U.S. travel for Chinese organizations that are involved with cyber espionage. Dr. Mulvenon suggested to the Commission the United States needs "to create a constituency of people in China who want to succeed but are being harmed by government cyber espionage efforts that they had nothing to do with." He believes placing Chinese companies and universities involved with cyber espionage on a list of entities that are barred from entry into the United States would help to build this constituency. However, Dr. Mulvenon warned this policy would have to be implemented carefully and deliberately, because sanctioning Chinese companies that are connected to foreign multinational companies "would be self-defeating in some cases."[73] For example, if a U.S. company has a partnership with a Chinese company, such measures might hinder the U.S. company's ability to do business with its Chinese partner.

Use counterintelligence techniques, such as deliberately providing incorrect information to cyber spies to "poison the well."[74] Dr. Mulvenon explained to the Commission this could lead the Chinese government "to spend more and more resources actually figuring out whether things are true or not." He argued, "The more problems they have in that system will lead them to begin to accelerate the trends toward centralization of authority and decision-making, and . . . I think the goal of our policy should be to make it as difficult to get a computer network exploit operation approved in the Chinese system as it is currently in our system."*[75] However, David Merkel, Mandiant's chief technology officer, doubts the effectiveness of this tactic. He said, "Those kinds of techniques can be effective in highly-targeted ways, used by specialists to get some particular result like learning more information about an adversary . . . but as some kind of broad-based defense or mechanism to change the economics of stealing digital information, I just don't see it."[76] Mr. Merkel explained, "When I go take a look at a large organization and the challenges it has managing its own legitimate information, and then you talk about managing legitimate disinformation and being able to tell one from the other and being able to make decisions based on what happens with it seems pretty far fetched."[77]

Encourage the U.S. government, military, and cleared defense contractors to implement measures to reduce the effectiveness of Chinese cyber operations and increase the risk of conducting such operations for Chinese organizations. For example, the IP Commission recommends measures such as "meta-tagging, water-

*Dr. Mulvenon said that in China there is a "bottom up, grassroots, entrepreneurial sort of cyber espionage framework." He described U.S. cyber espionage as "top down . . . and controlled," and involving a great deal of oversight. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

Deterring Chinese Cyber Theft against U.S. Companies—*Continued*

marking, and beaconing,"[78] because they can help identify sensitive information and code a digital signature within a file to better detect intrusion and removal.[79] These tags also might be used as evidence in criminal, civil, or trade proceedings to prove data was stolen.

Clarify the legal rights of companies, and the types of action that are prohibited, regarding finding and recovering intellectual property that is stolen through cyber intrusions. Mr. Kamphausen said U.S. companies "need the right tools that afford them the protections, legal and otherwise, so that they can do what's in their own interest."[80]

Pass legislation permitting U.S. companies to conduct offensive cyber operations in retaliation against intrusions into their networks. Such operations could range from "actively retrieving stolen information" to "physically disabling or destroying the hacker's own computer or network." The IP Commission explores this option in its report but ultimately does not endorse it at the current time, because the possibility that retaliatory actions could significantly impair neutral computers or networks makes this option undesirable.[81]

Improve opportunities for U.S. companies to pursue legal action in the United States against Chinese commercial espionage. The IP Commission recommends the Economic Espionage Act (18 U.S.C. § 1831–1839) be amended to "provide a federal private right of action for trade secret theft."[82] Mr. Kamphausen explained, "This essentially means you can bring your own [law] suit. You don't have to wait for the government to take one up on your behalf."[83]

Shift jurisdiction for all appeals in Economic Espionage Act cases to the Court of Appeals for the Federal Circuit. The IP Commission recommends Congress "make the Court of Appeals for the Federal Circuit (CAFC) the appellate court for all actions under the [Economic Espionage Act]."[84] At present, appeals in Economic Espionage Act cases are handled by a court of appeals in one of the United States' 12 regional circuits.[85] The IP Commission writes, "The CAFC serves as the appellate court for nearly all IP-related cases, and thus has a high degree of competency on IP issues. Making the CAFC the appellate court for all [Economic Espionage Act] issues ensures a degree of continuity in judicial opinion. Moreover, it helps support the federal circuit in expanding extraterritorial enforcement."[86]

Encourage U.S. companies and individuals to bring cases of cyber theft of intellectual property to intellectual property courts in China. According to Mr. Kamphausen, "Enormous strides have been made within the Chinese legal system with regard to protection of intellectual property and then enforcement actions

Deterring Chinese Cyber Theft against U.S. Companies—*Continued*

once cases are brought."[87] In his comments, he indicated to the Commission these courts may become a viable option for U.S. companies seeking recourse when their intellectual property has been stolen.

Furthermore, a variety of potential multilateral measures to deter Chinese cyber theft are under discussion, including the following:

Expand information sharing among countries regarding cyber threats. For example, countries could create an international list of "bad players" to which private companies could contribute information.[88]

Include standards for safeguarding intellectual property in negotiations of the Trans-Pacific Partnership (TPP) and the Transatlantic Trade and Investment Partnership (T–TIP) agreements.[89] Intellectual property rights is one of the issues partner countries are discussing in these negotiations.[90] However, the TPP negotiating parties have yet to reach consensus on this issue. They met in Tokyo in October 2013 to discuss the intellectual property chapter of the TPP.[91] The United States and the European Union only recently started negotiating the T–TIP, thus discussions of intellectual property rights in this forum are in the beginning stage.[92]

Finally, some discussions focus on improving the U.S. government's ability to develop and implement cyber policy as necessary steps to address Chinese cyber theft. Suggestions include the following:

Appoint a Cabinet-level official to oversee an interagency process regarding the protection of intellectual property. According to the IP Commission, this step is necessary, because executive branch "efforts to protect American intellectual property will involve literally thousands of detailed actions—data gathering and research, interagency coordination, work with the private sector, coordination with Congress, and interactions with foreign government agencies."[93] The IP Commission adds this undertaking will involve "expert officials across many departments and agencies."[94]

Enhance cooperation between the U.S. government and private companies. During the Commission's roundtable, Bruce Quinn, vice president for government relations with Rockwell Automation, stressed the importance of improving cooperation between the U.S. government and the private sector to protect U.S. intellectual property from cyber intrusions. Most importantly, he said the government could provide companies with information about threats to their intellectual property as well as suggestions for protecting it. Mr. Quinn would like to see a model whereby if a company shares information about a threat with the govern-

Deterring Chinese Cyber Theft against U.S. Companies—*Continued*

ment, the government would later provide the company with a report detailing its understanding of that threat. He said the government should provide companies with a point-of-contact for information regarding cyber threats to intellectual property.* According to Mr. Quinn, this is particularly important for small- and medium-sized companies. He explained Rockwell has "contacts with the government. . . . But these small- and medium-sized companies that funnel into us, that are critical to us being successful, they don't have that access." He suggested the U.S. Department of Commerce's Foreign Commercial Service could be this point-of-contact. Under such an arrangement, the Foreign Commercial Service would have access to threat information from other U.S. government agencies. He explained, "It doesn't have to be detailed information, but it has to be enough that they can sensitize these small- and medium-sized manufacturers to the threat and make recommendations to them if they're looking at entering certain markets, how to best protect themselves, what to look for, what are the red flags." He also suggested, given the government's knowledge about cyber threats, the U.S. Defense Advanced Research Projects Agency could partner with U.S. companies to develop defensive technologies to combat cyber intrusions and then release those technologies for purchase by the public.[95]

Implications for the United States

China's cyber espionage against U.S. commercial firms poses a serious threat to U.S. business interests and competiveness in key industries. While it is clear the economic cost of cyber espionage to the United States is significant, precise numbers are impossible to calculate. A July 2013 interim report based on an ongoing study by McAfee and CSIS estimates the annual cost of both cyber crime† and cyber espionage targeting U.S. persons and entities is between $24 billion and $120 billion. The report does not separate out the cost of cyber espionage, in particular, from the total amount or estimate the cost of cyber espionage originating from specific countries, such as China.[96] *The IP Commission Report* assesses the damage to the U.S. economy due to the theft of intellectual property by all means to be around $300 billion a year. Using a range of estimates from prominent studies of this issue, the IP Commission states 50 to 80 percent of international intellectual property theft originates in China. *The IP Commission Report* lists what it appraises to be the numerous difficulties with calculating the cost of intellectual

*This proposal differs from President Obama's February 2013 executive order regarding cybersecurity, in that the executive order is focused on information sharing between the government and critical infrastructure providers. The White House, "Executive Order—Improving Critical Infrastructure Cybersecurity" (Washington, DC: February 12, 2013). *http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity*.

†The McAfee and CSIS report defines cyber crime as the theft of financial assets, whereas the report's examination of cyber espionage is focused on the theft of intellectual property and confidential information from companies. James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: CSIS, July 22, 2013), pp. 8–11.

property theft, including using surveys of a sample of companies to draw conclusions about an entire sector or a variety of sectors.* [97] General Keith Alexander, director of the NSA and commander of U.S. Cyber Command, assessed the cost to U.S. companies of intellectual property theft to be about $250 billion a year, although not all the losses are due to Chinese activity.[98]

The theft of trade secrets is a major concern for U.S. businesses with operations in China. The U.S.-China Business Council's 2013 survey of its members found they "cited trade secrets as the intellectual property (IP) issue of most concern in China." [99] If effective action to curb commercial espionage is not taken, this problem might worsen for U.S. companies. Dr. Lewis testified to the House Committee on Energy and Commerce's Subcommittee on Oversight and Investigations that although, "for China, there has been a lag of several years, perhaps as many as ten, between successful acquisition through espionage and the ability to produce competing products (be they military or civil) . . . [the] lag time between acquisition and the appearance of a competing product based on stolen technology is decreasing, as China's ability to absorb and utilize technology has increased." [100] This suggests the demand for U.S. intellectual property from within China could increase and with it the amount and value of intellectual property stolen.

If Chinese companies are able to duplicate technology and products using intellectual property acquired by cyber theft from U.S. companies, they may be able to compete even more effectively with U.S. companies in markets worldwide. Stealing intellectual property could allow Chinese companies to forgo some of the time and expenditure necessary for research and development.[101] Beyond theft of proprietary information regarding technology or products, the theft of corporate e-mail correspondence or internal documents can aid Chinese companies in competitive bidding for commercial contracts.[102] In each of these cases, U.S. companies might lose revenue and lay off workers or even go out of business. The theft of intellectual property, if publicized, also might lead to a drop in a company's stock value.[103] Moreover, the authors of the McAfee and CSIS report write, "Cyber espionage and crime may slow the pace of innovation, distort trade, and create social costs from job loss. This larger effect may be more important than . . . [the] actual number [of dollars lost]." [104]

China's cyber espionage also has security implications. Information gained from intrusions into the networks of U.S. military contractors likely improves China's insight into U.S. weapon systems, enables China's development of countermeasures, and shortens China's research and development timelines for military technologies.[105] In addition, the same intrusions Chinese cyber actors use for espionage also could be used to prepare for offensive cyber operations. Chinese cyber actors could place latent capabilities in U.S. software code or hardware components that might be employed in a potential conflict between the United States and China.

---

*For the IP Commission's full assessment of the difficulties in calculating the cost of intellectual property theft, see The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), pp. 23–30. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.*

Conclusions

- The Chinese government is directing and executing a large-scale cyber espionage campaign against the United States and to date has successfully targeted the networks of U.S. government and private organizations, including those of DoD and private firms. These activities are designed to achieve a number of broad economic and strategic objectives, such as gathering intelligence, providing Chinese firms with an advantage over their competitors worldwide, advancing long-term research and development objectives, and gaining information that could enable future military operations.
- China has not reduced its cyber intrusions against the United States despite recent public exposure of Chinese cyber espionage in technical detail. This suggests Beijing has decided to continue its cyber campaign against the United States.
- Developments in cloud computing in China may present cybersecurity risks for U.S. users and providers of cloud computing services. The relationship between China's Ministry of State Security and the Chongqing Special Cloud Computing Zone represents a potential espionage threat to foreign companies that might use cloud computing services provided from the zone or base operations there. In addition, the plan to link 21Vianet's data centers in China and Microsoft's data centers in other countries suggests the Chinese government one day may be able to access data centers outside China through Chinese data centers.
- There is an urgent need for Washington to take action to prompt Beijing to change its approach to cyberspace and deter future Chinese cyber theft. Actions and policies under discussion include the following: passing new legislation or modifying existing legislation; changing the cost-benefit calculus of Chinese cyber actors and China's leaders through sanctions and counterintelligence tactics; undertaking multilateral measures; appointing a Cabinet-level official to oversee an interagency process regarding the protection of intellectual property; and enhancing cooperation between the U.S. government and the private sector. These would be more effective if used in combination, as they probably would lead Beijing to make only temporary or minor changes to its cyber espionage activities if used in isolation.

ENDNOTES FOR SECTION 2

1. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: February 2013), pp. 2–4, 9, 21–23. *http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf*.

2. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: February 2013), p. 9. *http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf*.

3. House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Hearing on Cyber Espionage and the Theft of U.S. Intellectual Property and Technology,* written testimony of Larry M. Wortzel, 113th Cong., 1st sess., July 9, 2013.

4. Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure* (Arlington, VA: Project 2049 Institute, November 2011), pp. 7–11. *http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf*.

5. Danny Radron and Siobhan Gorman, "U.S., Firms Draw a Bead on Cyberspies," *Wall Street Journal*, July 12, 2013. *http://online.wsj.com/article/SB10001424127887324694904578600041603746114.html*.

6. Craig Timberg, "Vast majority of global cyber-espionage emanates from China, report finds," *Washington Post*, April 22, 2013. *http://www.washingtonpost.com/business/technology/vast-majority-of-global-cyber-espionage-emanates-from-china-report-finds/2013/04/22/61f52486-ab5f-11e2-b6fd-ba6f5f26d70e_story.html*.

7. Verizon, *2013 Data Breach Investigations Report* (April 2013), pp. 5, 9, 11, 21. *http://www.verizonenterprise.com/DBIR/2013/*.

8. Tom Simonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," *MIT Technology Review*, August 2, 2013. *http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/*.

9. Larry M. Wortzel, *The Dragon Extends its Reach: Chinese Military Power Goes Global* (Washington, DC: Potomac Books, 2013), p. 142.

10. Larry M. Wortzel, *The Dragon Extends its Reach: Chinese Military Power Goes Global* (Washington, DC: Potomac Books, 2013), p. 145.

11. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: U.S. Department of Defense, May 2013), p. 36.

12. David Alexander, "Cyber Threats Pose 'Stealthy, Insidious' Danger: Defense Chief," Reuters, May 31, 2013. *http://www.reuters.com/article/2013/05/31/us-usa-defense-hagel-cyber-idUSBRE94U05Y20130531*.

13. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012* (Washington, DC: U.S. Department of Defense, May 2012), p. 9.

14. David Helvey, "Press Briefing on 2012 DoD Report to Congress on *Military and Security Developments Involving the People's Republic of China"* (Washington, DC: May 18, 2012). *http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5036*.

15. William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (London and New York: Routledge, 2013), pp. 225–226.

16. Ministry of Foreign Affairs (China), *"2013 Nian 2 Yue 19 Ri Waijiaobu Fayanren Honglei Zhuchi Lixing Jizhehui"* (Ministry of Foreign Affairs Spokesperson Hong Lei Presides Over Regular Press Conference) (Beijing, China: February 19, 2013). *http://www.fmprc.gov.cn/mfa_chn/fyrbt_602243/t1014798.shtml*.

17. Ministry of National Defense (China), *"Zhonguo Junfang Jixu Pibo 'Wangluo Gongji' Bushi Zhize"* (China's Military Continues to Refute False Accusations of "Cyber Attacks") (Beijing, China: February 20, 2013). *http://news.mod.gov.cn/headlines/2013-02/20/content_4433454.htm*.

18. Don Lee, "China Dismisses U.S. Accusations of Cyber-Spying," *Los Angeles Times*, May 7, 2013. *http://articles.latimes.com/2013/may/07/world/la-fg-wn-china-us-cyber-spying-20130507*.

19. Nicole Perlroth, "Hackers in China Attacked the Times for the Last 4 Months," *New York Times*, January 30, 2013. *http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?hp&_r=1&*; Siobhan Gorman, Devlin Barrett, and Danny Yadron, "Chinese Hackers Hit U.S. Media," *Wall Street Journal*, January 31, 2013. *http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html*.

20. Nicole Perlroth, "Hackers in China Attacked the Times for the Last 4 Months," *New York Times*, January 30, 2013. *http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?hp&_r=1&*.

21. Nicole Perlroth, "Hackers in China Attacked the Times for the Last 4 Months," *New York Times*, January 30, 2013. *http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?hp&_r=1&*.

22. Siobhan Gorman, Devlin Barrett, and Danny Yadron, "Chinese Hackers Hit U.S. Media," *Wall Street Journal*, January 31, 2013. *http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html;* Craig Timberg and Ellen Nakashima, "Chinese Hackers Suspected in Attack on The Post's Computers," *Washington Post*, February 1, 2013. *http://articles.washingtonpost.com/2013-02-01/business/36685685_1_chinese-hackers-cyberattacks-mandiant*.

23. Siobhan Gorman, Devlin Barrett, and Danny Yadron, "Chinese Hackers Hit U.S. Media," *Wall Street Journal*, January 31, 2013. *http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html*.

24. Ellen Nakashima, "Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say," *Washington Post*, May 20, 2013. *http://articles.washingtonpost.com/2013-05-20/world/39385755_1_chinese-hackers-court-orders-fbi*.

25. Ellen Nakashima, "Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say," *Washington Post*, May 20, 2013. *http://articles.washingtonpost.com/2013-05-20/world/39385755_1_chinese-hackers-court-orders-fbi*.

26. Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: October 10, 2012), p. 1. *http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf*.

27. Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *Washington Post*, May 27, 2013. *http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html*.

28. U.S. Department of Justice, "Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets" (Washington, DC: June 27, 2013). *http://www.justice.gov/opa/pr/2013/June/13-crm-730.html*.

29. Melanie Hart, "Criminal Charges Mark New Phase in Bellwether U.S.-China Intellectual Property Dispute" (Washington, DC: Center for American Progress, June 2013). *http://www.americanprogress.org/issues/china/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/*; U.S. Department of Justice, "Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets" (Washington, DC: June 27, 2013). *http://www.justice.gov/opa/pr/2013/June/13-crm-730.html*.

30. Erin Ailworth, "Files Trace Betrayal of a Prized China-Mass. Partnership," *Boston Globe*, July 10, 2013. *http://www.bostonglobe.com/business/2013/07/09/global-chase-cracked-corporate-espionage-case/8HC7wKBJezDkNFNSWB5dFO/story.html*; U.S. Department of Justice, "Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets" (Washington, DC: June 27, 2013). *http://www.justice.gov/opa/pr/2013/June/13-crm-730.html*.

31. Carl Sears and Michael Isikoff, "Chinese Firm Paid Insider 'to Kill My Company,' American CEO Says," *NBC News*, August 6, 2013. *http://investigations.nbcnews.com/_news/2013/08/06/19566531-chinese-firm-paid-insider-to-kill-my-company-american-ceo-says?lite*.

32. Erin Ailworth, "Files Trace Betrayal of a Prized China-Mass. Partnership," *Boston Globe*, July 10, 2013. *http://www.bostonglobe.com/business/2013/07/09/global-chase-cracked-corporate-espionage-case/8HC7wKBJezDkNFNSWB5dFO/story.html*.

33. Melanie Hart, "Criminal Charges Mark New Phase in Bellwether U.S.-China Intellectual Property Dispute" (Washington, DC: Center for American Progress, June 2013). *http://www.americanprogress.org/issues/china/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/*.

34. Reuters, "U.S., China Agree To Work Together on Cyber Security," April 13, 2013. *http://www.reuters.com/article/2013/04/13/us-china-us-cyber-idUSBRE93C05T20130413*.

35. BBC News, "US-China Cyber Security Working Group Meets," July 8, 2013. *http://www.bbc.co.uk/news/world-asia-china-23177538*.

36. U.S. Department of State, "U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track" (Washington, DC: July 12, 2013). *http://www.state.gov/r/pa/prs/ps/2013/07/211861.htm*.

37. House Foreign Affairs Committee, Subcommittee on Asia and the Pacific, *Hearing on Asia: The Cybersecurity Battleground,* written testimony of James A. Lewis, 113th Cong., 1st sess., July 23, 2013.

38. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (June

7, 2013), p. 8. *https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/$FILE/A%2068%2098.pdf*.

39. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (June 7, 2013), p. 8. *https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/$FILE/A%2068%2098.pdf*.

40. James Crawford, *Articles on Responsibility of States for Internationally Wrongful Acts (2001)* (New York: United Nations Audiovisual Library of International Law, 2012). *http://legal.un.org/avl/ha/*rsiwa/*rsiwa.html*.

41. Jen Psaki, "Statement on Consensus Achieved by the UN Group of Governmental Experts On Cyber Issues," (Washington, DC, June 7, 2013). *http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm*; Philip Rucker and Ellen Nakashima, "Obama Begins Summit With Xi as China Agrees to Cyber Framework," *Washington Post*, June 7, 2013. *http://articles.washingtonpost.com/2013-06-07/politics/39823657_1_president-obama-chinese-president-xi-jinping-obama-and-xi*.

42. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

43. Adam Segal, "China, International Law, and Cyberspace," Asia Unbound, October 2, 2012. *http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/*; Timothy Farnsworth, "Expert Group Coalesces on Cyberspace," *Arms Control Today*, July/August 2013. *http://www.armscontrol.org/act/2013_0708/Expert-Group-Coalesces-on-Cyberspace*; and Philip Rucker and Ellen Nakashima, "Obama Begins Summit With Xi as China Agrees to Cyber Framework," *Washington Post*, June 7, 2013. *http://articles.washingtonpost.com/2013-06-07/politics/39823657_1_president-obama-chinese-president-xi-jinping-obama-and-xi*.

44. Lana Lam, "Edward Snowden: US Government Has Been Hacking Hong Kong and China for Years," *South China Morning Post* (Hong Kong), June 14, 2013. *http://www.scmp.com/news/hong-kong/article/1259508/edward-snowden-us-government-has-been-hacking-hong-kong-and-china?page=all*.

45. Chris Buckley, "Chinese Defense Ministry Accuses U.S. of Hypocrisy on Spying," *New York Times*, June 27, 2013. *http://www.nytimes.com/2013/06/28/world/asia/chinese-defense-ministry-accuses-us-of-hypocrisy-on-spying.html?_r=0*.

46. The White House, "Press Briefing by National Security Advisor Tom Donilon" (Washington, DC: June 8, 2013). *http://www.whitehouse.gov/the-press-office/2013/06/09/press-briefing-national-security-advisor-tom-donilon*; *Bloomberg TV*, "Obama: Blunt Conversation with China on Hacking," June 18, 2013. *http://www.bloomberg.com/video/obama-blunt-conversation-with-china-on-hacking-EvHIfGSCRsGYoAVpMiuCmA.html*; and The White House, "Readout of the President's Meeting with the Co-Chairs of the U.S.-China Strategic and Economic Dialogue" (Washington, DC: July 11, 2013). *http://www.whitehouse.gov/the-press-office/2013/07/11/readout-president-s-meeting-co-chairs-us-china-strategic-and-economic-di*.

47. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

48. Mike Rogers and C.A. Dutch Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (Washington, DC: House Permanent Select Committee on Intelligence, October 8, 2012), pp. vi, 1, 3.

49. Christopher Joye, "Transcript: Interview with Former CIA, NSA Chief Michael Hayden," *Australian Financial Review*, July 19, 2013. *http://www.afr.com/p/national/transcript_interview_with_former_KnS7JDIrw73GWlljxA7vdK*.

50. Kathleen Miller, "China Video Tools for U.S. Help Spurs Spy Anxiety," Bloomberg, August 18, 2013. *http://www.bloomberg.com/news/2013-08-19/china-video-tools-for-u-s-with-american-help-spurs-spy-anxiety.html*.

51. Tom Pullar-Strecker, "Huawei Founder Gives First Ever Media Interview," *Fairfax Media* (Auckland), May 9, 2013. *http://www.stuff.co.nz/business/industries/8651260/Huawei-CEO-gives-first-ever-interview*.

52. Kathleen Miller, "China Video Tools for U.S. Help Spurs Spy Anxiety," Bloomberg, August 18, 2013. *http://www.bloomberg.com/news/2013-08-19/china-video-tools-for-u-s-with-american-help-spurs-spy-anxiety.html*.

53. U.S. Customs and Border Protection, "Notice of Issuance of Final Determination Concerning Video Teleconference Server," September 11, 2013. *http://www.ofr.gov/OFRUpload/OFRData/2013-22765_PI.pdf*.

54. Kathleen Miller, "China Video Tools for U.S. Help Spurs Spy Anxiety," Bloomberg, August 18, 2013. *http://www.bloomberg.com/news/2013-08-19/china-video-tools-for-u-s-with-american-help-spurs-spy-anxiety.html*.
55. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2011* (Public Law 111–383), 111th Cong., 2nd sess., January 7, 2011. *http://www.gpo.gov/fdsys/pkg/PLAW-111publ383/pdf/PLAW-111publ383.pdf*.
56. Special Assistant to the DoD Chief Information Officer, Office of the Assistant Secretary of Defense for Legislative Affairs, e-mail interview with Commission staff, May 28, 2013.
57. Special Assistant to the DoD Chief Information Officer, Office of the Assistant Secretary of Defense for Legislative Affairs, e-mail interview with Commission staff, May 28, 2013.
58. IBM, "What is Cloud Computing?" *http://www.ibm.com/cloud-computing/us/en/what-is-cloud-computing.html*. For a fuller explanation of China's efforts in this arena, see Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013).
59. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), pp. 32–34.
60. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), pp. 37.
61. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), p. 37.
62. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), p. 39.
63. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), p. 43.
64. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), p. 38.
65. Dan Mcwhorter, "APT1 Three Months Later—Significantly Impacted, Though Active & Rebuilding," *M-unition*, May 21, 2013. *https://www.mandiant.com/blog/apt1-months-significantly-impacted-active-rebuilding/*; Richard Bejtlich (chief security officer at Mandiant), telephone interview with Commission staff, August 21, 2013.
66. Richard Bejtlich (chief security officer at Mandiant), telephone interview with Commission staff, August 21, 2013.
67. Danny Radron and Siobhan Gorman, "U.S., Firms Draw a Bead on Cyberspies," *Wall Street Journal*, July 12, 2013. *http://online.wsj.com/article/SB10001424127887324694904578600041603746114.html*.
68. Richard Bejtlich (chief security officer at Mandiant), e-mail interview with Commission staff, November 12, 2013.
69. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).
70. U.S. Senate, *Deter Cyber Theft Act* (S. 884), 113th Cong., 1st sess. (introduced in Senate May 7, 2013). *http://thomas.loc.gov/cgi-bin/query/z?c113:S.884:*.
71. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 66. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf*.
72. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).
73. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).
74. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013); *Economist*, "Admit nothing and deny everything," June 8, 2013. *http://www.economist.com/news/china/21579044-barack-obama-says-he-ready-talk-xi-jinping-about-chinese-cyber-attacks-makes-one*.
75. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).
76. John Reed, "DoD Says Don't Worry About Hackers Accessing Key U.S. Weapons Designs," *Foreign Policy*, May 28, 2013. *http://killerapps.foreignpolicy.com/*

posts/2013/05/28/dod_says_dont_worry_about_hackers_accessing_key_us_weapons_designs.

77. John Reed, "DoD Says Don't Worry About Hackers Accessing Key U.S. Weapons Designs," *Foreign Policy*, May 28, 2013. *http://killerapps.foreignpolicy.com/posts/2013/05/28/dod_says_dont_worry_about_hackers_accessing_key_us_weapons_designs*.

78. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 81. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf*.

79. Cisco, "Data Loss Prevention." *http://www.cisco.com/en/US/netsol/ns895/index.html*.

80. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

81. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 81. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf*.

82. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 5.

83. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

84. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 5. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf*.

85. Trade Secrets Institute, "Cases from Economic Espionage Act" (Brooklyn, NY: Brooklyn Law School). *http://tsi.brooklaw.edu/category/legal-basis-trade-secret-claims/economic-espionage-act*; United States Courts, "Courts of Appeals." *http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/CourtofAppeals.aspx*.

86. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 74. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf*.

87. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

88. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

89. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

90. European Commission, "EU and US conclude first round of TTIP negotiations in Washington," July 12, 2013. *http://trade.ec.europa.eu/doclib/press/index.cfm?id=941*; Shawn Donnan and Ben Bland, "TPP leaders say 'significant progress made," *Financial Times*, October 8, 2013. *http://www.ft.com/intl/cms/s/0/fdfe4b36-2fe5-11e3-9eec-00144feab7de.html?siteedition=intl#axzz2ho8IOsYP*.

91. Kyodo News (Tokyo), "TPP Countries To Speed Up Talks On Intellectual Property: Official," October 28, 2013. *http://e.nikkei.com/e/fr/tnks/Nni20131028D28JF572.htm*.

92. European Commission, "EU and US conclude first round of TTIP negotiations in Washington," July 12, 2013. *http://trade.ec.europa.eu/doclib/press/index.cfm?id=941*.

93. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 63. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf*.

94. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 63. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf*.

95. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

96. James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: CSIS, July 22, 2013), p. 5. *http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf*.

97. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), pp. 2–3, 23. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf*.

98. Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *Foreign Policy*, July 9, 2012. *http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history*.

99. U.S.-China Business Council, "Shanghai: Battling Trade Secrets and Data Theft in China." *http://www.uschina.org/battling-trade-secrets-and-data-theft-china*.

100. House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Hearing on Cyber Espionage and the Theft of U.S. Intellectual Property and Technology,* written testimony of James A. Lewis, 113th Cong., 1st sess., July 9, 2013.

101. Mike McConnell, Michael Chertoff, and William Lynn, "Cyber Thievery is National Policy—And Must be Challenged," *Wall Street Journal*, January 27, 2012. *http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html*.

102. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013); James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: CSIS, July 22, 2013), p. 10. *http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf*.

103. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 10. *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf*.

104. James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: CSIS, July 22, 2013), p. 5. *http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf*.

105. Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *Washington Post*, May 27, 2013. *http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html*.