SECTION 4: COMMERCIAL CYBER ESPIONAGE AND BARRIERS TO DIGITAL TRADE IN CHINA

Introduction

China causes increasing harm to the U.S. economy and security through two deliberate policies targeting the United States: coordinated, government-backed theft of information from a variety of U.S.-based commercial enterprises and widespread restrictions on content, standards, and commercial opportunities for U.S. businesses. This section examines how hackers working for the Chinese government—or with the government's support and encouragement—have infiltrated the computer networks of U.S. agencies, contractors, and companies, and stolen their trade secrets, including patented material, manufacturing processes, and other proprietary information. The Chinese government has provided that purloined information to Chinese companies, including state-owned enterprises (SOEs).

The Chinese government also imposes heavy-handed censorship on Internet content and social media, which has driven from the Chinese market those U.S. companies unwilling to follow the authoritarian dictates of the government.* The Chinese government has also begun to censor material originating outside its borders by directing distributed denial of service (DDoS) attacks against U.S.-based information providers. In addition, Beijing has implemented discriminatory regulations and standards in China to limit the commercial opportunities for U.S. companies seeking to conduct legitimate business there.

The United States is ill prepared to defend itself from cyber espionage when its adversary is determined, centrally coordinated, and technically sophisticated, as is the Chinese Communist Party (CCP) and government. The design of the Internet—developed in the United States to facilitate open communication between academia and government, and eventually expanded to include commercial opportunities—leaves it particularly vulnerable to spies and thieves. As the largest and most web-dependent economy in the world, the United States is also the largest target for cyber espionage of commercial intellectual property (IP). "Well-resourced, advanced cyber threats that use sophisticated tactics, techniques and procedures are able to bypass [U.S.] conventional security deployments almost at-will," according to Jen Weedon, manager of threat intelligence at FireEye, Inc., a cybersecurity firm. "American

*The France-based watchdog group Reporters Without Borders ranked China 175 out of 180 countries in its 2014 worldwide *Index of Press Freedom*. Among the U.S.-based companies excluded or heavily censored by China are Google, Facebook, Twitter, and Instagram. For more on Chinese censorship, see Beina Xu, "Media Censorship in China," *Council on Foreign Relations*, April 7, 2015.

companies are being forced to fight a battle against adversaries possessing nation-state capabilities, which is not a fair fight." [1]

These activities by China's government were the subject of the Commission's June 15 *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, held shortly after the Office of Personnel Management (OPM) revealed that its computer network experienced an intrusion apparently originating in China. This network breach resulted in the theft of personal information on more than 22 million federal employees, retirees, contractors, applicants for government jobs, and their contacts and families.* Some of the stolen files included SF–86 application forms, which contain detailed personal information of federal workers and contractors applying for security clearances.[2]

Cyber Espionage for Commercial and Strategic Advantage

The Cost and Extent of Chinese Cyber Espionage

The incidence of sophisticated cyber intrusions into U.S. government and private computer networks—particularly those involving "zero-day attacks"† and the exfiltration of large amounts of commercial data and personally identifiable information‡—is on the increase. Cyber espionage for the purpose of commercial gains "presents one of the most significant economic and national security challenges facing the United States," according to Paul Tiao, a former Federal Bureau of Investigation (FBI) official who now is an attorney in private practice at Hunton & Williams in Washington, DC, and who testified before the Commission.[3] The economic cost of cyber crime and espionage is estimated at $375 billion to $575 billion annually worldwide, or between 15 percent and 20 percent of the value created by the Internet, according to a 2014 study by Intel Corporation's McAfee cybersecurity branch and the Center for Strategic and International Studies.[4] The study estimates that cyber attacks against targets in the United States could result in a permanent reduction of as many as 200,000 U.S. jobs due to lost business income and expenses to repair the damage. The cost of defending against such attacks is also increasing. The global market for cybersecurity products and services is estimated to be $77 billion in 2015—about the size of all the Federal Government's public information technology (IT) spending budget—with spending growing twice as fast as general spending on IT.[5]

The cost of individual cyber intrusions, which includes detection, repair, and remediation, has also been on the rise. A 2014 survey

---

* For more information on China's cyber espionage and related activities, see U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress*, November 2012, and *2013 Annual Report to Congress*, November 2013.

† Zero-day attacks employ hacking techniques and malware tailored to a specific target rather than generic products available online, which can be detected through the use of commercially available cybersecurity software.

‡ Personally identifiable information can include name, Social Security number, passport number, driver's license number, taxpayer identification number, financial account or credit card number, banking information, address, date of birth, place of birth, religion, race, weight, activities, employment and medical information, education, fingerprints, retinal scan, voice signature, facial geometry, photographic image, and travel records. Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information: Recommendations of the National Institute of Standards and Technology* (Special Publication 800–122), *National Institute of Standards and Technology*, *U.S. Department of Commerce*, April 2010.

of 59 large U.S. companies by the Ponemon Institute and Hewlett-Packard found the average annual cost of responding to commercial cyber attacks was $12.7 million, up 96 percent from the previous five years.[6] During this period, the number of attacks against the 59 firms was up 176 percent, with an average of 138 successful attacks each week. The average time taken to detect an attack was 170 days, with an average of 45 days spent resolving the damage. The costs included detection, data recovery, loss of information, and business disruption.[7]

The cost of a network breach can impact a company in a variety of ways, according to Mr. Tiao. They include:

- Loss of IP to a potential competitor that may be able to use it to develop and sell a competing product or to reduce research and development costs;
- Reduced incentives for technological innovation by targeted companies;
- Loss of confidential business-sensitive information that may, for example, be used by a company to underbid the victim for a lucrative contract or to undermine the victim's strategy in business negotiations;
- Opportunity costs in the form of service and employment disruptions, lost sales and revenues, and reduced trust and use of online commercial activities;
- Costs of securing networks, cyber insurance, and recovery from cyber attacks;
- Legal fees associated with breach-related litigation and government enforcement actions; and
- Reduced stock prices and reputational harm suffered by victim companies.[8]

Even companies that have not been victimized have substantial costs to subtract from their bottom lines, according to Mr. Tiao:

> *Prior to an incident taking place, large companies devote extensive financial, staff, and consultant resources to keeping information security policies up to date, implementing technical network security programs, developing and exercising breach response plans, participating in public-private and private-private cybersecurity information sharing arrangements, negotiating the information security terms of third-party vendor agreements, ensuring that those vendors maintain adequate information security, and purchasing cyber security insurance, and training employees*.[9]

Since at least 2009, China has directed "the single largest, most intensive foreign intelligence gathering effort since the Cold War," according to cybersecurity firm Medius Research.[10] The increased success rate for intrusions against U.S. companies is often attributed to the presence of government-run or government-sponsored

teams of hackers—with China the primary culprit. The U.S. government is equating the struggle in cyberspace to a war directed against the U.S. economy, U.S. aerospace and weapons contractors, and the energy grid, among other public targets. Former Director of National Intelligence Mike McConnell warned in 2015 that "the United States is fighting a cyber war and we are losing."[11] At the Commission's June 15 hearing, witness Dennis F. Poindexter, a 30-year veteran of the U.S. Intelligence Community, noted that if, during the Cold War, "we had done nuclear deterrence the way we do cyber deterrence [against China], we'd all be speaking Russian now."[12]

Concern over the cyber theft of personally identifiable information and trade secrets has grown as massive intrusions into U.S. corporate and government computer networks have come to light. By most authoritative accounts, the largest benefactor of that transfer is China, whose government has adopted a strategy of exfiltrating large amounts of data from U.S. networks and sharing that information with Chinese competitors. "Out of the dozens of advanced cyber threat groups that we track, by far the most prevalent and focused are those that are engaging in commercial cyber espionage," testified Ms. Weedon during the Commission's June 15 hearing. According to Ms. Weedon, Chinese government hacker groups "continue to engage in widespread commercial data theft at staggering rates."[13]

In 2012, then director of the National Security Agency (NSA) General Keith Alexander said in a speech to a Colorado audience that cyber espionage represented "the biggest transfer of wealth in history."[14] In testimony before the Senate Armed Services Committee, Director of National Intelligence General James R. Clapper warned in February that, "[c]yber threats to U.S. national and economic security are increasing in frequency, scale, sophistication and severity of impact; [and] the ranges of cyber threat actors, methods of attack, targeted systems and victims are also expanding,"[15] On April 1, 2015, President Barack Obama noted that "the increasing prevalence and severity of malicious cyber-enabled activities constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[16] The President followed with a "declaration of a national emergency to deal with this threat."[17]

Mr. Poindexter describes the U.S. relationship with China as an escalating, multifaceted economic and "information war":

> *The Chinese use their intelligence services and military to collect information from the competition and feed that back into their companies. From a policy view, they steal information as a part of their national strategy to win an economic war. Their military owns some companies and what they don't own, the Central Committee controls. They win bids; they control their own commodity prices; they harass the competition as they did with Walmart and Rio Tinto. They steal intellectual property, which they then use to compete with the companies they steal it from. They leverage their surplus for political benefit and manipulate their currency valuation.*[18]

Not all China-based groups are the same, though, as Ms. Weedon noted:

> *They have different government sponsors, different targets, and varying degrees of state sponsorship or support. Some threat actors and groups that we track appear to be contractors. Certain individuals may moonlight on the side and operate for financial gain. In spite of these differences, though, the vast majority of China-based APT [Advanced Persistent Threat]* groups that we track are engaged in massive theft of IP from global corporations, particularly those involved in what the Chinese government views as areas of strategic importance*.[19]

Ms. Weedon told the Commission that China's strategic emerging industries—high-tech sectors singled out by the Chinese government for development and special support in the 12th Five-Year Plan—act as "an almost to-do list" for China-based hackers.[20] During its work on behalf of Western and Japanese clients, FireEye identified 22 "separate groups of actors stealing information" from the strategic emerging industries. Table 1 correlates the strategic emerging industries with the number of known China-based hacking groups engaging in cyber theft of information in that industry, based on figures compiled by FireEye. (This list likely understates the extent of Chinese cyber spying on behalf of strategic emerging industries in China.)

Table 1: China's Strategic Emerging Industries

Strategic Emerging Industry	Number of China-Based APT Groups Targeting This Strategic Emerging Industry
Clean Energy Technology	3
Next-Generation IT	19
Biotechnology	6
High-End Equipment Manufacturing	22
Alternative Energy	7
New Materials	12
New Energy Vehicles	6

Source: U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Jen Weedon, June 15, 2015.

Other sectors targeted for infiltration by the Chinese government include electronics, telecommunications, robotics, data services, pharmaceuticals, mobile phone services, satellite communications and imagery, and business application software.[21]

*APT stands for Advanced Persistent Threat, a designation that indicates the hackers are using sophisticated techniques over a long period to extract large amounts of information. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 2013.

The U.S. government has recognized and documented the threat posed by cyber espionage and has singled out China as the cause. A 2009 study for the Commission by Northrup Grumman warned that Chinese hacking of U.S. networks "now comprises the single greatest threat to U.S. technology and has the potential to erode the United States' long-term position as a world leader in [science and technology], innovation, and competitiveness."[22] A 2011 report from the Office of the National Counterintelligence Executive acknowledged that "Chinese actors are the world's most active and persistent perpetrators of economic espionage."[23] FBI Director James B. Comey said that Chinese hackers are "at the top of the list" of international cyber spies: "They are extremely aggressive and widespread in their efforts to break into American systems to steal information that would benefit their industry. There are two kinds of big companies in the United States; there are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."[24]

Attributing Cyber Attacks to China

China routinely denies any official involvement in cyber espionage against U.S. government or U.S. corporate networks. Chinese authorities maintain that such accusations are "baseless," and "irresponsible, and unscientific," and choose instead to accuse the United States itself of cyber espionage.[25] China's official news agency, Xinhua, said that "while [the United States] has rarely made [a] direct response to widespread concerns over appalling revelations of its cyber spying programs, some of its people, out of ulterior motives, habitually scapegoat and demonize China, repeatedly leveling groundless allegations and accusations against China."[26]

Attributing individual computer network intrusions can require intensive forensic investigation and is not always conclusive. Cyber attacks can be routed through servers in multiple countries in an attempt to disguise their origin. "Cyber operations are extraterritorial," said Mr. Poindexter, "You can conduct operations from Russia that go through China and attack the United States. You can do the reverse. . . . Anybody can attack from anywhere because of virtualization of our computer systems."[27] And there is no international convention or agreement on what constitutes attribution.[28] Consequently, says one expert, "many states currently prefer to respond to such attacks using only passive computer security measures, at least until there is more information available about the origin and the intent of the attack."[29]

Nevertheless, according to Mr. Tiao, the U.S. government and private cybersecurity companies "are so much further along in our ability to establish attribution and to identify individuals and entities that are responsible for this sort of hacking activity than we were five years ago or four years ago."[30] Attribution can be accomplished when forensics experts find patterns in "tools, tactics and procedures" and link "intrusion sets" to hacker groups and even to individuals.[31]

U.S. companies that specialize in investigating cyber attacks and espionage trace many intrusions back to servers and hackers in China. In 2013, U.S. Internet security firm Mandiant said its hun-

dreds of investigations showed that groups hacking into U.S. newspapers, government agencies, and companies "are based primarily in China and the Chinese government is aware of them."[32]

The U.S. government and cyber counterintelligence firms have grown more comfortable revealing their attribution methodology. For example, when the *New York Times* hired Mandiant to determine who hacked into its newsroom computer system to steal such sensitive data as the identities of reporters' confidential sources, the firm released a detailed report along with the methodology it used to trace the network intrusion back to the Chinese government.[33] In February 2013, Mandiant released a report tracing a major set of intrusions to a particular Chinese military intelligence unit housed in a 12-story building in Shanghai. Mandiant also published details of more than 3,000 domain names, Internet protocol addresses, encryption certificates, and malware programs of one digital spy network run by the People's Liberation Army (PLA), "Unit 61398," which Mandiant named "APT1." The unit "has systemically stolen hundreds of terabytes of data from at least 141 companies spanning 20 major industries," the Mandiant report said.[34] According to the firm, "Once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of IP, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizers' leadership."[35]

Recent Cyber Intrusions Originating in China

The improved ability of the U.S. government and cybersecurity firms to attribute cyber attacks paints a damning picture of China as an active perpetrator of cyber espionage. Table 2 summarizes select recent attacks.

Table 2: Recent Examples of Cyber Intrusions Originating in China

Recent Cyber Intrusions from China	Date Identified	Target	Source of Attack
PLA Espionage	May 2014	Six U.S. entities involved in nuclear power, metals, and solar power.	Five PLA officers indicted in May 2014
USPS Espionage	November 2014	Personal data of 800,000 employees of the U.S. Postal Service, including Social Security numbers and addresses.	China
Anthem Hack	February 2015	Social Security numbers and health information of 80 million Anthem users.	"Deep Panda" (according to CrowdStrike's analysis)
The Great Cannon Attack	April 2015	Chinese cyber weapon executed DDoS attacks against U.S. websites GitHub and GreatFire.	Chinese government (according to University of Toronto's Citizen Lab)

Table 2: Recent Examples of Cyber Intrusions Originating in China—*Continued*

Recent Cyber Intrusions from China	Date Identified	Target	Source of Attack
Mysterious Eagle Attack	April 2015	Journalists, dissidents, economic data, and military organizations that have a relation to China.	Chinese government (according to FireEye report)
OPM Hack	April 2015	Millions of sensitive and classified documents, as well as personally identifiable information of more than 22 million Americans.	China is officially the "leading suspect"
Engineering Universities Hacks	May 2015	Penn State University's engineering school, along with the school's 500 research partners. Other U.S. engineering schools hacked include Johns Hopkins University, Carnegie Mellon University, the University of California-Berkeley, and the Massachusetts Institute of Technology.	Chinese hackers (according to FireEye's analysis)
United Airlines Hack	July 2015	Personal and flight information of United Airlines passengers.	Same group as the OPM hack

Source: News reports and official U.S. documents; compiled by Commission staff.

PLA Hackers

A federal grand jury in May 2014 indicted five Chinese PLA officers for hacking and economic espionage directed at six U.S. entities involved in nuclear power, metals, and solar power.[36] According to the indictments, the five PLA officers belong to Unit 61398, the same network identified by Mandiant in 2013.[37] The May 2014 indictment was unusual for several reasons: it was a rare indictment brought under the economic espionage statute of a foreign state actor; it specifically identified individuals who are government employees, including their names, office addresses, and even their photographs and nicknames; and it identified the victims and described the attackers' methodologies. All five Chinese PLA officers are charged with 31 counts of computer fraud, identify theft, computer hacking, and trade secret theft. The espionage charge carries a penalty of up to 15 years in prison. The victims include Westinghouse Electric Company, U.S. subsidiaries of SolarWorld, United States Steel Corp., Allegheny Technologies, Inc., Alcoa, Inc., and the United Steelworkers Union.

At the time of the hack, Westinghouse was negotiating terms for construction of a nuclear power plant with a Chinese SOE. Allegheny was in a joint venture with a Chinese SOE while pursuing a trade complaint against the company, and Alcoa was also in a partnership with an SOE. The *Financial Times* reported in October 2015 that according to U.S. authorities three large Chinese SOEs—steelmaker Baosteel, aluminum manufacturer Chinalco, and SNPTC, a nuclear power company—gained an advantage over their U.S. competitors as a result of the PLA's cyber espionage.[38]

The U.S. Department of Justice promised more attempts at prosecutions and noted that, "state actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country's flag."[39] The indictments will have a limited effect on the accused since China likely will not extradite the five for a trial in the United States.* However, by releasing details of the alleged crimes involving Chinese government employees, the Administration sought to highlight the role of the Chinese government in a practice that Beijing has repeatedly refused to acknowledge. In retaliation for the indictment, the Chinese government suspended bilateral talks with the United States on cyber spying. The diplomatic loss to the United States was minimal since the Chinese negotiators were unlikely to make concessions on a practice they insisted did not exist.

Chinese Hackers Breach U.S. Postal Service Network

Chinese government hackers are suspected of an intrusion into the U.S. Postal Service's (USPS) personnel database.[40] The breach was detected in September 2014. The loss included the names, Social Security numbers, addresses, dates of birth, dates of employment, emergency contacts, and other information of all 800,000 of the Postal Services' employees, from letter carriers to the postmaster general. Data on customers who contacted the Postal Service Customer Care Service by phone or e-mail were also obtained by the hackers. Randy Miskanic, the head of the USPS digital security testified before a House committee that the hack was "very sophisticated."[41] The revelation coincided with the visit of President Obama to Beijing for talks with CCP General Secretary and President Xi Jinping, which included a discussion about China's cyber spying. At the time, former NSA general counsel Steward A. Baker noted that while most countries are cautious about getting caught cyber spying, "It's only the Chinese that think there are no consequences to getting caught."[42] The hack is being investigated by the FBI, but no details have been released and no charges have been filed.

The Great Cannon

A months-long attack in early 2015 against two U.S.-based websites, GreatFire.org and GitHub †—which provide methods to allow Chinese citizens to circumvent government-imposed, network-level censorship—was attributed in May to the Chinese government by the University of Toronto's Citizen Lab.[43] Nicknamed "the Great Cannon," the Chinese cyber weapon provides the government the

*The *Washington Post*, quoting unnamed Administration officials, reported on October 9 that the Chinese government had "quietly arrested a handful of hackers at the urging of the U.S. government—an unprecedented step to defuse tensions with Washington at a time when the Obama Administration has threatened economic sanctions." Those arrested were not named nor were their particular offenses revealed. According to the *Washington Post*, the action was taken by Chinese authorities in advance of President Xi's visit to Washington in response to an Administration list of hackers "identified by U.S. officials as having stolen commercial secrets from U.S. firms to be sold or passed along to Chinese state-owned companies." Ellen Nakashima and Adam Goldman, "In a First, Chinese Hackers are Arrested at the Behest of the U.S. Government," *Washington Post*, October 9, 2015.

†GitHub is a U.S. website for developers that hosts content forbidden in China and GreatFire.org, is an organization that monitors Internet censorship in China.

means to harness Internet traffic and redirect it to flood websites it considers dangerous, even those overseas. If the attack is successful, the offending websites are overloaded and cease functioning due to the DDoS attack. Before fielding the Great Cannon, the Chinese government simply attempted to filter out content from foreign and domestic media, or tried to block the websites entirely. That technique did not always work, particularly if Chinese citizens were using a virtual private network to access forbidden websites. Instead of blocking traffic entering China, the Great Cannon can be used to sabotage a website hosting material forbidden by Chinese censors, or to "aggressively go after sites outside China's borders deemed objectionable by Beijing."[44] The new Chinese cyber weapon was used to seize foreign web traffic headed to China's most popular search engine, Baidu, and redirect it to flood GitHub and GreatFire.org.[45]

Mysterious Eagle Preys on U.S. Businesses for a Decade

In mid-April 2015, the U.S. computer security firm FireEye identified a hacking group apparently backed by the Chinese government that has been stealing information for a decade about "journalists, dissidents, and political developments in relation to China, targeting government and military organizations and targeting economic sectors of interest to China's economy."[46] The group has been using malware that has been able to cross the "air gap"* and infect standalone computer networks not connected to the Internet. The malware's name, translated from Chinese, is "Mysterious Eagle."[47] FireEye called this hacker group "APT30," one of 20 such groups probably controlled by the Chinese government. "Such a sustained, planned development effort coupled with the group's regional targets and mission, leads us to believe that this activity is state sponsored, most likely by the Chinese government," the FireEye report said. APT30 also targeted at least 15 companies in communications, news media, technology, finance, and aviation.[48] The Chinese hackers gained access to these companies through spear phishing attacks: e-mails that appear legitimate from senders known to the recipient, but which contain malware inserted by the hackers. In the Mysterious Eagle case, network administrators were tricked into downloading malware on their home computers; when the network administrators transferred data from their home computers via thumb drives to the company network, they inadvertently introduced the malware from their home machines to the network.[49]

OPM Hack Affects More Than 22 Million Americans

On April 4, OPM revealed the first details of what turned out to be one of the largest data breaches of any U.S. network—an attack in which hackers gained access to the personally identifiable information of more than 22 million people, as well as millions of sensitive and classified documents.[50] Though the U.S. government has

*Air gap refers to a computer network with no connection to the Internet through which a hacker might gain access. In some cases, access to the air-gapped network is gained through the use of thumb drives to infect a network through USB ports that may transfer the virus from an infected thumb drive to an air gapped computer.

not officially attributed the attack to China, it is the "leading suspect," according to national intelligence director Clapper, who characterized the intrusions of the OPM computer network as government-to-government espionage.[51] Given the scope and difficulty of detecting the intrusion, said the former general, "you have to kind of salute the Chinese for what they did."[52] Hackers will continue to try to steal information from the government and from U.S. companies "until such time as we can create both the substance and the psychology of deterrence," he warned. Meanwhile, Director General Clapper said, because of an unresolved internal debate within the Administration on whether to retaliate, Washington must focus "a lot more attention to defense."[53] In addition, he continued, "That's frankly been a struggle for us, because of unintended consequences and other related policy issues."

The information taken from the OPM computer network included lengthy forms, dating back to 2000, completed by federal employees and contractors as part of the process to obtain and maintain security clearances. The records include such personal identifiers as fingerprints, Social Security numbers, birthdates, and financial records, as well as such sensitive information as admissions of past drug abuse, arrests, and mental health treatment, foreign travel, interviews of colleagues and neighbors, and reports by security clearance investigators, and the names of relatives and foreign contacts for millions of current and former federal employees. "The impact on national security is staggering," said Dmitri Alperovitch, founder of CrowdStrike Inc., a cybersecurity company in Arlington, Virginia.[54] Said FBI Director Comey: "It is a very big deal from a national security perspective and from a counterintelligence perspective. . . . It's a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government."[55] Among the "treasures" are 5.6 million fingerprints that could be used to identify undercover government agents or to fashion duplicates to biometric data to obtain access to classified areas.*[56]

According to the *New York Times*, the inspector general at OPM had warned in November 2014 that computer security at the agency was inadequate: OPM had not inventoried the computer servers and devices with access to its networks, did not require anyone gaining access to information from the outside to use the kind of basic authentication techniques most Americans use for online banking, and did not regularly scan for vulnerabilities in the system.[57] The inspector general found that 11 of the 47 computer systems that were supposed to be certified as safe for use were not "operating with a valid authorization."[58] Although OPM claims to have employed the most up-to-date intrusion detection software programs, including the Einstein 3 system and the Continuous Diagnostics and Mitigation program, those systems apparently failed. Even more important, none of OPM's data were encrypted, and the malware detection system did not detect the intrusions for four months.[59]

---

*The *Washington Post* reported that unnamed officials told the newspaper that the CIA "pulled a number of officers from the U.S. Embassy in Beijing as a precautionary measure in the wake" of the OPM breach. Ellen Nakashima and Adam Goldman, "CIA Pulled Officers from Beijing after Breach of Federal Personnel Records," *Washington Post*, September 29, 2015.

Under current law, the Federal Information Security Modernization Act of 2014, federal agencies are responsible for their own security. No agency officially responsible for national cybersecurity, such as the Department of Homeland Security, is actually responsible for enforcing any standards on any other Federal Government agency.[60] Thus, no one is responsible for enforcing standards across the Federal Government.

Despite the numerous press accounts quoting named and unnamed Administration officials blaming China for the intrusion, including Director of National Intelligence Clapper and former NSA and Central Intelligence Agency Director Michael Hayden, the Administration has not officially attributed the action to China.*

Chinese Hackers Breach Major Engineering Universities

Hackers apparently based in China gained access to and stole information from Penn State University's engineering school for more than two years, the school disclosed on May 16 after a report by federal and private investigators.[61] The data breach included information about the school's 500 research partners, including government agencies, companies, and other schools. Penn State specializes in aerospace engineering, and has a significant research partnership with the U.S. Department of Defense.[62] The California-based network security company FireEye said forensic analysis showed that Chinese hackers were among at least one of two separate groups that stole data from the college, based on an examination of the malware and other tools used to breach the network. Other U.S. engineering schools targeted by Chinese hackers are Johns Hopkins University, Carnegie Mellon University, the University of California-Berkeley, and the Massachusetts Institute of Technology.[63]

Chinese Hackers Breach United Airlines and Anthem for Customer Data

The group responsible for the OPM intrusion also exfiltrated data on passengers flying on United Airlines aircraft and on enrollees in California's largest health care insurer, Anthem Blue Cross Blue Shield, according to numerous news reports.[64] United, the world's second-largest airline, is often used by U.S. government employees, who are required to fly on U.S. carriers whenever possible. In the hack, United likely lost records that contained the names of passengers, their flights, destinations, passport numbers, and expiration dates, dates of birth, frequent flyer numbers, and home addresses. The data can be cross-referenced with other data taken from OPM to track the movement of federal workers, including those in the 17 different intelligence agencies whose workers are also required to fly on U.S.-flagged carriers. The Anthem breach exposed Social Security numbers and sensitive details about the health of 80 million customers, marking the attack as one of the biggest thefts of medical-related customer data in U.S. history.[65]

---

*Director Hayden said the OPM data was "a legitimate foreign intelligence target" and that "this is not shame on China; this is shame on us for not protecting that kind of information. . . . This is a tremendously big deal. And my deepest emotion is embarrassment." *Wall Street Journal*, "Michael Hayden Says U.S. Is Easy Prey for Hackers," June 21, 2015.

Cybersecurity firm CrowdStrike has attributed the Anthem breach to a Chinese hacker group nicknamed "Deep Panda," and has been following the group's efforts, including a data theft from RSA, another cybersecurity firm.[66]

Remedies and Retaliation for Cyber Attacks from China

Executive Order to Impose Sanctions

On April 1, 2015, President Obama issued an executive order following the attacks on the U.S. affiliate of Sony, Inc. by North Korea, China's ally. The President declared a national emergency due to the "increasing prevalence and severity of malicious cyber-enabled activities" from abroad, constituting "an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[67] Under the order, a wide variety of cyber activities could result in sanctions, including "malicious cyber-enabled activity" that leads to theft of or harm to

> *critical infrastructure, misappropriating funds or economic resources, trade secrets, personal identifiers or financial information for commercial or competitive advantage or private financial gain; knowingly receiving or using trade secrets that were stolen by cyber enabled means for commercial or competitive advantage or private financial gain; disrupting the availability of computer or network of computers (for example through a DDoS attack) and attempting, assisting, or providing a material support for any of the above activities*.[68]

The President's executive order also followed Congress' inaction on an Administration-supported bill to establish standards for privately owned critical infrastructure, such as telecommunications, electricity, and financial services. Following objections from the business community that even voluntary standards might become mandatory, the bill was defeated. A 2013 executive order establishing the Cybersecurity Framework to encourage adoption of cybersecurity standards is entirely voluntary.[69] Legislation on threat data sharing is pending in Congress.

Following revelations of the breach on the OPM computer network in mid-April, the Administration did not announce any sanctions under the April 1 executive order. The wording of the executive order appears to support the argument that it covers commercial cyber espionage. The order specifies that it is intended to punish those responsible or "complicit" in "malicious cyber-enabled activities that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, economic health or financial stability of the United States."[70] It also lists the theft of "personal identifiers" as being among the "malicious cyber-enabled activities" covered by the executive order. The standard of evidence for naming any malefactor is low—"a reasonable basis to believe or a reasonable cause to believe." Taken together, this wording appears to include the theft of personal identifiers in the OPM hack as a "malicious cyber-enabled activity" covered by the executive order.[71]

The White House refrained from interpreting whether the executive order would cover commercial espionage but left little doubt

that sanctions were being considered. Deputy National Security Adviser Ben Rhodes told reporters September 22 in advance of President Xi's visit to Washington that, "While our preference is resolving this through dialogue, we're not averse to punitive measures, including sanctions, if we feel like there are actors in China and entities that are engaged in activities that are sanctionable." [72] President Obama, in a speech to the Business Roundtable before President Xi's visit noted, "We are preparing a number of measures that will indicate to the Chinese that this is not just a matter of us being mildly upset, but is something that will put significant strains on the bilateral relationship if not resolved, and that we are prepared to [take] some countervailing actions in order to get their attention." [73]

One hurdle to explicitly blaming China, however, may be the reluctance of the Administration to detail the sources and methods used to identify the Chinese government as the originator or the sponsor of the hack. In a briefing describing the circumstances for invoking the sanctions under the executive order, White House Cyber Coordinator Michael Daniel noted that "we will consider whether we have the evidence in a form that we are willing to disclose publicly." [74]

Weighing Defensive and Offensive Countermeasures

As the evidence has increased that nation states are involved in cyber attacks and espionage, the principal response has remained defensive: principally shoring up systems to detect network intrusions and malware. A more offensive strategy has slowly evolved, however, even as its details remain largely classified. The U.S. Department of Defense in 2011 published a doctrine equating the most damaging cyber attacks—those directed against public infrastructure—with an act of war, and theoretically allowing equivalent retaliation.[75] "When warranted, we will respond to hostile attacks in cyberspace as we would to any other threat to our country," the Pentagon said in the report to Congress. "We reserve the right to use all necessary means—diplomatic, informational, military, and economic—to defend our nation, our allies, our partners and our interests." In 2012, then Defense Secretary Leon Panetta made the doctrine more explicit, noting that a cyber attack on the United States resulting in large-scale property destruction and loss of life—a "cyber Pearl Harbor"—could be considered an act of war and could justify proportionate cyber retaliation.[76] Defense Secretary Ashton Carter updated the strategy in 2015 "to fit the age of probe, thievery, and assault over computer networks." [77] At the core of the strategy is a hierarchy of cyber attacks: Fending off routine commercial attacks remains the responsibility of targeted companies. The Department of Homeland Security is responsible for detecting more complex attacks and helping the private sector defend against them. The most damaging attacks would be handled by the military's Cyber Command, which is based at the NSA headquarters in Maryland. "As a matter of principle, the United States will seek to exhaust all network defense and law enforcement options to mitigate any potential cyber risk to the U.S. homeland or U.S. interests before conducting a cyberspace operation," the strategy says.[78]

At a speech at Stanford University unveiling the new doctrine, Secretary Carter defined a major cyber attack as "something that threatens significant loss of life, destruction of property, or lasting economic damage."[79] The new doctrine also lays out the case for the threat of cyber retaliation to deter attacks, much as the threat of nuclear deterrence kept the missiles from flying during the Cold War:

> *Deterrence is partially a function of perception. It works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed. The United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the overall resilience of U.S. systems to withstand a potential attack if it penetrates the United States' defenses*.[80]

But as Secretary Carter acknowledged, such a policy is easier to declare than to implement. The overall head of NSA's Cyber Command, Admiral Michael S. Rogers, has often noted that the price of conducting cyber attacks is still far too low for many countries to resist computer network attacks.[81] Secretary Carter and NSA Director Rogers have said that the United States should develop a plan to signal hackers about the consequences of their actions.[82]

One recent proposal from the Council for Foreign Relations criticizes the Administration for tolerating "incessant cyber-attacks by China on the U.S. government, critical infrastructure, and businesses."[83] The paper says that "virtually nothing has been done to stop this cyber assault," and that U.S. "passivity" must end, "especially since there is no way to reach a verifiable cyber-security agreement with China."[84] The authors believe current U.S. strategy to confront Chinese government commercial espionage lacks the following: (1) the imposition of costs on China that are in excess of the benefits it receives from its violations in cyberspace; (2) increased U.S. offensive cyber capabilities to dissuade China's leaders from using cyber attacks against the United States and its partners in the region; (3) continued improvement in U.S. cyber defenses, including a law regulating information sharing between intelligence agencies and the corporate world; and (4) legislation, such as the Cyber Information Security Protection Act, allowing businesses to rapidly share intelligence on cyber threats with each other and the government without fear of lawsuits.[85]

In its June hearing, the Commission considered testimony on the idea of government-directed offensive operations against other nation states as a form of retaliation and deterrence. The Commission also considered the possibility of U.S. corporations mounting retaliatory cyber strikes against Chinese companies or seeking damages against companies that either mounted attacks or benefited from information stolen by government or private hackers.

Given that the Internet is a relatively new phenomenon and that war is rooted in ancient history, it is not surprising that internationally recognized laws of war embodied in the Geneva Conven-

tions and elsewhere have not kept up.[86] The authors of an authoritative law review article note that

> *the law of war provides a useful legal framework for only the very small slice of cyber attacks that amount to an armed attack or that take place in the context of an ongoing armed conflict. . . . Other existing legal frameworks—both domestic and international—offer equally fragmentary assistance in addressing cyber attacks through law. Examining existing law leads to a clear conclusion: A new, comprehensive legal framework is needed to address cyber attacks. That framework includes a more robust system of domestic enforcement but a truly effective solution to this global challenge will require global cooperation.*[87]

Mr. Poindexter cautioned that a counterattack could escalate beyond the theft of data to "real destructive mechanisms."[88] Mr. Tiao warned that the many U.S. economic ties with China would make cyber retaliation difficult: "In order to take action against a nation state like China where we have a complex economic and security relationship, it's a little more complicated than taking sort of a quick strike action against, say, the North Koreans with which we don't have a similarly complicated relationship."[89] Mr. Tiao, however, suggested an indictment of individual hackers could form the legal basis for a trade retaliation case or economic sanctions. And, the creation of a Foreign Intelligence Cyber Court could also provide the legal basis for further action. However, noted Mr. Tiao, U.S. companies cannot retaliate or "hack back" without violating current U.S. law* prohibiting computer hacking.

When the Commission on the Theft of American Intellectual Property (IP Commission) examined the issue in 2013, it noted that current U.S. law does not permit corporations that have been hacked to use an an active defense. An "active network defense . . . allows companies not only to stabilize a situation but to take further steps, including actively retrieving stolen information, altering it within the intruder's networks, or even destroying the information within an unauthorized network [and] . . . photographing the hacker using his own system's camera, implanting malware in the hacker's network, or even physically disabling or destroying the hacker's own computer or network."[90] Among the reasons the IP Commission cited for not allowing an active defense are the potential for collateral damage to the Internet and the possibility of doing damage to an innocent third party. The IP Commission recommended further study of the issue while acknowledging that "entirely defensive measures are likely to continue to become increasingly expensive and decreasingly effective, while being unlikely to change the cost benefit calculus of hackers away from attacking corporate networks."[91]

Asked at the June Commission hearing to comment on one suggestion that U.S. intelligence agencies could aid U.S.-based companies whose IP or competitive bids had been stolen by a Chinese company, Mr. Poindexter responded: "We have a lot of restrictions on what the Intelligence Community is allowed to supply a busi-

* 18 U.S.C. § 1030 criminal law, "Fraud and Related Activity in Connection with Computers."

ness, and the Intelligence Community doesn't want to supply that because they know what the problems are going to be. . . . Who do you support? Do you support BAE, a big British company? They are in the United States. They get hacked. What do we do then? Do we do the same kind of work?"

Mr. Tiao suggested that a Section 337 trade act case identifying the stolen IP might be easier to pursue in court rather than an ordinary tort case that would require proof of monetary damages from the theft of IP—far beyond what a U.S. cyber intelligence agency might be able to provide.* Doing so, however, would likely require a publicly traded U.S. company to file an 8–K report with the U.S. Securities and Exchange Commission (SEC). (The report's purpose would be to notify shareholders of a situation that could have a "material" effect on the earnings of a company and, therefore, its share price.) The SEC has not issued guidance specifically on what circumstances would trigger the disclosure requirement in the case of theft of IP through a computer network intrusion. U.S. companies have strongly opposed any requirement that they disclose to the public or to the SEC the intrusions on their computer network.[92] According to the Office of the National Counterintelligence Executive, "no legal requirement to report a loss of sensitive information or a remote computer intrusion exists, and announcing a security breach of this kind could tarnish a company's reputation and endanger its relationships with investors, bankers, suppliers, customers, and other stakeholders."[93]

In the absence of criminal prosecution, U.S. companies may be able to pursue a civil action against a hacker for the theft of IP. In the case of a cyber attack or intrusion from abroad, the civil case might require evidence obtained by a U.S. intelligence agency in order to be successful.† While that has not become commonplace, Mr. Tiao noted that since a 2013 executive order,‡ U.S. intelligence agencies made it "a major priority for the government to push information that the intelligence community was collecting and the law enforcement agencies were collecting in a timely fashion out to companies that had been identified as victims."[94]

Recent Attempts to Negotiate a Solution to Chinese Cyber Espionage

The visit of President Xi to the United States in late September provided an opportunity to raise directly Washington's objections to Chinese commercial cyber espionage, intrusions into U.S. government computer networks, and the imposition of regulations and standards in China meant to disadvantage foreign-based providers

---

*Section 337 of the Tariff Act of 1930, 19 U.S.C. §1337, allows the seizure by customs authorities of imports that contain stolen IP.

†One possible remedy is Section 337 of the Tariff Act of 1930, 19 U.S.C. §1337, which allows the seizure by customs authorities of imports that contain stolen IP.

‡Executive Office of the President, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013. The National Institute for Standards and Technology was ordered to work with the private sector to develop guidelines on information sharing, privacy, and the adoption of cybersecurity practices. Similar legislation was considered by Congress but did not pass, due in part to opposition from the business community based on fears that voluntary guidelines would eventually become mandatory. The National Institute for Standards and Technology subsequently released a framework agreement in February 2014. The program remains entirely voluntary. Congress is considering new legislation, the Cybersecurity Information Sharing Act, which has been endorsed by the U.S. Chamber of Commerce.

of Internet services. The actual negotiations preceded the official state visit.

The Administration revealed in early September that it had conducted a series of talks in Washington with a Chinese delegation headed by Meng Jianzhu, secretary of the CCP's Central Political and Legal Affairs Commission. He met with a number of high-ranking officials, including National Security Adviser Susan Rice, FBI Director James Comey, Department of Homeland Security Secretary Jeh Johnson, and Secretary of State John Kerry.[95] Mr. Meng said that China "resolutely opposes cyber attacks and cyber espionage" and promised that "whoever carries out cyber attacks and cyber espionage in China violates the national law and will be held accountable by law."[96]

President Xi began his trip to the United States with a stop in Seattle, where he met with executives of some of the top U.S. technology companies, such as Microsoft—the host of the event—Apple, IBM, Facebook, Google, and Cisco Systems. President Xi repeated stock denials that the Chinese government conducts or sponsors or tolerates commercial cyber espionage or attacks on U.S. government agencies. "Both commercial cyber theft and hacking against government networks are crimes that must be punished in accordance with the law or relevant international treaties," President Xi told the conference group.[97] "The Chinese government will not in whatever form engage in commercial theft," he added.[98] After Presidents Xi and Obama met in Washington, DC, the White House distributed a fact sheet stating that the two leaders had agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[99] The two leaders also agreed to establish a "high-level joint dialogue mechanism on fighting cybercrime and related issues" that will meet twice a year. A previous dialogue at a lower level was suspended by the Chinese government to protest the indictment in May 2014 of five PLA officers for cyber espionage.

The form of the announcement—a fact sheet released solely by the White House—along with the lack of any signed document and a lack of precision on the meaning of "cyber theft," "cyber attack," "cyber espionage," "economic espionage," "economic cyber spying," and "cyber-enabled theft of intellectual property," led some to question the level of commitment by both sides.[100] As President Obama said at the joint press conference September 25: "What I've said to President Xi and what I say to the American people is the question now is, are words followed by actions? And we will be watching carefully to make an assessment as to whether progress has been made in this area."[101] The White House fact sheet explained, in part:

> *Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate.*

The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.[102]

This agreement appears to create a much narrower definition of cyber misbehavior than is encompassed by President Obama's April 1 executive order. That executive order appears to cover the theft of personally identifiable information, such as the Office of Personnel Management theft of the personal details of 22.1 million federal employees, applicants, and contractors.

Regulatory Barriers to Digital Trade in China, and Costs to U.S. Firms

Censorship

China's authoritarian government maintains tight control over the flow of information across and within its borders with a system termed the "Great Firewall."[103] As part of this effort to control dissent by restricting speech, news, and social media, the Chinese government has implemented a policy of replacing foreign IT and Internet providers with Chinese companies. This not only affects human rights in China and skews the thinking of Chinese citizens about the United States and their own country, it also has a profound impact on a large segment of the U.S. economy. At the Commission's June hearing, Mr. Poindexter said that China's government is "not content to manage only their own content; they want to manage ours. . . . China controls the distribution of ideas, modifies them to suit its own needs, removes them, or allows access to them and monitors who has them."[104]

The U.S. economy has much at stake. The United States has the most advanced IT and software industry in the world and accounts for 55 percent of global expenditures on research and development, according to a study by the U.S. Department of Commerce.[105] U.S. firms in digitally intensive industries sold $935.2 billion in products and services online in 2012 (latest data available), including $222.9 billion in exports—about a quarter of the total sales, according to a 2014 study by the U.S. International Trade Commission.[106] That makes the IT and software sector one of the most export-dependent industries in the United States. The U.S. International Trade Commission estimates removing existing foreign barriers to U.S. digital trade would increase the U.S. real gross domestic product (GDP) by an estimated $16.7 billion to $41.4 billion.[107] Since China is the second largest trading partner of the United States, and its other major trading partners—Canada, Japan, and Europe—do not discriminate against U.S. digital products, China's adverse policies are the single-largest drag on U.S. exports of digital services.

The Chinese government heavily regulates, monitors, and controls online content, and requires all market participants in China to comply with vague guidelines and regulations through self-censorship. In cases where foreign sites and services have refused to comply with China's censorship policies, Chinese authorities have

blocked online access to them. Examples include the *New York Times*, Bloomberg News, the *Guardian*, Facebook, Picasa, Twitter, Tumblr, Google, Foursquare, Hulu, YouTube, Flickr, Dropbox, and LinkedIn.[108] China's censors can block any search result; in the past, sensitive subjects (including Tibet, Tiananmen Square, the names of dissidents, and the wealth of the families of China's top leaders) and coverage of news events (such as the capsized ferry boat in the Yangtze River near Shanghai and the slow government response to the 2008 Sichuan earthquake) have been or remain blocked. Three organizations that monitor freedom of expression—the Open Network Initiative, Freedom House, and Reporters Without Borders—found China to be a "pervasive" censor.[109]

The Great Firewall directly limits the participation of U.S. information and communication technology (ICT) companies in China's market in a variety of ways:

- Censoring the information available on foreign-based websites or requiring Internet-based companies to self-censor to access the market;
- Using the Great Firewall to slow down or degrade or redirect some foreign web-based services rather than block them outright;
- Blocking access to key words and web page advertising domains;
- Requiring Internet search engines to remove results; and
- Issuing technology mandates that hobble user privacy and security.[110]

In his testimony at the Commission's June hearing, Matthew Schruers, vice president for law and policy at the Computer and Communications Industry Association, noted that orders by Chinese authorities to filter and block information online are "unpublished and unappealable through state control or influence over the communications infrastructure."[111] Mr. Schruers continued, "Some have explained the elaborate Chinese censorship system as being geared towards maximizing the economic benefits of the Internet while maintaining strict social control; whatever the domestic aim of these mechanisms may be, they function, intentionally or not, as unlawful barriers to international trade."[112]

Some cases of discrimination against U.S. firms have been more blatant. Chinese authorities have redirected traffic sent to U.S.-based search engines to Baidu—the China-based competitor to Google, Yahoo, and Microsoft search engines—presumably, in part, because Baidu does not respond to searches for banned terms such as Tiananmen Square massacre, Tibet, Nobel Peace Prize winner Liu Xiaobo, or the artist Ai Weiwei.[113] Stepped-up censorship efforts in recent months include a crackdown on virtual private networks, which are often used by companies and individuals to access secure data and blocked websites. More than 80 percent of U.S. companies surveyed by the American Chamber of Commerce in China in 2015 reported being limited by the censorship of Internet

content and websites when conducting business.* Other reported censorship methods include blocking sites by Internet protocol addresses, and blocking and filtering uniform research locators (URLs) and search engine results.

These nontariff market barriers may violate China's World Trade Organization (WTO) commitments to treat foreign and domestic businesses equally. While the WTO has not been asked to rule on the issue, one theory holds that China in particular could be vulnerable to such a charge, based on its relatively sophisticated censorship capabilities. Although countries might successfully claim to impose censorship on moral or religious grounds, "there is a good chance that a panel might rule that permanent blocks [by China] on search engines, photo-sharing applications, and other services are inconsistent with the GATS [General Agreement on Trade in Services]† provisions, even given morals and security exceptions; less resourceful countries, without means of filtering more selectively, and with a censorship based on moral and religious rounds, might be able to defend such bans in the WTO."[114] GATS also stipulates that a system of judicial or administrative review be available to WTO members—a process that is not available in China.[115] By contrast, Chinese Internet firms enjoy a fast-growing and walled-off market on the Mainland while they have unrestricted market access to the United States, including the ability to access U.S. capital markets to fund expansion at home and abroad.[116] To date, the United States has not brought any WTO cases against China on its nontariff barriers against foreign information and communication technology companies.

Regulations and Standards as a Barrier to Trade

The Chinese government is in the process of passing and implementing comprehensive new laws and regulations that affect the use of information and software technology and the Internet and have the potential to limit or exclude U.S. technology companies from key tech-intensive sectors of the Chinese market. Existing regulations combined with new and stricter proposals would impose localization requirements, market access limits, data privacy and protection requirements, IP rights infringement, and uncertain legal liability rules. Among the digitally intensive industries affected are: newspapers, periodicals, books, directories and mailing lists, motion pictures, sound recordings, video and music production and distribution, broadcasting, news syndicates, banking and insurance, credit card transactions, online retail trade, and wholesale trade in business-to-business transactions.[117] As part of the effort, the Chinese government asked U.S. technology companies over the summer to sign a pledge that they would, among other commitments, store Chinese user data within the country and provide the government access to its networks and, according to some interpretations, encryption keys and source code.[118]

According to testimony from Samm Sacks, a technology analyst at the Eurasia Group in Washington, U.S. technology companies

*The figure in 2013 was 55 percent. American Chamber of Commerce in China, "China Business Climate Survey Report," May 2015, 30.

†GATS is an international trade agreement within the WTO.

may be required by China's central government to "undergo invasive audits, turn over source code, and provide encryption keys for surveillance." [119] The key legislation and policy directives that have been proposed or are under consideration include:

- A purge of foreign firms from government-sanctioned procurement lists;
- Restrictions on foreign equipment in the banking sector requiring suppliers to meet "secure and controllable" standards;
- A draft counterterrorism law compelling telecom and Internet companies to provide encryption keys to enable government surveillance on stored data on local Chinese servers;
- A new national security law that will expand Beijing's regulatory powers under a broad and far-reaching definition of national security and calls for sovereignty in cyberspace;
- Creation of a cyberspace review body to evaluate security for all Internet and IT products;
- A new cybersecurity law or framework; and
- A 13th Five-Year Plan for software and "big data" focused on boosting data security for SOEs, financial institutions, and government agencies.[120]

National Security Law

The central government's Standing Committee approved a new National Security Law on July 1 that expands the nation's authoritative rule over a far greater list of "core interests," including control over the press, social media, and the entire Internet in China, which must be made "secure and controllable." [121] Zheng Shuna, a National People's Congress official, explained at the unveiling of the new National Security Law in Beijing that "Internet space within the territories of the People's Republic of China is subject to the country's sovereignty." [122] He added that "the country must defend its sovereignty, security, and development interests. It must also maintain political and social stability. . . . Any government will stand firm and will not leave any room for disputes, compromises, and interference when it comes to protecting core interests. China is no exception." [123] (For more information, see Chapter 1, Section 2, "Foreign Investment Climate in China.")

Cybersecurity Law

A week after the new national security law received approval, China's central government proposed a cybersecurity law that would likely put the Cyberspace Administration of China and the Ministry of Industry and Information Technology in charge of "comprehensively planning and coordinating network security efforts and related supervision and management efforts." [124] The law is intended to "ensure network security, to preserve cyberspace sovereignty, national security and societal public interest, to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the healthy development of economic and social information," according to the draft.[125] Among the 67 ar-

ticles in the draft are several declaring that network providers are responsible for the material on their websites, which must not contain "state secrets"—a term with a constantly shifting meaning that can include information the government has already made public. Network providers must also ensure that those using their service are identifiable to the government. "Critical information infrastructure operators" are required to exclusively store data on servers within China.[126] Foreign companies seeking to obtain Internet service provider licenses in China must partner with a domestic company that holds a license.[127]

Foreign Investment Control

China's insistence on applying the principle of sovereignty to the Internet, which respects no borders, "suggests that the Chinese government is pursuing a policy strategy that could eventually over the long term lead to fragmentation of the U.S.-led global Internet," Ms. Sacks told the Commission.[128] The concept also is likely to provide the legal basis for an expanded protocol for national security reviews of inbound foreign investment, which is also in the draft of a new foreign investment law. The policy, warned Ms. Sacks, could justify restricting inbound foreign investment on the basis of "strategic, economic, social, ideological, and technical readings of national security."[129] (For more information, see Chapter 1, Section 2, "Foreign Investment Climate in China.")

Banking Regulations

The China Banking Regulatory Commission also decreed last September that financial institutions in China must increasingly use "secure and controllable" ICT products and services in order to "meet banking information security requirements."[130] The goal, according to the China Banking Regulatory Commission, is for 75 percent of ICT products in Chinese banking institutions to be considered "secure and controllable" by 2019. Less than 15 percent of banks operating in China meet the criteria.[131] The new rules accompany China's efforts to reduce its reliance on U.S. technology, a plan that "picked up steam after former U.S. National Security Agency contractor Edward Snowden alleged in 2013 that the U.S. government used some of the country's technology firms to spy on foreign governments," according to some news accounts.[132]

While "secure and controllable" is not defined in the national security, cybersecurity, or banking laws, business groups have interpreted it as an excuse to favor Chinese software, hardware, and services over foreign competing products.[133] A January 28 letter signed by 18 U.S. business groups addressed to the CCP Central Leading Group for Cyberspace Affairs warned that under the banking regulation, ICT products and services would be required to "undergo intrusive security testing, contain indigenous Chinese intellectual property (IP), implement local encryption algorithms, comply with country-specific (Chinese) security standards, disclose source code and other sensitive and proprietary information to the Chinese government, and engineer their products so as to restrict the flow of cross-border data."[134] In the letter, the U.S. business groups suggested these policies would effectively exclude sales of

U.S. hardware, software, and services to Chinese banks, and would violate China's WTO commitments to refrain from technical barriers to trade and to not discriminate against imports.[135] In addition, disclosing source code could provide government hackers access to private computer networks.

Subsequent letters signed by U.S. ICT business associations and Republican House leaders urged the Chinese leadership to postpone implementation pending further dialogue. In response to unnamed "financial institutions and related parties," the China Banking Regulator Commission instructed Chinese banks on April 13 to temporarily "suspend implementation" of the rules, which are expected to be revised and reissued after integrating suggestions from relevant domestic parties.[136] However, Ms. Sacks told the Commission at its June hearing that the banking law "remains in play" and is unlikely to be altered in any substantial way.[137] Indeed, in August, the China Banking Regulatory Commission summoned to a meeting several Western technology companies, including IBM, Microsoft, and Cisco Systems Inc., and told them the banking regulations were being revived, jeopardizing hundreds of millions of dollars in revenue for foreign tech companies selling a wide range of products from servers to cloud computing software.[138] In addition to revelations of NSA cyberspying, Chinese officials cited as justification for the impending restrictions on foreign technology the opposition in Congress to purchases by U.S. telecommunications companies of equipment manufactured by the Chinese IT companies Huawei and ZTE.[139]

Counterterrorism Law

China's draft counterterrorism law presents another obstacle for foreign ICT firms. Expected to go into effect in the coming months, the law would require ICT firms to submit encryption keys to the Chinese government and to install security back doors to allow access to government officials. The initial draft of the law requires companies to keep servers and user data within China (localization), provide communications records to law enforcement authorities, and censor terrorism-related Internet content.[140]

According to President Obama, the counterterrorism provisions "would essentially force all foreign companies, including U.S. companies, to turn over to the Chinese government mechanisms where they can snoop and keep track of all the users of those services. . . . [T]hey are going to have to change [the ICT policy] if they are to do business with the United States." [141]

In response to this criticism, National People's Congress spokeswoman Fu Ying said the ICT proposals in China's draft counterterrorism law were "in accordance with the principles of China's administrative law as well as international common practices, and won't affect Internet firms' reasonable interests." [142] She pointed to Edward Snowden's allegations that operatives of the NSA and its British equivalent, the Government Communications Headquarters, hacked into the internal computer network of the Dutch multinational firm Gemalto, the largest manufacturer of subscriber identity module (SIM) cards in the world, stealing encryption keys that can be used to monitor mobile communications.[143]

Less obvious but of equal importance to the new regulations is the reorganization of China's Internet regulatory authority, Ms. Sacks told the Commission at the June hearing. President Xi Jinping has assumed the top post at the Central Leading Small Group for Network Security and Informationization. The agency was created in February 2014 to consolidate the leadership's role, which had been fragmented. Of the 22 members of the group, according to Ms. Sacks, half hold the most senior rank among Party, military, and government officials. In the top-down Chinese government where the Party occupies the pinnacle, this agency is expected to be the last word on policy and implementation.[144]

Import Substitution Policies

To boost its homegrown technology sector and address its cybersecurity concerns, China is shifting from foreign to domestic technology suppliers in sensitive segments of the economy by 2020, including banking, military, SOEs, and key government agencies.[145] House Republican leaders say that if these new ICT policies are fully implemented, they will "negatively impact other sectors, such as banking, manufacturing, and health care, and harm the U.S. economy and jobs due to falling sales, outright theft of business secrets, and companies simply leaving the market." [146]

The Chinese government has started to implement these policies. The number of foreign technology brands on China's list of ICT products approved for government purchase fell by one-third, while more than half of foreign suppliers of security-related products were dropped from the approval list.[147] For example, the number of government-approved products made by U.S. network equipment maker Cisco Systems Inc. fell from 60 in 2012 to zero in 2014.[148] In some cases, U.S. companies that lose business operating licenses or government procurement approval will be forced to partner with a Chinese firm to preserve at least some business for their Chinese affiliate company.

Internet Plus

Ms. Sacks also noted two related policies implemented by President Xi—the Made in China 2025 initiative and the Internet Plus plan—as the main channels to promote local high-value-added technology sectors as the economy slows.[149] (See Chapter 1, Section 3, "China's State-Led Market Reform and Competitiveness Agenda," for discussion of the Made in China 2025 plan.) The Internet Plus plan seeks to capitalize on China's huge online consumer market by building up the country's domestic mobile Internet, cloud computing, big data, and the "Internet of Things," * and to create global competitors by assisting domestic firms' expansion abroad.[150] China's Internet Network Information Center reported there were 649 million Internet users and 557 million mobile device users in China as of December 2014, far outstripping the second-largest Internet user country, the United States.[151] McKinsey & Company, a global management and consulting firm, estimated

*The Internet of Things is the interconnectivity between physical objects such as a smartphone or electronic appliance via the Internet that allows these objects to share data. For more information, see Harald Bauer, Mark Patel, and Jan Veira, "The Internet of Things: Sizing Up the Opportunity," *McKinsey & Company*, December 2014.

that starting in 2013, e-commerce would contribute up to 22 percent of China's productivity growth by 2025 and fuel between 7 and 22 percent of the total GDP through 2025.[152] Furthermore, McKinsey estimated e-commerce could create 46 million new jobs between 2013 and 2025.[153]

U.S. technology firms seeking to enter the fast-growing Chinese market face increasing costs of doing business due to censorship-related restrictions, onerous regulations, and preferential support for domestic firms.[154] Because Google, Facebook, Twitter, and YouTube remain blocked in China due to their refusal to censor content, domestic copycats such as Baidu, RenRen, Weibo, and Youku have filled the gap.[155] (See Chapter 1, Section 2, "Foreign Investment Climate in China," for further discussion of China's investment climate for foreign firms.)

Implications for the United States

China's increasing use of cyber espionage directed against commercial targets in the United States and abroad has already cost U.S. companies tens of billions of dollars in lost sales and the expenses of repairing and remediating the damage. The largest and most sophisticated cyber attacks have been traced to government-sponsored or government-run teams of hackers in China. In many cases, the trade secrets and confidential information about bidding and business strategy have been turned over to Chinese government-owned competitors. This has led to the creation of global competitors to U.S. companies and industries, where none would otherwise exist. Some of those IP thefts have done harm to the national security and the economy of the United States, particularly because they have targeted large U.S. defense contractors such as Northrup Grumman and Lockheed Martin.

The United States has relied on a passive defense, and the U.S. government has failed to create an overall strategy to counter the increasingly sophisticated cyber attacks on some of our most valuable technology companies. Legislation to encourage U.S. companies to share information about cyber intrusions among each other and to voluntarily report theft of their information to the government has not been enacted into law. U.S. law has not kept up with the challenges posed by cyber attacks from government-sponsored hackers, nor does international law adequately address the issue. Although some policy discussions on offensive operations to counter cyber attacks have taken place, nothing has been decided. As a result of this inertia, the United States remains unable to thwart state-sponsored or state-supported cyber attacks.

The United States has the most advanced and globally integrated digital economy in the world.[156] Exports from its digitally intensive industries make up nearly a quarter of total industry sales.[157] Of the world's 35 digital "category kings," the United States claims half, including such names as Google, Facebook, Twitter, LinkedIn, YouTube, and Instagram. There are currently 83 U.S. based, venture-backed companies founded since 2000 that have reached a $1 billion valuation.[158] But that success is jeopardized by a concerted Chinese government effort to wall off the fastest-growing market in the world for digital commerce.

China is employing a combination of censorship, regulations, and support for homegrown companies over international competitors. Longstanding censorship has already forced major U.S. companies to limit their business dealings in China or to exit the country. Meanwhile, the Chinese government has been removing foreign software and hardware companies from its official procurement lists in an effort to shift buying to domestic information and communications technology companies. The result will be the continuing loss of market access for U.S. firms, declining revenue, and a reduction in jobs in the United States.

Conclusions

- China's government conducts and sponsors a massive cyber espionage operation aimed at stealing personally identifiable information and trade secrets from U.S. corporations and the U.S. government. Some of the stolen information is provided to Chinese state-owned businesses that compete with U.S. firms in China and abroad. Other recipients of U.S. trade secrets include sectors of the Chinese economy that the central government designated as Strategic Emerging Industries, which China intends to nurture into global competitors.
- The cost to the U.S. economy and to U.S. companies of government-sponsored cyber theft has been on the rise as network intrusions have become more sophisticated and harder to detect. The financial damage results from the loss of trade secrets such as copyrights and patents, manufacturing processes, foregone royalties, the costs of cyber defense, the loss of business and jobs, and the expense of remediating and repairing the damage to computer networks.
- U.S. cybersecurity companies and the Federal Government have become more adept at attributing computer network attacks to specific countries and to groups of hackers within those countries. Their willingness to release details on the culprits has also increased. U.S. companies have also become more willing to reveal details of the attacks on their computer networks.
- The U.S. reaction to the increasing number and sophistication of foreign cyber espionage and malicious network attacks has been mostly defensive. U.S. law does not allow retaliatory cyber attacks by private citizens and corporations, nor does it appear to allow counterintrusions (or "hack backs") for the purpose of recovering, erasing, or altering stolen data in offending computer networks. International law has not kept up with developments in cyber warfare, and no international consensus exists on how to attribute or appropriately respond to cyber attacks. However, a policy discussion on the issue of offensive and retaliatory cyber operations has begun.
- The Chinese government appears to believe that it has more to gain than to lose from its cyber espionage and attack campaign. So far, it has acquired valuable technology, trade secrets, and intelligence. The costs imposed have been minimal compared to the perceived benefit. The campaign is likely to continue and may well escalate as the Chinese Communist Party leadership con-

tinues to seek further advantage while testing the limits of any deterrent response.

- The Chinese government maintains strict censorship controls over the flow of information across and within its borders, and holds Internet providers, websites, search engines, and online news media responsible for censoring their content on the basis of vague guidelines and arbitrary rulings. The Chinese government's obsession with limiting citizen access to information harms U.S. companies attempting to compete in China. Some U.S. companies have faced retaliation, including the filtering or outright blocking of their websites, and all foreign companies risk loss of business licenses for violating the Chinese government's unpredictable sensitivities.
- The Chinese government is in the process of passing comprehensive new laws and regulations on cybersecurity that would affect trade in digital goods and services in a wide range of industries, including the news media, banking, credit card transactions, online retail trade, entertainment media, and telecommunications. Some of the new rules would have the effect of excluding U.S. companies from participating in the world's fastest-growing digital market by requiring, for example, that servers containing information about Chinese citizens and companies be located exclusively in China, and that companies doing business in China provide encryption keys to allow government entry into their databases.

ENDNOTES FOR SECTION 4

1. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Jen Weedon, June 15, 2015.
2. Damian Paletta, "Breached Network's Security Is Criticized," *Wall Street Journal*, June 24, 2015, 1.
3. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Paul Tiao, June 15, 2015.
4. McAfee and the Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," June 9, 2014; International Trade Administration, *Jobs Supported by Exports: An Update*, March 12, 2012.
5. Bill Whyman and Matthew L. Williams, "The Cybersecurity Imperative: 'Defend & Spend' in a New Landscape," *Evercore ISI Research*, May 19, 2015, 1.
6. Agency France-Press, "Cost of Cyber Attacks Jumps for U.S. Firms: Study," October 16, 2014.
7. Agency France-Press, "Cost of Cyber Attacks Jumps for U.S. Firms: Study," October 16, 2014.
8. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Paul Tiao, June 15, 2015.
9. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Paul Tiao, June 15, 2015.
10. Michael Stevens, "China's Cyber Threat Growing," *Security Week*, July 8, 2010.
11. Mark Slavit, "McConnell Said U.S. Losing Cyber War," *KRCGTV.com*, March 12, 2015.
12. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Dennis F. Poindexter, June 15, 2015.
13. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Jen Weedon, June 15, 2015.
14. Ken Dilanian, "General Warns of Dramatic Increase of Cyber-Attacks on U.S. Firms," *World Now* (*Los Angeles Times* blog), July 27, 2012.
15. Evercore ISI, "The Cybersecurity Imperative: 'Defend & Spend in a New Landscape,'" May 19, 2015.
16. The White House, Office of the Press Secretary, *Executive Order—Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, April 1, 2015.
17. The White House, Office of the Press Secretary, *Executive Order—Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, April 1, 2015.
18. Dennis F. Poindexter, *The Chinese Information War: Espionage, Cyberwar, Communications Control, and Related Threats to United States Interests*, McFarland & Company, Inc., 2013, 7.
19. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Jen Weedon, June 15, 2015.
20. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Jen Weedon, June 15, 2015
21. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Jen Weedon, June 15, 2015.
22. Northrup Grumman Corporation, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," October 9, 2009.
23. Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011*, October 2011.
24. CBS News, "FBI Director on Threat of ISIS, Cybercrime" (Interview with FBI Director James Comey), October 5, 2014.
25. Ellen Nakashima, "China Compiling Americans' Data," *Washington Post*, June 6, 2015.

26. Zhu Junqing, "Commentary: U.S. Wronging of China for Cyber Breaches Harms Mutual Trust," Xinhua (English edition), June 6, 2015.
27. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Dennis F. Poindexter, June 15, 2015.
28. Dimitar Kostadinov, "The Attribution Problem in Cyber Attacks," *Infosec Institute*, February 1, 2013.
29. Dimitar Kostadinov, "The Attribution Problem in Cyber Attacks," *Infosec Institute*, February 1, 2013.
30. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Paul Tiao, June 15, 2015.
31. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 2013.
32. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 2013.
33. Nicole Perlroth, "Hackers in China Attacked the Times for Last 4 Months," *New York Times*, January 30, 2013, 1.
34. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 2013.
35. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 2013.
36. U.S. Department of Justice, Office of Public Affairs, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014; Dune Lawrence, "U.S. Charges Five Chinese Military Hackers with Online Spying," Bloomberg News, May 19, 2014.
37. Mark A. Stokes, "The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398," *Project 2049 Institute*, July 27, 2015.
38. Geoff Dyer, Gina Chon, Hannah Kuchler, "Cyber Tensions Rise as U.S. Says Three Big Chinese Groups Benefitted from Hacking," *Financial Times*, October 8, 2015.
39. U.S. Department of Justice, Office of Public Affairs, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014; Dune Lawrence, "U.S. Charges Five Chinese Military Hackers with Online Spying," Bloomberg News, May 19, 2014.
40. Ellen Nakashima, "China Suspected of Breaching U.S. Postal Service Computer Networks," *Washington Post*, November 10, 2014.
41. Keith Wagstaff, "USPS Hack that Affected 800,000 Employees 'Very Sophisticated,'" NBC News, November 19, 2014.
42. Ellen Nakashima, "China Suspected of Breaching U.S. Postal Service Computer Networks," *Washington Post*, November 10, 2014.
43. Sarah Logan, "Beijing's Great Cannon Exposes Vulnerable Chinese Tech Firms," *Interpreter*, May 4, 2015.
44. Paul Mozur, "Attack on GitHub Appears to Have Ended," *Bits* (*New York Times* blog), April 1, 2015.
45. Christian de Loope, "China Develops 'Great Cannon' Censorship Tool—Is It Gearing up for a Cyber War?" *Tech Times*, April 13, 2015.
46. Charles Clover, "China Accused of Decade-Long Asia Cyber Espionage Campaign," *Financial Times*, April 13, 2015; FireEye, "APT30 and the Mechanics of a Long-Running Cyber Espionage Operation," April 2015.
47. Charles Clover, "China Accused of Decade-Long Asia Cyber Espionage Campaign," *Financial Times*, April 13, 2015.
48. Tim Culpan, "Decade-Long Cyberspy Attack Hacked Southeast Asian Targets," Bloomberg Businessweek, April 12, 2015.
49. Newley Purnell, "China's Hackers Run 10-Year Spy Campaign in Asia, Report Finds," *Wall Street Journal*, April 12, 2015.
50. Cory Bennett, "OPM Hack Hit over 22 Million People," *Hill*, July 9, 2015.
51. Damien Paletta, "U.S. Intelligence Chief James Clapper Suggests China behind OPM Breach," *Wall Street Journal*, June 25, 2015; Kristen Finklea, et al., "Cyber Intrusion into U.S. Office of Personnel Management: In Brief," *Congressional Research Service* (R44111), July 17, 2015.
52. Damien Paletta, "U.S. Intelligence Chief James Clapper Suggests China behind OPM Breach," *Wall Street Journal*, June 25, 2015.
53. Damien Paletta, "U.S. Intelligence Chief James Clapper Suggests China behind OPM Breach," *Wall Street Journal*, June 25, 2015.

54. Damien Paletta and Danny Yadron, "Over 21 Million Hit by Hack," *Wall Street Journal*, July 10, 2015, 2.
55. Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *Federal Eye (Washington Post* blog), July 9, 2015.
56. Jose Pagliery, "OPM Hack's Unprecedented haul: 1.1 million Fingerprints, *CNN Money*, July 10, 2015; Jason Miller, "OPM Finds Fivefold Increase in Fingerprint Data Stolen during Data Hack," *Federal News Radio*, September 23, 2015.
57. David E. Sanger, Julie Hirshfeld Davis, and Nicole Perlroth, "U.S. Was Warned of System open to Cyberattacks," *New York Times*, June 5, 2015.
58. David E. Sanger, Julie Hirshfeld Davis, and Nicole Perlroth, "U.S. Was Warned of System open to Cyberattacks," *New York Times*, June 5, 2015.
59. Sean Lyngaas, "Security Experts: OPM Breach Shows Einstein Isn't Enough" *Federal Computer Week*, June 5, 2015.
60. Senate Committee on Homeland Security and Government Affairs, testimony of Andy Ozment, Assistant Secretary for Cybersecurity and Communications, Department of Homeland Security, June 25, 2015.
61. Felicia Schwartz, "Penn State's Engineering School Computers Hacked," *Wall Street Journal*, May 16, 2015.
62. Felicia Schwartz, "Penn State's Engineering School Computers Hacked," *Wall Street Journal*, May 16, 2015.
63. Felicia Schwartz, "Penn State's Engineering School Computers Hacked," *Wall Street Journal*, May 16, 2015.
64. Michael Riley and Jordan Robertson, "China-Tied Hackers That Hit U.S. Said to Breach United Airlines," Bloomberg Businessweek, July 29, 2015; David E. Sanger, Julie Hirshfeld Davis, and Nicole Perlroth, "U.S. Wars Warned of System open to Cyberattacks," *New York Times*, June 5, 2015.
65. Michael Riley and Jordan Robertson, "China State-Sponsored Hackers Suspected in Anthem Attack," Bloomberg Business, February 5, 2015.
66. Jeremy Wagstaff, "Hunt for Deep Panda Intensifies in Trenches of U.S.-China Cyberwar," Reuters, June 21, 2015.
67. White House Office of the Press Secretary, *Executive Order—Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, April 1, 2015.
68. White House Office of the Press Secretary, *Statement by the President on Executive Order—Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, April 1, 2015.
69. National Institute of Standards and Technology, *Cybersecurity Framework Frequently Asked Questions*.
70. White House Office of the Press Secretary, *Statement by the President on Executive Order—Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, April 1, 2015.
71. White House Office of the Press Secretary, *Statement by the President on Executive Order—Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, April 1, 2015.
72. White House Office of the Press Secretary, *Conference Call to Preview the Visit of President Xi Jinping of the People's Republic of China*, via telephone, September 22, 2015; Politico, "Rhodes: Sanctions Still on the Table," September 23, 2015.
73. White House Office of the Press Secretary, *Remarks by the President to the Business Roundtable*, September 16, 2015.
74. White House Office of the Press Secretary, *On-the-record Press Call on the President's Executive Order*, via telephone, April 1, 2015.
75. U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011.
76. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S." *New York Times*, October 11, 2012.
77. David E. Sanger, "Pentagon Announces New Strategy for Cyberwarfare," *New York Times*, April 23, 2015.
78. David E. Sanger, "Pentagon Announces New Strategy for Cyberwarfare," *New York Times*, April 23, 2015.
79. U.S. Department of Defense, *News Transcript: Remarks of Secretary Carter at the Drell Lecture Cemex Auditorium, Stanford Graduate School of Business*, April 23, 2015.
80. U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011.
81. David E. Sanger, "Pentagon Announces New Strategy for Cyberwarfare," *New York Times*, April 23, 2015.

82. Damien Paletta, "U.S. Intelligence Chief James Clapper Suggests China behind OPM Breach," *Wall Street Journal*, June 25, 2015.
83. Robert D. Blackwill and Ashley J. Tellis, "Revising U.S. Grand Strategy toward China," *Council on Foreign Relations*, March 2015, 27.
84. Robert D. Blackwill and Ashley J. Tellis, "Revising U.S. Grand Strategy toward China," *Council on Foreign Relations*, March 2015, 27.
85. Robert D. Blackwill and Ashley J. Tellis, "Revising U.S. Grand Strategy toward China," *Council on Foreign Relations*, March 2015, 27.
86. Oona A. Hathaway, et al., "The Law of Cyber-Attack," *California Law Review*, 2012.
87. Oona A. Hathaway, et al., "The Law of Cyber-Attack," *California Law Review*, 2012, 1.
88. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Dennis F. Poindexter, June 15, 2015.
89. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Paul Tiao, June 15, 2015.
90. National Bureau of Asian Research, "The Report of the Commission on the Theft of American Intellectual Property," May 2013, 81.
91. National Bureau of Asian Research, "The Report of the Commission on the Theft of American Intellectual Property," May 2013, 81.
92. Matthew Eggers, Senior Director, National Security and Emergency Preparedness Department, U.S. Chamber of Commerce, interview with Commission staff, August 18, 2015.
93. Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*, October, 2011, 3.
94. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Paul Tiao, June 15, 2015.
95. Shannon Tiezzi, "U.S., China Hold Cyber Talks before Xi's Visit," *The Diplomat*, September 15, 2015.
96. Shannon Tiezzi, "U.S., China Hold Cyber Talks before Xi's Visit," *The Diplomat*, September 15, 2015.
97. *China Trade Extra*, "Xi Pledges Cooperation on Cybertheft, Implies Other U.S. Complaints are Baseless," September 23, 2015.
98. Elise Viebeck, "Will the Chinese Really Stop Hacking?" *Washington Post*, September 28, 2015, A19.
99. The White House Office of the Press Secretary, *FACT SHEET: President Xi Jinping's State Visit to the United States*, September 25, 2015.
100. Review & Outlook, "The Obama-Xi Cyber Mirage," *Wall Street Journal*, September 28, 2015, A16; Jack Goldsmith, "What Explains the U.S.-China Cyber 'Agreement?'" Lawfare Blog, September 26, 2015; Greg Austin, "China-U.S. Cyber Agreements: Has Beijing Outmaneuvered Washington?" *Diplomat,"* September 28, 2015.
101. The White House Office of the Press Secretary, *Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference*, September 25, 2015.
102. The White House Office of the Press Secretary, *FACT SHEET: President Xi Jinping's State Visit to the United States*, September 25, 2015.
103. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Dennis F. Poindexter, June 15, 2015.
104. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Dennis F. Poindexter, June 15, 2015.
105. U.S. Department of Commerce, SelectUSA initiative, *The Software and Information Technology Services Industry in the United States*.
106. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, August 2014, 1.
107. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, August 2014, 1.
108. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, August 2014, 98.
109. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 1*, July 2013.

110. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Matt Schruers, June 15, 2015.
111. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Matt Schruers, June 15, 2015.
112. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Matt Schruers, June 15, 2015.
113. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Matt Schruers, June 15, 2015.
114. Fredrick Erixon, Brian Hindley, and Hosuk Lee-Makiyama, "Protectionism Online: Internet Censorship and International Trade Law," *European Centre for International Political Economy*, 12, 2009, 1.
115. Fredrick Erixon, Brian Hindley, and Hosuk Lee-Makiyama, "Protectionism Online: Internet Censorship and International Trade Law," *European Centre for International Political Economy*, 12, 2009, 15.
116. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Matt Schruers, June 15, 2015.
117. U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, August 2014, 1.
118. Paul Mozur, "China Tries to Extract Pledge of Compliance from U.S. Tech Firms," *New York Times*, September 16, 2015.
119. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Samm Sacks, June 15, 2015.
120. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Samm Sacks, June 15, 2015.
121. Edward Wong, "Security Law Suggests a Broadening of China's Core Interests," *New York Times*, July 2, 2015; U.S.-China Economic and Security Review Commission, "Beijing Expands Control with Sweeping New Security Law" in *Monthly Analysis of U.S.-China Trade Data*, July 7, 2015.
122. Tom Mitchell, "China Passes Sweeping National Security Law," *Financial Times*, July 2, 2015, 1.
123. Tom Mitchell, "China Passes Sweeping National Security Law," *Financial Times*, July 2, 2015, 1.
124. Austin Ramzy, "What You Need to Know about China's Draft Cybersecurity Law," *Sinosphere* (*New York Times* blog), July 9, 2015.
125. National People's Congress, *Cybersecurity Law (Draft), China Law Translate*, July 6, 2015.
126. National People's Congress, *Cybersecurity Law (Draft), China Law Translate*, July 6, 2015.
127. U.S.-China Economic and Security Review Commission, *Red Cloud Rising: Cloud Computing in China*, March 2014.
128. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Samm Sacks, June 15, 2015.
129. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Samm Sacks, June 15, 2015.
130. Eva Dou, "U.S., China Discuss Proposed Banking Security Rules," *Wall Street Journal*, February 13, 2015.
131. Eva Dou, "U.S., China Discuss Proposed Banking Security Rules," *Wall Street Journal*, February 13, 2015.
132. Eva Dou, "U.S., China Discuss Proposed Banking Security Rules," *Wall Street Journal*, February 13, 2015.
133. *China Trade Extra*, "Tech Groups Call on USG to Fight Chinese Cybersecurity Policies," Vol. 33, No. 5, March 4, 2015.
134. Letter from various U.S. business associations to the Chinese Communist Party Central Leading Group for Cyberspace Affairs, January 28, 2015.
135. *China Trade Extra*, "Tech Groups Call on USG to Fight Chinese Cybersecurity Policies," Vol. 33, No. 5, March 4, 2015.
136. *China Trade Extra*, "Tech Groups Call on USG to Fight Chinese Cybersecurity Policies," Vol. 33, No. 5, March 4, 2015.

137. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Samm Sacks, June 15, 2015.
138. Gerry Shih, Michael Martina, and Matthew Miller, "China Summons Western Tech Firms, Revives Bank Cyber Rules," Reuters, August 8, 2015.
139. Gerry Shih, Michael Martina, and Matthew Miller, "China Summons Western Tech Firms, Revives Bank Cyber Rules," Reuters, August 8, 2015.
140. Michael Martina, "China Draft Counterterror Law Strikes Fear in Foreign Tech Firms," Reuters, February 27, 2015.
141. Jeff Mason, "Exclusive: Obama Sharply Criticizes China's Plans for New Technology Rules," Reuters, March 2, 2015.
142. Gerry Shih and Paul Carsten, "China Says Tech Firms Have Nothing to Fear from Anti-Terror Law," Reuters, March 4, 2015.
143. Jeremy Scahill and Josh Begley, "The Great SIM Heist," *Intercept*, February 19, 2015.
144. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Samm Sacks, June 15, 2015.
145. Steven Yang, Keith Zhai, and Tim Culpan, "China Said to Plan Sweeping Shift from Foreign Technology to Own," Bloomberg News, December 17, 2014.
146. *China Trade Extra*, "House Republican Leaders Urge Obama to Fight Harder against China Cybersecurity Rules," February 20, 2015.
147. Paul Carsten, "China Drops Leading Tech Brands for Certain State Purchases," Reuters, February 27, 2015.
148. Paul Carsten, "China Drops Leading Tech Brands for Certain State Purchases," Reuters, February 27, 2015.
149. U.S.-China Economic and Security Review Commission, *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China*, testimony of Samm Sacks, June 15, 2015; Michael Kan, "China Aims to Help Local Internet Firms Cross into the Market," *PC World*, March 5, 2015.
150. National Development and Reform Commission, *Report on the Implementation of the 2014 Plan for National Economic and Social Development and on the 2015 Draft Plan for National Economic and Social Development*, Third Session of the Twelfth National People's Congress, March 5, 2015, 23.
151. China Internet Network Information Center, *CNNIC Released the 35th Statistical Report on Internet Development in China*, February 4, 2015. Internet Live Stats, "Internet Users by Country (2014)."
152. McKinsey & Company, "China's Digital Transformation: The Internet's Impact on Productivity and Growth," July 2014.
153. McKinsey & Company, "China's Digital Transformation: The Internet's Impact on Productivity and Growth," July 2014, 5–6.
154. Scott D. Livingston, "Will China's New Anti-Terrorism Law Mean the End of Privacy?" *ChinaFile*, April 22, 2015.
155. Michael Kan, "China Aims to Help Local Internet Firms Cross into the Market," *PC World*, March 5, 2015.
156. Irving Wladawsky-Berger, "The Rise of the Digital Capital Economy," *CIO Journal* (*Wall Street Journal* blog), April 17, 2015; Boston Consulting Group, "The Internet Economy in the G–20," *BCG Report*, March 2012.
157. U.S. Department of Commerce, SelectUSA initiative, *The Software and Information Technology Services Industry in the United States, Select USA*.
158. Al Ramadan et al., "Time to Market Cap: The New Metric That Matters," *Play Bigger Advisors, LLC*.; U.S. Department of Commerce, SelectUSA initiative, *The Software and Information Technology Services Industry in the United States, Select USA*.