SECTION 3: CHINESE INTELLIGENCE SERVICES AND ESPIONAGE THREATS TO THE UNITED STATES

Introduction

The United States faces a large and growing threat to its national security from Chinese intelligence collection operations. Among the most serious threats are China's efforts at cyber and human infiltration of U.S. national security organizations. These operations are not a recent phenomenon, but reports of Chinese espionage against the United States have risen significantly over the past 15 years.[1] The threat from Chinese intelligence operations also extends overseas. For example, China's growing technical intelligence* collection capabilities are increasing its ability to monitor deployed U.S. military forces. Moreover, by infiltrating and attempting to infiltrate defense entities in U.S. ally and partner countries, China could affect U.S. alliance stability and indirectly extract sensitive U.S. national defense information. Meanwhile, the national security implications of Chinese intelligence collection operations have grown amid U.S.-China competition and Beijing's expanding military might.

This section examines the threat to U.S. national security from Chinese intelligence collection. It discusses the structure, role, capabilities, process, and operations of China's intelligence services; U.S. responses to Chinese espionage; and the implications of Chinese intelligence collection for U.S. national security.

China's Intelligence Services

China's intelligence community includes Chinese government, People's Liberation Army (PLA), and Chinese Communist Party (CCP) institutions that target U.S. national security organizations. The following are descriptions of these organizations and their roles within China's intelligence community. In all cases, the top priority for these organizations is to support and preserve the CCP-led Chinese party-state.[2]

Ministry of State Security

The Ministry of State Security (MSS) is a Chinese government ministry answerable to both China's State Council—the chief administrative authority of the Chinese government—and the CCP Politburo Standing Committee.[3] According to Peter Mattis, fellow at the Jamestown Foundation, the MSS "is not unlike an amalgam of [the U.S. Central Intelligence Agency] and [the U.S. Federal Bureau of Investigation]."[4] The MSS conducts a variety of intelligence col-

*"Technical intelligence" here refers to signals, imagery, electronic, and measurements and signatures intelligence.

lection operations, such as human intelligence (HUMINT) and cyber operations.[5]

PLA Intelligence

PLA intelligence is responsible for collecting foreign military, economic, and political intelligence* to support military operations.[6] The PLA—with its subsidiary units responsible for intelligence collection—answers to China's Central Military Commission (CMC), China's leading military authority, which is dual-hatted as a Chinese government organization and a CCP organization.[7] PLA intelligence organizations conduct HUMINT operations, as well as technical intelligence collection operations, to include cyber operations.[8]

Reforms to PLA Intelligence

Since late 2015, China has initiated several reforms to the structure of the PLA† that have reshaped major elements of PLA intelligence. Although much is unknown about these reforms, some information has emerged that gives insight into the evolution of PLA intelligence.

New PLA Agencies

In January 2016, Chinese President and General Secretary of the CCP Xi Jinping announced the reorganization of the PLA's four general departments (the general staff, political, logistics, and armaments departments) into 15 new agencies under the CMC.[9] The PLA General Staff Department, which had been the primary authority for PLA foreign intelligence collection, was reorganized into the new Joint Staff Department; however, it is still unclear whether the newly created Strategic Support Force or the Joint Staff Department will take on the former General Staff Department's supervisory responsibilities for intelligence activities.[10]

Before the dissolution of the General Staff Department, the most prominent PLA organizations responsible for foreign intelligence collection were the second, third, and fourth departments of the General Staff Department. The Second Department (2PLA) was responsible for the collection and analysis of HUMINT, imagery intelligence, and tactical reconnaissance.[11] The Third Department (3PLA) was responsible for collecting signals intelligence and conducting cyber operations.[12] According to John Costello, fellow at think thank New America, 3PLA was "roughly equivalent to the U.S. National Security Agency in function and mission."[13] The Fourth Department (4PLA)—responsible for electronic warfare and electronic countermeasures—surveilled foreign information networks.[14] In addition, theater-level PLA Army, Navy, Air Force, and missile forces contained intelligence units that mirrored the structure of General Staff Department intelligence units.[15] It is unclear how elements of PLA intelligence under the former General Staff Department will be reorganized within the new Joint Staff Department.

---

*Political intelligence is intelligence concerned with the dynamics of the internal and external political affairs of foreign countries, regional groups, multilateral treaty arrangements, and organizations and foreign political movements directed against or having an impact on established governments or authority. Bruce W. Watson, Susan M. Watson, and Gerald W. Hopple, *United States Intelligence: An Encyclopedia*, Garland Publishing, Inc., 1990, 447.

†For more information on recent PLA reforms, see Chapter 2, Section 1, "Year in Review: Security and Foreign Affairs."

Strategic Support Force

In December 2015, President Xi announced the formation of the Strategic Support Force, a new branch of the PLA.[16] According to Song Zhongping, a professor at the PLA Rocket Force Equipment Research Academy and former PLA Second Artillery Force officer, the Strategic Support Force will consist of cyber forces "focusing on attack and defense," space forces "focus[ing] on reconnaissance and navigation satellites," and electronic warfare forces focusing on "jamming and disrupting enemy radar and communications."[17] This suggests the Strategic Support Force will take on and centralize some intelligence collection missions and processes previously spread among various elements of the PLA. It is likely that the former 3PLA and 4PLA will be subordinated to the Strategic Support Force.[18]

New Theater Command Structure

In February 2016, President Xi announced the reorganization of China's seven military regions into five "theater commands."[19] The structure of theater- and tactical-level military intelligence before and after this reorganization is difficult to discern using open sources, but it appears the PLA is moving toward greater jointness and integration of the intelligence collected by various military services to inform military decision makers.*[20]

Other Chinese Intelligence Services

Several other actors in the Chinese intelligence community collect foreign intelligence. The following are two notable examples of these organizations. Both have conducted influence operations in addition to intelligence collection operations.[21]

PLA General Political Department International Liaison Department

In addition to the PLA's primary military intelligence forces under the former General Staff Department, before the dissolution of the PLA's four general departments, the PLA General Political Department International Liaison Department was responsible for collecting foreign intelligence through networks of official and unofficial agents abroad.[22] International Liaison Department agents used informal contacts with foreign actors to identify and investigate individuals and organizations to collect intelligence and expand China's influence abroad.[23] It appears the new CMC Political Work Department may take over this mission.

CCP United Front Work Department

The United Front Work Department under the CCP Central Committee is responsible for, among other things, building and managing relationships with actors overseas to expand China's soft power and further the CCP's political agenda.[24] The department reported-

*It appears that PLA military services (the PLA Army, Air Force, Navy, and Rocket Force), in addition to the theater commands, will have integrated technical reconnaissance units and electronic warfare and electronic countermeasure units. However, the relationship between these units and the new CMC departments and Strategic Support Force is unclear. Junichi Takeda, "President Xi's Strong Army Strategy," *Gunji Kenkyu* (Japan), May 2016, 50–65; Chinese military expert, interview with Commissioner.

ly participates in building foreign intelligence collection networks, particularly in Taiwan.[25]

China's Intelligence Collection Capabilities

Assessing China's intelligence collection capabilities is difficult. Open source analysts often must rely on media reports, which are not necessarily authoritative and do not necessarily provide a full picture of China's intelligence activities. Case studies offer some insight, but public reports might not reflect the most sophisticated Chinese espionage operations.

Human Intelligence Capabilities

Because the affiliation of Chinese intelligence agents is unknown in many cases, it is often difficult to attribute reported infiltrations to either the MSS or the former 2PLA, the two primary foreign HUMINT collectors in China's intelligence community.[26]

- *2PLA:* 2PLA has demonstrated it can use HUMINT operations to infiltrate and extract intelligence from prominent U.S. national security organizations. Notably, between 2004 and 2008, an agent reportedly affiliated with 2PLA successfully recruited two U.S. Department of Defense (DOD) employees, James Fondren and Gregg Bergersen. Both men passed classified U.S. national defense information to the agent (see "Targets of Chinese Espionage," later in this section).[27] Open sources have not indicated how the reorganization of the CMC departments will affect the subordination and control of the PLA's HUMINT organizations.
- *MSS:* In the past ten years, reported cases of Chinese espionage against the United States have not suggested MSS HUMINT operations have been effective.[28] In the most recent high-profile HUMINT case reportedly handled by the MSS, the ministry's U.S. informant received tens of thousands of dollars from his handlers to apply for employment at U.S. national security organizations, but was apprehended by U.S. authorities before infiltrating these organizations (see "China's Approach to HUMINT," later in this section).[29] However, the MSS has been notably active and successful conducting HUMINT operations against Taiwan.[30]

China's HUMINT agencies could become more effective as China's intelligence community pursues more aggressive operations, and as China's access to detailed sources of personal information on U.S. actors—such as the information China reportedly obtained through the U.S. Office of Personnel Management (OPM) hack—gives Chinese HUMINT collectors a wealth of information to target and recruit U.S. actors.[31]

Technical Intelligence Collection Capabilities

The PLA operates an extensive and increasingly sophisticated array of ground-, sea-, air-, and space-based assets for the collection of technical intelligence.*[32] Many recent developments in China's military modernization—such as the rapid development and deployment

*"Technical intelligence" here refers to signals, imagery, electronic, and measurements and signatures intelligence.

of advanced intelligence, surveillance, and reconnaissance (ISR) ships, aircraft, and satellites—will increase China's ability to collect intelligence on U.S. military forces and the military forces of U.S. allies and partners.* Moreover, the PLA's drive to increase information sharing between military units will facilitate the integration of technical intelligence to create a more accurate, real-time picture of battlefield conditions.[33] These developments would strengthen China's hand in a military confrontation, or in the lead-up to a military confrontation, with the United States.[34]

Cyber Espionage

China has a large, professionalized cyber espionage community. Chinese intelligence services have demonstrated broad capabilities to infiltrate a range of U.S. national security (as well as commercial) actors with cyber operations (see "Targets of Chinese Espionage," later in this section). Units within the former 3PLA, in particular, have been responsible for a large number of cyber operations against U.S. actors.[35] According to Director of National Intelligence James Clapper, China—along with Russia, Iran, and North Korea—poses the most significant cybersecurity threat to the United States.[36] Moreover, according to DOD,

> *China is using its cyber capabilities to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs. The information targeted could potentially be used to benefit China's defense industry, high-technology industries, and provide the CCP insights into U.S. leadership perspectives on key China issues. Additionally, targeted information could inform Chinese military planners' work to build a picture of U.S. defense networks, logistics, and related military capabilities that could be exploited during a crisis.*[37]

In addition to the cyber espionage elements of the MSS and PLA, many unofficial Chinese actors target the United States with cyber espionage operations. These actors include government contractors, independent "patriotic hackers," and criminal actors.[38] Distinguishing between the operations of official and other Chinese cyber actors is often difficult, as is determining how these groups interact with each other. Some observers suggest China is shifting cyber espionage missions away from unofficial actors to centralize and professionalize these operations within its intelligence services.[39]

China's Intelligence Process

Understanding how Chinese intelligence services receive tasks, fuse intelligence, and disseminate intelligence products to decision makers is crucial to identifying what information reaches Chinese decision makers and how effectively that information is delivered. Analyzing this aspect of Chinese intelligence is difficult using open sources, but public reports and expert commentaries offer some insight.

---

*For more information on China's military modernization affecting its ISR capabilities, see U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress*, November 2015, 240–246; U.S.-China Economic and Security Review Commission, *2014 Annual Report to Congress*, November 2014, 299–314.

- *Tasking:* China's intelligence services are responsible for serving the interests of the Chinese state and the CCP.*[40] The extraction of U.S. national defense information would advance these priorities by aiding China's military modernization and offering insight into U.S. national security decision making. The MSS and PLA are subordinate to—and most likely receive tasks from—the CCP Politburo Standing Committee and the CMC, respectively, and tasking from these organizations may be coordinated by a variety of organizations across the CCP, the Chinese government, and the PLA.[41]
- *Processing and communication to decision makers:* China may lack a well-organized system for processing and communicating intelligence to decision makers.[42] However, Chinese intelligence services probably share intelligence to support each other's operations. In testimony before the Commission, Mark Stokes, executive director of the Project 2049 Institute, wrote that "the PLA's [signals intelligence] community presumably provides direct support to senior policymakers and [the] HUMINT community, including the MSS, CMC Joint Staff Department Intelligence Bureau, and the CMC Political Work Department Liaison Bureau."[43] Moreover, the PLA's increasing jointness most likely will facilitate the processing and communication of diverse sources of intelligence to military decision makers.[44]

China's Intelligence Collection Operations against U.S. National Security Entities

Chinese intelligence services conduct extensive intelligence collection operations against U.S. national security entities, including private U.S. defense companies. This section examines how China conducts HUMINT operations, in particular, and highlights the threat of Chinese espionage to U.S. national security by providing examples of Chinese infiltrations and alleged infiltrations of a wide range of U.S. national security entities.

China's Approach to HUMINT

China's approach to HUMINT is broadly similar to U.S. intelligence agencies' approach to HUMINT.[45] Chinese intelligence services conduct overt, covert, and clandestine intelligence collection operations † against U.S. targets through a network of agents within and outside of China working as—among other things—diplomats, defense attachés, and academics.[46] They employ a variety of means to recruit and handle intelligence collectors, such as blackmail, financial incen-

*Thomas Woodrow, former senior intelligence analyst for the Pacific Command Joint Intelligence Operations Center China Division, notes that Chinese leaders describe "national strategic priorities as 'core interests' [and that] … China's core interests include 'the political stability of China' and the 'sovereignty and security, territorial integrity, and national unity of China.' These core interests can also be viewed as red lines indicating a Chinese threshold for the potential use of military force." Thomas Woodrow, "The PLA and Cross-Border Contingencies in North Korea and Burma," in Andrew Scobell et al., *The People's Liberation Army and Contingency Planning in China*, National Defense University Press, 2015, 206.

†Overt operations are openly acknowledged by or are readily attributable to their sponsor. Covert operations are planned and executed to conceal the identity of or permit plausible denial by their sponsor. Clandestine operations are sponsored or conducted with the intent to assure the secrecy and concealment of the operation. U.S. Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, November 8, 2010, 33, 55, 180; William Safire, "Spookspeak," *New York Times Magazine*, February 13, 2005.

tives, and sexual entrapment.[47] They recruit and employ agents to collect a wide range of information, including U.S. national security secrets. Chinese intelligence services seek to recruit agents from a variety of backgrounds. According to the authors of *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, William C. Hannas, James Mulvenon, and Anna B. Puglisi,

> *While Chinese intelligence does have a historically strong track record of attempting to recruit ethnic Chinese, primarily because of cultural and language affinity, more recent cases suggest that they have broadened their tradecraft to recruit non-ethnic assets as well.*[48]

Moreover, China has demonstrated interest in collecting intelligence through U.S. sources with indirect access to U.S. national security information.[49] According to Mr. Mattis,

> *In one case that I am aware, Chinese intelligence pitched someone with a think tank affiliation in D.C., and his value was in, at least as it was described to him, being able to write reports about U.S.-China relations or U.S. policy toward [China] because of a broad range of contacts to whom he could reach out and speak.*[50]

Notably, in at least one confirmed case, Chinese intelligence recruited a recent U.S. college graduate, Glenn Duffie Shriver, while he was living in China shortly after studying abroad in China in 2002–2003.[51] In October 2010, Mr. Shriver pleaded guilty to conspiring to provide U.S. national defense information to Chinese intelligence officers.[52] He received more than $70,000 from his Chinese handlers to apply to the U.S. Foreign Service and the Central Intelligence Agency National Clandestine Service with the intention of communicating classified U.S. national defense information to them after gaining employment.[53]

Although Chinese intelligence services approach foreign HUMINT collection with a similar framework to their U.S. counterparts,[54] their tactics differ on several points. In testimony before the Commission, Mr. Mattis said, "The distinctions between the U.S. and Chinese approaches to HUMINT probably are questions of specific techniques and comfort operating overseas."[55] For example, Chinese intelligence agents have not been observed conducting dead drops,* a common method in Western intelligence collection for the transmission of items between agents and their case officers.[56] Moreover, Chinese intelligence services historically appeared to recruit nearly all their agents within China, rather than recruiting agents in target or other foreign countries, although in a significant evolution, Chinese intelligence services in recent years have appeared increasingly willing to recruit agents abroad.[57]

Targets of Chinese Espionage

Chinese intelligence services target a broad range of U.S. national security actors, including military forces, defense industrial compa-

*A "dead drop" is a covert procedure in which an agent leaves a message or material in a safe location for retrieval by another agent or controller at a later time. Bruce W. Watson, Susan M. Watson, and Gerald W. Hopple, *United States Intelligence: An Encyclopedia*, Garland Publishing, Inc., 1990, 148.

nies, national security decision makers, and critical infrastructure entities. These operations have far-reaching implications for U.S. national security.[58] Moreover, the threat to U.S. national security extends overseas. China's infiltration of the systems of U.S. allies and partners could have serious implications for U.S. alliance stability and the security of U.S. national defense information.

Although this section focuses on Chinese intelligence collection against U.S. national security entities, Chinese commercial espionage also harms U.S. national security. As National Counterintelligence Executive Bill Evanina said in July 2015, "Economic security is national security."[59] Intrusions by Chinese actors into U.S. companies and other commercial institutions harm both the individual companies and the overall U.S. economy, to the benefit of China.* China recognizes the link between economic and national security, and its commercial and national security espionage efforts function in tandem to exploit it.[60]

The following are selected examples of China's infiltration or alleged infiltration of entities with a role in U.S. national security. In general, China's attempts to infiltrate these targets are almost certainly increasing.[61]

U.S. Military Forces

China's intelligence collection operations targeting U.S. military forces could give China insight into U.S. operational plans. This could allow China to more fully anticipate and more efficiently and effectively counter U.S. military operations.

- According to the Senate Committee on Armed Services, "Hackers associated with the Chinese government successfully penetrated the computer systems of U.S. Transportation Command contractors at least 20 times in a single year [from June 2012 to May 2013], intrusions that show vulnerabilities in the military's system to deploy troops and equipment in a crisis."[62]
- In March 2014, Benjamin Pierce Bishop, a former defense contractor at U.S. Pacific Command and retired lieutenant colonel in the U.S. Army, pleaded guilty to communicating classified national defense information, including information on joint training between the U.S. and South Korean militaries, to an unauthorized person—a Chinese woman with whom he was involved in a romantic relationship.[63]
- In September 2009, James Fondren, former deputy director of Pacific Command's liaison office in Washington, DC, was found guilty of engaging in unlawful communication of classified information.[64] According to court documents, he had written "opinion papers" containing classified DOD information concerning the PLA and sold them to a Chinese intelligence agent.[65]
- In March 2008, Gregg Bergersen, former analyst at the Defense Security Cooperation Agency (an agency within DOD), pleaded guilty to conspiring to disclose national defense information to persons not entitled to receive it.[66] Mr. Bergersen had passed

*For additional discussion of China's commercial cyber espionage, see U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress*, November 2015, 192–228.

information to a Chinese intelligence agent and received money and gifts from the agent.[67] Mr. Bergersen leaked information about anticipated U.S. arms sales to Taiwan, among other subjects.[68]

U.S. Defense Industrial Entities

China's intelligence collection operations targeting U.S. defense industrial entities and its acquisition of sensitive defense technology could undermine U.S. military superiority by accelerating China's military modernization and giving China insight into the capabilities and operation of U.S. weapons and weapons systems.

- In June 2016, Wenxia "Wency" Man, a Chinese-born naturalized U.S. citizen, was convicted of conspiring with an agent in China to illegally export to China the MQ–9 Reaper/Predator B unmanned aerial vehicle, as well as engines used in the F–35, F–22, and F–16 jet fighters and technical data associated with these platforms.[69]
- In June 2016, Amin "Amy" Yu, a Chinese national and permanent resident of the United States, pleaded guilty to illegally acting as an agent of the Chinese government.[70] Ms. Yu illegally exported commercial technology used in marine submersible vehicles* to conspirators at China's Harbin Engineering University, a research institute that supports PLA Navy military modernization.[71]
- In March 2016, Su Bin, a Chinese national, pleaded guilty to conspiring from 2008 to 2014 to steal U.S. military technical data, including data on the Boeing C–17 Globemaster military transport aircraft and jet fighter aircraft, and export this information to China.[72] Some of Mr. Su's co-conspirators were members of the PLA Air Force.[73]

National Security Decision Makers and Government Organizations

China's intelligence collection operations targeting U.S. national security decision makers and government organizations could give China insight into highly sensitive U.S. national security decision making processes.

- In August 2016, Kun Shan "Joey" Chun, a Chinese-born naturalized U.S. citizen, pleaded guilty to illegally acting as an agent of the Chinese government.[74] Mr. Chun was a Federal Bureau of Investigation (FBI) electronics technician. He passed sensitive information to China on, among other things, surveillance technologies used by the FBI.[75] Mr. Chun's Chinese contacts provided him with financial payments and partially paid for a trip to Italy and France, during which he met with a Chinese intelligence officer.[76]
- According to an NBC report from August 2015, since 2010 China has targeted and infiltrated the personal e-mail accounts of

*According to the U.S. Department of Justice, "marine submersible vehicles" refers to "unmanned underwater vehicles, remotely operated vehicles, and autonomous underwater vehicles." U.S. Department of Justice, *Florida Woman Charged in 18-Count Indictment for Conspiracy to Illegally Export Systems, Components, and Documents to China*, April 21, 2016.

many Obama Administration officials.[77] As of 2014 the infiltrations were ongoing, according to the report.[78]

- In July 2015, OPM announced that hackers had extracted personnel records of roughly 22 million U.S. citizens.[79] The hackers were reportedly affiliated with the MSS.[80] Some of the stolen files contained detailed personal information of federal workers and contractors who have applied for security clearances. Among the information extracted were the fingerprints of 5.6 million people, some of which could be used to identify undercover U.S. government agents or to create duplicates of biometric data to obtain access to classified areas.[81]
- In 2010, China reportedly attempted to infiltrate the e-mail accounts of top U.S. national security officials, including then Joint Chiefs of Staff chairman Admiral Mike Mullen and then chief of naval operations Admiral Gary Roughead.[82]
- In May 2016, Mr. Clapper said U.S. intelligence has seen evidence that foreign actors have targeted the 2016 presidential campaigns with cyber operations.[83] These actors most likely include Chinese intelligence services, as well as actors in Russia and other countries.[84] During the 2008 U.S. presidential election, China reportedly infiltrated information systems of the campaigns of then senator Barack Obama and Senator John McCain.[85]

U.S. Critical Infrastructure

U.S. critical infrastructure* entities are a major target of Chinese cyber operations, and China is capable of significantly disrupting or damaging these entities.[86] In 2013, the U.S. Department of Homeland Security reported that attacks—including cyber intrusions—on critical infrastructure could disrupt "the ability of government or industry to … carry out national security-related missions."[87] At a November 2014 hearing of the House of Representatives Permanent Select Committee on Intelligence, Admiral Michael Rogers, commander of U.S. Cyber Command and director of the National Security Agency, indicated he believed "advanced nation state adversaries" like China or Russia have the capability to "shut down vital infrastructure like oil and gas pipelines, power transmission grids, and water distribution and filtration systems."[88] China reportedly has already infiltrated many U.S. critical infrastructure entities,†

*According to the U.S. Department of Homeland Security, critical infrastructure entities are entities "considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." A Presidential Policy Directive from February 2013 defines 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems. U.S. Department of Homeland Security, *Critical Infrastructure Sectors*, October 27, 2015; White House Office of the Press Secretary, *Presidential Policy Directive: Critical Infrastructure Security and Resilience*, February 12, 2013.

†In April 2016, Szuhsiung "Allen" Ho, a Chinese-born naturalized U.S. citizen, and China General Nuclear Power Company, a Chinese state-owned enterprise, were indicted for conspiracy to unlawfully engage and participate in the production and development of special nuclear material outside the United States. Maria L. La Ganga, "Nuclear Espionage Charge for China Firm with One-Third Stake in UK's Hinkley Point," *Guardian*, August 10, 2016; U.S. Department of Justice, *U.S. Nuclear Engineer, China General Nuclear Power Company, and Energy Technology International Indicted in Nuclear Power Conspiracy against the United States*, April 14, 2016.

such as power transmission grids, and installed software that could be used to disable or destroy infrastructure components in a crisis or military conflict.[89]

U.S. Allies and Partners

At a minimum, China has targeted several U.S. ally and partner countries with intelligence collection operations. To the extent that the United States has shared military technology, weapons and weapons systems, and operational plans with these countries, China's infiltration of their defense establishments could compromise U.S. national security. These infiltrations also threaten U.S. alliance stability.

Among U.S. allies and partners, Taiwan is a prominent target of Chinese espionage. David Major, chief executive officer and president of the CI Centre, testified to the Commission that 56 agents of China were arrested in Taiwan from 2002 to 2016 for involvement in Chinese espionage plots to extract sensitive information—including U.S. military technology shared with Taiwan—from Taiwan defense and intelligence organizations.[90] The implications of this challenge for the U.S.-Taiwan relationship are particularly significant.[91] Taiwan relies on defense cooperation with the United States—including the transfer of U.S. military equipment—to help maintain its self-defense capabilities in the face of China's rapidly growing military might.[92] Moreover, Taiwan's strategic position in the Western Pacific makes its defensibility an important aspect of the U.S. alliance system and strategy for the region.[93]

In addition, cases of alleged Chinese infiltrations, including the following, have affected other U.S. partners:

- In July 2016, the Finnish cybersecurity firm F-Secure published a report suggesting China was responsible for cyber intrusions into the information systems of the Philippines Department of Justice, organizers of the Asia Pacific Economic Cooperation summit, and an unidentified international law firm representing the Philippines in the lead-up to the July 2016 decision by the Permanent Court of Arbitration at The Hague regarding the China-Philippines territorial dispute in the South China Sea.[94]
- In February 2016, a senior Norwegian intelligence official said actors in China had stolen confidential information from Norwegian companies that is now being used in Chinese military technology.[95] Norway is a member of the North Atlantic Treaty Organization.
- In December 2015, the Australian Broadcasting Corporation published a report suggesting China was responsible for a massive cyber intrusion into the systems of the Australian Bureau of Meteorology, which provides data to the Australian Department of Defence.[96] Australia is a U.S. treaty ally.
- China-based actors have conducted extensive cyber operations targeting Japan.[97] In February 2015, the Japan National Institute of Information and Communications Technology reported that China was responsible for 40 percent of approximately 26 billion attempts to compromise Japanese information systems in 2014.[98] Japan is a U.S. treaty ally.

- Chinese intelligence has recruited agents in Thailand and, reportedly, the Philippines, both of which are U.S. treaty allies.[99] Moreover, China allegedly handled a U.S. informant while he was traveling in Italy and France.[100] China's apparent shift toward more overseas recruitment and handling operations[101] could create a greater espionage threat environment in these and other U.S. partner countries.

U.S. Responses to Chinese Espionage

Recent U.S. responses to Chinese espionage have included an April 2015 executive order allowing for sanctions in response to foreign "malicious cyber-enabled activities,"* a September 2015 memorandum of understanding between the United States and China agreeing that neither government would "conduct or knowingly support cyber-enabled theft of intellectual property … with the intent of providing competitive advantages to companies or commercial sectors,"[102] and increased U.S. Department of Justice (DOJ) investigations and prosecutions of espionage cases involving Chinese actors. (For more information on the status of the September 2015 memorandum of understanding, see Chapter 1, Section 1, "Year in Review: Economics and Trade.") This section considers DOJ's responses in detail, as well as the U.S. Intelligence Community's response and enhanced U.S. government cybersecurity measures.†

DOJ Responses

U.S. prosecutions of alleged Chinese commercial espionage have risen sharply over the past several years. From 2014 to 2015 alone, Chinese commercial espionage cases accounted for a large portion of a 53 percent rise in commercial espionage cases investigated by the FBI.‡[103] Because DOJ sometimes has approached cases of defense-related espionage as commercial espionage cases—that is, cases prosecuted under commercial espionage laws, rather than defense espionage laws—these statistics probably capture a rise in Chinese espionage operations targeting U.S. national security actors.[104] Moreover, as noted earlier, non-defense-related Chinese commercial espionage itself threatens U.S. national security.

In February 2013, as a part of the Obama Administration's rollout of a national strategy to protect U.S. trade secrets, then attorney general Eric Holder said DOJ "has made the investigation and prosecution of trade secret theft a top priority," and that DOJ's National Security Division Counterespionage Section "has taken a leading role in economic espionage cases—and others affecting national security and the export of military and strategic commodities or technology."[105] In the same speech, Mr. Holder highlighted the threat from China by listing successful prosecutions of individuals

*The Obama Administration has not yet applied the sanctions against China or any other country. For additional information about the sanctions, see U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress,* November 2015, 204–205.

†For more information on the April 2015 executive order, see U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress*, November 2015, 204–205.

‡In May 2014, a federal grand jury indicted five PLA officers for computer hacking and economic espionage conducted against U.S. companies, among other offenses. Since the indictment, the U.S. government has taken no further actions in the case. U.S. Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014.

for transferring trade secrets—including, in one case, defense information—to China.[106]

U.S. Intelligence Community Responses

The U.S. counterintelligence response to Chinese espionage has suffered from a lack of coordination within the U.S. Intelligence Community. According to the Office of the Director of National Intelligence (ODNI) *National Counterintelligence Strategy of the United States of America 2016*, "The current and emerging [counterintelligence] challenges facing the United States require an integrated, whole-of-government response."[107] The document outlines priorities for achieving this objective, such as "strengthen[ing] secure collaboration, responsible information sharing and safeguarding, and effective partnerships" among counterintelligence organizations.[108] However, ODNI's Office of the National Counterintelligence Executive, which is statutorily responsible for developing the U.S. government National Counterintelligence Strategy, does not appear to have practical authority to make structural changes within the U.S. Intelligence Community toward this goal.[109] Michelle Van Cleave, former national counterintelligence executive, testified to the Commission that "instead of looking at the strategic implications of China's intelligence operations, the U.S. government for the most part has adopted a case-by-case approach to dealing with the threat they represent."[110] This approach has—at least publicly—largely manifested as a series of isolated espionage prosecutions, rather than a coordinated counterintelligence effort across the Federal Government.

Enhanced U.S. Government Cybersecurity Measures

The Obama Administration has taken some steps to enhance cybersecurity measures at federal agencies and government contractors, including the following:

- In December 2015, DOD issued an interim amendment to the Defense Federal Acquisition Regulation Supplement that strengthened cybersecurity requirements and cyber incident reporting requirements for defense contractors.[111]
- In February 2016, the Obama Administration announced the creation of the Commission on Enhancing National Cybersecurity.[112] The commission's mandate includes making recommendations for measures to increase "the quality, quantity, and level of expertise of the cybersecurity workforce in the Federal Government and private sector."[113] In August 2016, the commission released a request for information on critical infrastructure cybersecurity and cybersecurity research and development, among other topics.[114]
- In May 2016 the Federal Acquisition Regulation was amended to impose higher requirements on U.S. government contractors to safeguard their information systems from cyber intrusions and to require them to "identify, report, and correct information and information system flaws in a timely manner."[115]
- The Obama Administration's fiscal year (FY) 2017 budget proposal allotted more than $19 billion for cybersecurity—an increase of more than 35 percent over FY 2016.[116]

- In July 2016, the White House issued a Presidential Policy Directive on "Cyber Incident Coordination."[117] The directive created a coordination mechanism and clarified the division of labor between U.S. government agencies responsible for responding to "significant cyber incidents" affecting U.S. government and private entities.[118]

The U.S. government's efforts to increase cybersecurity at national security organizations have not always been communicated clearly. In April 2016, an e-mail from U.S. Air Force Cyber Command circulated within the Air Force indicated that products of Lenovo Group Ltd.—a technology company affiliated with the Chinese government—would be removed from DOD's "Approved Products List," and that all Lenovo products currently in use would be removed from DOD systems.[119] However, within several days an Air Force spokeswoman said the message should not have been sent and indicated that DOD had not banned Lenovo products.[120] It is unclear how this situation was resolved.

Increased cybersecurity measures could mitigate, but will not eliminate, the threat of Chinese cyber espionage. Cyber intruders generally develop new approaches more quickly than their targets can develop defenses.[121] Moreover, the human element of cyber espionage is difficult, and sometimes impossible, to defend against. Poor personal cybersecurity practices and procedures among insiders, as well as intentional leaks by insiders, can aid infiltrators.[122]

Implications for U.S. National Security

China's illicit extraction of sensitive U.S. national security information has far-reaching consequences for U.S. interests.

In recent years, Chinese agents have extracted data on some of the most advanced weapons and weapons systems in the U.S. arsenal, such as jet fighters and unmanned submersible vehicles. The loss of these and other sensitive defense technologies undermines U.S. military superiority by accelerating China's military modernization and giving China insight into the capabilities and operation of U.S. weapons and weapons systems.

The United States shares weapons, weapons systems, and operational plans with its allies and partners, many of whom China has targeted with espionage operations. China's infiltrations of these countries' defense establishments have significant implications for U.S. alliance stability. If the United States perceives significant security risks in sharing information and equipment with its partners, it could hesitate to provide such support in the future.[123] Even when China is not successful in extracting sensitive information, public reports of failed espionage attempts—such as the many recent reports of Chinese agents apprehended in Taiwan[124]—could undermine U.S. confidence in its partners and contribute to a deterioration in bilateral defense relations.

China's infiltrations of the information systems of U.S. government organizations with a role in national security, along with infiltrations of the e-mail accounts of prominent U.S. government officials, could give China insight into U.S. government national security decision making and provide China with opportunities to manipulate it. These breaches could give China insight into inter-

nal U.S. discussions of issues relevant to U.S.-China contingencies, potentially allowing China to anticipate and counter U.S. actions, including military operations. Moreover, these breaches could give Chinese intelligence information useful for targeting and recruiting agents for espionage and influence operations.

The Chinese intelligence threat to U.S. national security will grow as China reforms and centralizes its intelligence apparatus and gains experience conducting intelligence collection operations. Its HUMINT operations, in particular, already appear to be growing more aggressive and extensive.[125] China's intelligence processing and communication to decision makers is likely to become more effective and efficient as the PLA moves toward joint, integrated intelligence operations. The potential resubordination and centralization of elements of the former PLA General Staff Department intelligence departments to the new Strategic Support Force also could create a more streamlined and well-coordinated intelligence apparatus.

Conclusions

- Chinese intelligence has repeatedly infiltrated U.S. national security organizations and extracted information with serious consequences for U.S. national security, including information on the plans and operations of U.S. military forces and the designs of U.S. weapons and weapons systems. This information could erode U.S. military superiority by aiding China's military modernization and giving China insight into the operation of U.S. platforms and the operational approaches of U.S. forces to potential contingencies in the region.
- China's growing technical intelligence collection capabilities could strengthen China's hand in a contingency. Its extensive network of intelligence, surveillance, and reconnaissance (ISR) assets and continued development and deployment of increasingly advanced ISR platforms will increase the ability of the People's Liberation Army (PLA) to monitor U.S. forces. Moreover, the enhanced jointness of PLA intelligence at the theater level will facilitate the integration of data collected by these platforms to form a more comprehensive, real-time battlefield picture.
- Chinese intelligence reportedly has repeatedly targeted and succeeded in infiltrating the personal e-mail accounts of leading U.S. government officials. These infiltrations could give China insight into highly sensitive U.S. national security decision-making processes.
- China's infiltration of the national security establishments of U.S. allies and partners could allow China to indirectly access sensitive U.S. national security information. Moreover, these breaches could undermine the strength and stability of U.S. alliances by causing the United States to hesitate to share sensitive information with its partners.

RECOMMENDATIONS

Chinese Intelligence Services and Espionage Threats to the United States

The Commission recommends:

- Congress direct the U.S. Department of State to develop educational materials to alert U.S. citizens living and traveling abroad about recruitment efforts by Chinese intelligence agents, and to make these materials available to U.S. universities and other institutions sending U.S. students to China. Congress should also direct the U.S. Department of Defense to develop and implement a program to prepare U.S. students studying in China through Department of Defense National Security Education Programs to recognize and protect themselves against recruitment efforts by Chinese intelligence agents.
- Congress direct the Federal Bureau of Investigation to provide a classified report to Congress on what risks and concerns have been identified as associated with information systems acquired by the U.S. government, and how those risks are being mitigated. This report should identify information systems or components that were produced, manufactured, or assembled by Chinese-owned or –controlled entities.

ENDNOTES FOR SECTION 3

1. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of David Major, June 9, 2016.

2. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016.

3. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of John Costello, June 9, 2016; Robert Windrem, "China Read Emails of Top U.S. Officials," NBC, August 10, 2015; Susan V. Lawrence, "China's Political Institutions and Leaders in Charts," *Congressional Research Service*, November 12, 2013, 8; and U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress*, November 2009, 152.

4. Peter Mattis, "A Guide to Chinese Intelligence Operations," *War on the Rocks* (Blog), August 18, 2015.

5. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016; Ellen Nakashima, "Following U.S. Indictments, China Shifts Commercial Hacking away from Military to Civilian Agency," *Washington Post*, November 30, 2015; and Peter Mattis, "A Guide to Chinese Intelligence Operations," *War on the Rocks* (Blog), August 18, 2015.

6. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of John Costello, June 9, 2016; Mark A. Stokes, "The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398," *Project 2049 Institute*, July 27, 2015, 11; CrowdStrike, "CrowdStrike Intelligence Report: Putter Panda," June 9, 2014; and U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2013*, May 2013, 36.

7. Susan V. Lawrence, "China's Political Institutions and Leaders in Charts," *Congressional Research Service*, November 12, 2013, 10.

8. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of John Costello, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016; and U.S. Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014.

9. Xinhua, "China Reshuffles Military Headquarters," January 11, 2016; China Military Online, "China's New Central Military Commission Organ Established," January 11, 2016.

10. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of John Costello, June 9, 2016; James Mulvenon, "China's 'Goldwater-Nichols'? The Long-Awaited PLA Reorganization Has Finally Arrived," *China Leadership Monitor* 49 (Winter 2016): 2.

11. Mark A. Stokes, "The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398," *Project 2049 Institute*, July 27, 2015, 11; Peter Mattis, "China's Espionage against Taiwan (Part II): Chinese Intelligence Collectors," *Jamestown Foundation*, December 5, 2014; and Peter Mattis, "The Analytic Challenge of Understanding Chinese Intelligence Services," *Studies in Intelligence* 56:3 (September 2012): 52.

12. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of John Costello, June 9, 2016; Peter Mattis, "The Analytic Challenge of Understanding Chinese Intelligence Services," *Studies in Intelligence* 56:3 (September 2012): 53.

13. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of John Costello, June 9, 2016.

14. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of John Costello, June 9, 2016; John Costello, "The Strategic Support Force: China's Information Warfare Service," *Jamestown Foundation*, February 8, 2016.

15. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of John Costello, June 9, 2016.

16. Xinhua, "China Inaugurates PLA Rocket Force as Military Reform Deepens," January 1, 2016.

17. John Costello, "The Strategic Support Force: China's Information Warfare Service," *Jamestown Foundation*, February 8, 2016.

18. Kenneth Allen, Dennis J. Blasko, and John F. Corbett, "The PLA's New Organizational Structure: What Is Known, Unknown, and Speculation (Part 1)," *Jamestown Foundation*, February 4, 2016; Bill Gertz, "Chinese Military Revamps Cyber Warfare, Intelligence Forces," *Washington Free Beacon*, January 27, 2016; John Costello, "China Finally Centralizes Its Space, Cyber, Information Forces," *Diplomat* (Japan), January 20, 2016; and Bowen Press, "Former Intelligence Service Department Makes 'Last-Ditch Attempt' to Illegally Build Cases against Xi Jinping's Trusted Allies," January 17, 2016.

19. Xinhua, "China's Military Regrouped into Five PLA Theater Commands," February 1, 2016.

20. Zheng Zhidao, "General Commander Xi Jinping Inspects Central Military Commission Joint Operations Command Center – Mysterious Organization Pixelized in Recent News Program," *Guancha Zhe* (China), April 21, 2016; Wang Yinfang, "Gain Combat Strength through the Build-up of Command Capability," *PLA Daily* (China), April 7, 2016.

21. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Peter Mattis, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Mark Stokes, June 9, 2016.

22. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Mark Stokes, June 9, 2016; Mark Stokes and Russell Hsiao, "The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics," *Project 2049 Institute*, October 14, 2013, 3, 14–15.

23. Peter Mattis, "China's Espionage against Taiwan (Part II): Chinese Intelligence Collectors," *Jamestown Foundation*, December 5, 2014; Jason Pan, "Top Navy Brass Gets 14 Months in Prison for Spying for China," *Taipei Times*, October 3, 2014; Larry Wortzel, "The Chinese People's Liberation Army and Information Warfare," *U.S. Army War College Strategic Studies Institute*, March 5, 2014, 33; Mark Stokes and Russell Hsiao, "The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics," *Project 2049 Institute*, October 14, 2013, 3, 14–15; and Andrew Chubb and John Garnaut, "The Enigma of CEFC's Chairman Ye," *South Sea Conversations* (Blog), June 7, 2013.

24. Luisetta Mudie, "The Hard and Soft Faces of China's 'United Front' Work," *Radio Free Asia*, May 22, 2015; Peter Mattis, "China's Espionage against Taiwan (Part II): Chinese Intelligence Collectors," *Jamestown Foundation*, December 5, 2014; and Yimou Lee and Faith Hung, "Special Report: How China's Shadowy Agency Is Working to Absorb Taiwan," Reuters, November 26, 2014.

25. Peter Mattis, "China's Espionage against Taiwan (Part II): Chinese Intelligence Collectors," *Jamestown Foundation*, December 5, 2014; John Dotson, "Retired Taiwan Officer Exchanges Offer Insight into a Modern 'United Front,'" *Jamestown Foundation*, October 14, 2011; and U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress*, November 2009, 153.

26. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016.

27. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016; David Wise, *Tiger Trap: America's Secret Spy War with China*, Houghton Mifflin Harcourt Publishing Company, 2011, 220–226; Bill Gertz, "Chinese Spy Buy Caught on Surveillance Video," *Washington Times*, March 1, 2010; U.S. Department of Justice, *Defense Department Official Sentenced to 36 Months for Espionage, False Statement Charges*, January 22, 2010; Bill Gertz, "Chinese Spymaster Complains about News Leak," *Washington Times*, October 8, 2009; and U.S. Department of Justice, *Former Defense Department Official Sentenced to 57 Months in Prison for Espionage Violation*, July 11, 2008.

28. Peter Mattis, "China's New Intelligence War against the United States," *War on the Rocks* (Blog), July 22, 2015.

29. U.S. Department of Justice, *Michigan Man Sentenced 48 Months for Attempting to Spy for the People's Republic of China*, January 21, 2011.

30. Peter Mattis, "China's Espionage against Taiwan (Part II): Chinese Intelligence Collectors," *Jamestown Foundation*, December 5, 2014; Peter Mattis, "China's Espionage against Taiwan (Part I): Analysis of Recent Operations," *Jamestown Foundation*, November 7, 2014.

31. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of John Costello, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Mark Stokes, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016; and Peter Mattis, "China's New Intelligence War against the United States," *War on the Rocks* (Blog), July 22, 2015.

32. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of John Costello, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Mark Stokes, June 9, 2016; United States Senate Committee on Armed Services, *Worldwide Threat Assessment of the US Intelligence Community*, written testimony of James R. Clapper, February 9, 2016; U.S.-China Economic and Security Review Commission, *2015 Annual Report to Congress*, November 2015, 240–246; and Mark A. Stokes, "The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398," *Project 2049 Institute*, July 27, 2015, 8.

33. Wang Yinfang, "Gain Combat Strength through the Build-up of Command Capability," *PLA Daily* (China), April 7, 2016; Dong Xianwen and Luo Erwen, "System of Systems Operations: The Stirring Training Fields," *Zhongguo Kongjun* (China), January 1, 2013.

34. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016*, April 26, 2016, 62, 66, 90.

35. United States Senate Committee on Armed Services, *Hearing to Receive Testimony on Worldwide Threats*, oral testimony of James R. Clapper, February 9, 2016; Mark A. Stokes, "The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398," *Project 2049 Institute*, July 27, 2015, 11; and Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," February 2013.

36. Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, written testimony of James R. Clapper, February 9, 2016.

37. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016*, April 26, 2016, 64.

38. FireEye iSight Intelligence, "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," June 2016.

39. David E. Sanger, "Chinese Curb Cyberattacks on U.S. Interests, Report Finds," *New York Times*, June 20, 2016; U.S.-China Economic and Security Review Commission, private discussion with cybersecurity experts, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of John Costello, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Mark Stokes, June 9, 2016; and Jack Detsch, "Report: China Bolsters State Hacking Powers," *Christian Science Monitor*, February 4, 2016.

40. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016.

41. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of John Costello, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016.

42. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of John Costello, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Peter Mattis, June 9, 2016; and U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Mark Stokes, June 9, 2016.

43. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Mark Stokes, June 9, 2016.

44. Zheng Zhidao, "General Commander Xi Jinping Inspects Central Military Commission Joint Operations Center – Mysterious Organization Pixelized in Recent News Program," *Guancha Zhe* (China), April 21, 2016; Wang Yinfang, "Gain Combat Strength through the Build-up of Command Capability," *PLA Daily* (China), April 7, 2016; Peter Mattis, "China's Military Intelligence System Is Changing," *War on the Rocks*, December 29, 2015; and Dong Xianwen and Luo Erwen, "System of Systems Operations: The Stirring Training Fields," *Zhongguo Kongjun* (China), January 1, 2013.

45. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Peter Mattis, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016.

46. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016.

47. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016; United States Attorney's Office District of Hawaii, *Hawaii Man Pleads Guilty to Communicating Classified National Defense Information to an Unauthorized Person*, March 13, 2014; David Wise, "Mole-in-Training: How China Tried to Infiltrate the CIA," *Washingtonian*, June 7, 2012; and Justin McCurry, "Japan Says Diplomat's Suicide Followed Blackmail by China," *Guardian*, December 29, 2005.

48. William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, Routledge, 2013, 199.

49. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Peter Mattis, June 9, 2016.

50. Peter Mattis, Fellow, Jamestown Foundation, interview with Commission staff, September 15, 2016.

51. Peter Mattis, "Shriver Cases Highlights Traditional Chinese Espionage," *Jamestown Foundation*, November 5, 2010.

52. U.S. Department of Justice, *Michigan Man Pleads Guilty to Attempting to Spy for the People's Republic of China*, October 22, 2010.

53. U.S. Department of Justice, *Michigan Man Pleads Guilty to Attempting to Spy for the People's Republic of China*, October 22, 2010.

54. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Peter Mattis, June 9, 2016.

55. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016.

56. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of David Major, June 9, 2016.

57. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of David Major, June 9, 2016.

58. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016*, April 26, 2016, 64.

59. Wesley Bruer, "FBI Sees Chinese Involvement amid Sharp Rise in Economic Espionage Cases," CNN, July 24, 2015.

60. U.S.-China Economic and Security Review Commission, *Roundtable on U.S.-China Cybersecurity Issues,* testimony of James Mulvenon, July 11, 2013; U.S.-China Economic and Security Review Commission, *Roundtable on U.S.-China Cybersecurity Issues,* testimony of Roy Kamphausen, July 11, 2013.

61. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of David Major, June 9, 2016; Gina Chon, "FBI Blames China for 53% Spy Case Surge," *Financial Times*, July 23, 2015.

62. United States Senate Committee on Armed Services, *SASC Investigation Finds Chinese Intrusions into Key Defense Contractors*, September 17, 2014.

63. U.S. Department of Justice, *Hawaii Man Sentenced to 87 Months Imprisonment for Communicating Classified National Defense Information to Unauthorized Person*, September 17, 2014; United States Attorney's Office District of Hawaii, *Hawaii Man Pleads Guilty to Communicating Classified National Defense Information to an Unauthorized Person*, March 13, 2014.

64. U.S. Department of Justice, *Defense Department Official Sentenced to 36 Months for Espionage, False Statement Charges*, January 22, 2010.

65. *United States* v. *Fondren*, 09–5136 (4th Cir. 2011); U.S. Department of Justice, *Defense Department Official Sentenced to 36 Months for Espionage, False Statement Charges*, January 22, 2010.

66. U.S. Department of Justice, *Former Defense Department Official Sentenced to 57 Months in Prison for Espionage Violation*, July 11, 2008.

67. U.S. Department of Justice, *Former Defense Department Official Sentenced to 57 Months in Prison for Espionage Violation*, July 11, 2008.

68. U.S. Department of Justice, *Former Defense Department Official Sentenced to 57 Months in Prison for Espionage Violation*, July 11, 2008.

69. U.S. Department of Justice, *California Resident Convicted of Conspiring to Illegally Export Fighter Jet Engines and Unmanned Aerial Vehicle to China*, June 9, 2016.

70. U.S. Department of Justice, *Florida Woman Pleads Guilty to Acting as Illegal Agent of Foreign Government and Conspiring to Commit Money Laundering*, June 10, 2016.

71. U.S. Department of Justice, *Florida Woman Pleads Guilty to Acting as Illegal Agent of Foreign Government and Conspiring to Commit Money Laundering*, June 10, 2016; Wendell Minnick, "Details Emerge in Secretive Chinese Drone Case," *Defense News*, April 26, 2016; Julia Edwards, "U.S. Charges Woman for Exporting Underwater Drone Technology to China," Reuters, April 21, 2016; U.S. Department of Justice, *Florida Woman Charged in 18-Count Indictment for Conspiracy to Illegally Export Systems, Components, and Documents to China*, April 21, 2016; and *United States of America* v. *Amin Yu*, U.S. District Court, Middle District of Florida, March 16, 2016, indictment No. 6:16-cr-23-Orl-37GJK.

72. Wendell Minnick, "Chinese Businessman Pleads Guilty of Spying on F–35 and F–22," *Defense News*, March 24, 2016; U.S. Department of Justice, *Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information*, March 23, 2016.

73. U.S. Department of Justice, *Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison*, July 13, 2016.

74. U.S. Department of Justice, *FBI Employee Pleads Guilty to Acting in the United States as an Agent of the Chinese Government*, August 1, 2016.

75. U.S. Department of Justice, *FBI Employee Pleads Guilty to Acting in the United States as an Agent of the Chinese Government*, August 1, 2016.

76. U.S. Department of Justice, *FBI Employee Pleads Guilty to Acting in the United States as an Agent of the Chinese Government*, August 1, 2016.

77. Robert Windrem, "China Read Emails of Top U.S. Officials," NBC, August 10, 2015.

78. Robert Windrem, "China Read Emails of Top U.S. Officials," NBC, August 10, 2015.

79. Ellen Nakashima, "Chinese Government Has Arrested Hackers It Says Breached OPM Database," *Washington Post*, December 2, 2015; Mike Levine and Jack Date, "22 Million Affected by OPM Hack, Officials Say," ABC, July 9, 2015.

80. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of John Costello, June 9, 2016; Ellen Nakashima, "Chinese Government Has Arrested Hackers It Says Breached OPM Database," *Washington Post*, December 2, 2015.

81. Jason Miller, "OPM Finds Five-Fold Increase in Fingerprint Data Stolen during Data Hack," *Federal News Radio*, September 23, 2015; Jose Pagliery, "OPM Hack's Unprecedented Haul: 1.1 Million Fingerprints," CNN, July 10, 2015.

82. Robert Windrem, "China Read Emails of Top U.S. Officials," NBC, August 10, 2015.

83. Deb Riechmann, "US Intelligence: Foreign Hackers Spying on Campaigns," Associated Press, May 18, 2016.

84. David E. Sanger and Eric Schmitt, "Spy Agency Consensus Grows that Russia Hacked D.N.C.," *New York Times*, July 26, 2016; Deb Riechmann, "US Intelligence: Foreign Hackers Spying on Campaigns," Associated Press, May 18, 2016.

85. BBC, "US Presidential Campaigns 'Hacked,' Top Intelligence Chief Warns," May 18, 2016; Michael Isikoff, "Chinese Hacked Obama, McCain Campaigns, Took In-

ternal Documents, Officials Say," NBC, June 6, 2013; and William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, Routledge, 2013, 224.

86. Robert Windrem, "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets," NBC, July 30, 2015; House Permanent Select Committee on Intelligence, *Hearing on Cybersecurity Threats: The Way Forward*, oral testimony of Michael Rogers, November 20, 2014.

87. U.S. Department of Homeland Security, *Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*, 2013, 8–9.

88. House Permanent Select Committee on Intelligence, *Hearing on Cybersecurity Threats: The Way Forward*, oral testimony of Michael Rogers, November 20, 2014.

89. Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, Simon & Schuster, 2016, 4–5; Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, April 8, 2009.

90. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of David Major, June 9, 2016.

91. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of David Major, June 9, 2016.

92. U.S.-China Economic and Security Review Commission, meeting with scholar, Taipei, Taiwan, June 22, 2016; U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016*, April 26, 2016, 87–91; and Yen-fan Liao and Michael Thim, "Defense of Taiwan Post-2016 Elections: Legacy and New Challenges of Military Transformation," *Jamestown Foundation*, January 12, 2016.

93. Ian Easton, "Taiwan's Transition is a Strategic Opportunity for the United States," *Diplomat* (Japan), May 17, 2016; Mark Stokes and Sabrina Tsai, "The United States and Future Policy Options in the Taiwan Strait," *Project 2049 Institute*, February 1, 2016, 3.

94. F-Secure, "Nanhaishu: RATing the South China Sea," July 12, 2016.

95. Tony Morbin, "Norway Officially Accuses China of Stealing Military Secrets," *SC Magazine*, February 26, 2016.

96. Linton Besser, Jake Sturmer, and Ben Sveen, "Government Computer Networks Breached in Cyber Attacks as Experts Warn of Espionage Threat," Australian Broadcasting Corporation, August 29, 2016; Chris Uhlmann, "China Blamed for 'Massive' Cyber Attack on Bureau of Meteorology Computer," Australian Broadcasting Corporation, December 1, 2015.

97. Agence France-Presse, "Japan Sees 25 Billion Cyber Attacks in 2014: Agency," February 17, 2015; Reuters, "Japan Cyber Attacks on Government Sites Surge, Government Mulling Steps to Respond," July 10, 2014; and *Telegraph*, "Japan Parliament Hit by China-Based Cyber Attack," October 25, 2011.

98. Agence France-Presse, "Japan Sees 25 Billion Cyber Attacks in 2014: Agency," February 17, 2015.

99. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of David Major, June 9, 2016; Peter Mattis, "China's Espionage against Taiwan (Part I): Analysis of Recent Operations," *Jamestown Foundation*, November 7, 2014.

100. U.S. Department of Justice, *FBI Employee Pleads Guilty to Acting in the United States as an Agent of the Chinese Government*, August 1, 2016.

101. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Peter Mattis, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of David Major, June 9, 2016.

102. White House Office of the Press Secretary, *Fact Sheet: President Xi Jinping's State Visit to the United States*, September 25, 2015.

103. Wesley Bruer, "FBI Sees Chinese Involvement amid Sharp Rise in Economic Espionage Cases," CNN, July 24, 2015.

104. David E. Sanger, "In Cyberspace, New Cold War," *New York Times*, February 24, 2013; William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, Routledge, 2013, 205–206.

105. Eric Holder, "Attorney General Eric Holder Speaks at the Administration Trade Secret Strategy Rollout" (Launch of the Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets, Washington, DC, February 20, 2013).

106. Eric Holder, "Attorney General Eric Holder Speaks at the Administration Trade Secret Strategy Rollout" (Launch of the Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets, Washington, DC, February 20, 2013).
107. Office of the Director of National Intelligence, *National Counterintelligence Strategy of the United States of America 2016*, 2016, 1.
108. Office of the Director of National Intelligence, *National Counterintelligence Strategy of the United States of America 2016*, 2016, 7.
109. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of David Major, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Michelle Van Cleave, June 9, 2016; and Intelligence Authorization Act for Fiscal Year 2003, Pub. L. No. 107–306, 116 STAT. 2432 (2002), codified at 50 USC § 402b (2002).
110. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Michelle Van Cleave, June 9, 2016.
111. U.S. Federal Register, *Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services*, 81 FR 81472–81474.
112. White House Office of the Press Secretary, *Executive Order: Commission on Enhancing National Cybersecurity*, February 9, 2016.
113. White House Office of the Press Secretary, *Executive Order: Commission on Enhancing National Cybersecurity*, February 9, 2016.
114. U.S. Federal Register, *Information on Current and Future States of Cybersecurity in the Digital Economy*, 81 FR 52827–52829.
115. U.S. Federal Register, *Federal Acquisition Regulation; Basic Safeguarding of Contractor Information Systems*, 81 FR 30439–30447.
116. White House Office of the Press Secretary, *Fact Sheet: Cybersecurity National Action Plan*, February 9, 2016.
117. White House Office of the Press Secretary, *Presidential Policy Directive: United States Cyber Incident Coordination*, July 26, 2016.
118. Ellen Nakashima, "In a Major Cyber-Hack, Whom Do You Call? The White House Spells It Out," *Washington Post*, July 26, 2016; White House Office of the Press Secretary, *Presidential Policy Directive: United States Cyber Incident Coordination*, July 26, 2016.
119. Hayley Tsukayama and Dan Lamothe, "How an Email Sparked a Squabble over Chinese-Owned Lenovo's Role at Pentagon," *Washington Post*, April 22, 2016.
120. Hayley Tsukayama and Dan Lamothe, "How an Email Sparked a Squabble over Chinese-Owned Lenovo's Role at Pentagon," *Washington Post*, April 22, 2016.
121. *Telegraph*, "From GCHQ to Google: The Battle to Outpace Hackers in the Cyber Race," July 11, 2016; Kenna Security, "Companies Leave Vulnerabilities Unpatched for up to 120 Days, Kenna Security Finds," September 29, 2015.
122. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of John Costello, June 9, 2016; U.S.-China Economic and Security Review Commission, private discussion with cybersecurity experts, June 9, 2016; and Bree Feng, "Among Snowden Leaks, Details of Chinese Cyberespionage," *Sinosphere* (*New York Times* Blog), January 20, 2015.
123. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of David Major, June 9, 2016.
124. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of David Major, June 9, 2016; Ralph Jennings, "Taiwan Readies for Fresh Wave of Espionage by China," *Voice of America*, April 28, 2016.
125. U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, written testimony of Peter Mattis, June 9, 2016; U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of Mark Stokes, June 9, 2016; and U.S.-China Economic and Security Review Commission, *Hearing on Chinese Intelligence Services and Espionage Operations*, oral testimony of David Major, June 9, 2016.