SECTION 2: CHINA'S CYBER CAPABILITIES: WARFARE, ESPIONAGE, AND IMPLICATIONS FOR THE UNITED STATES

Abstract

China has engaged in a massive buildup of its cyber capabilities over the past decade and poses a formidable threat to the United States in cyberspace today. The country has achieved this transformation by reorganizing its cyber policymaking institutions, developing sophisticated offensive cyber capabilities, and perpetrating cyberespionage to steal foreign intellectual property at industrial scale. China has also played by a different set of rules than the United States in cyberspace, mandating that civilian companies and researchers report software vulnerabilities they discover to the Chinese government prior to public notification and promoting its "cyber sovereignty" norm in contrast to widely held principles of a free and open global internet. As a result of these long-running efforts, China's activities in cyberspace are now more stealthy, agile, and dangerous to the United States than they were in the past. Urgent questions remain concerning the United States' readiness for the China cyber challenge, including the adequacy of resourcing for U.S. military cyber forces, the sufficiency of existing protections for U.S. critical infrastructure, and the scope of public-private cybersecurity cooperation.

Key Findings

- China's cyber operations pose a serious threat to U.S. government, business, and critical infrastructure networks in the new and highly competitive cyber domain. Under General Secretary of the Chinese Communist Party (CCP) Xi Jinping, the country's leaders have consistently expressed their intention to become a "cyber superpower." China has developed formidable offensive cyber capabilities over the past decade and is now a world leader in vulnerability exploitation. As a result, China's activities in cyberspace constitute a fundamentally different, more complex, and more urgent challenge to the United States today than they did a decade ago.
- China enjoys an asymmetric advantage over the United States in cyberspace due to the CCP's unwillingness to play by the same rules, reflecting a dynamic observable in other areas of U.S.-China relations. The United States and China diverge sharply on the norms that should guide responsible state behavior in cyberspace during peacetime. The main points of contention are China's perpetration of cyberespionage for illegitimate economic advantage, its emphasis on state control over the internet under the guise of cyber sovereignty, and its op-

position to the application of certain principles of international law in the cyber domain. China promotes its preferred norms in existing international and regional institutions and is creating new organizations to supplant existing cyber governance mechanisms in line with its vision for the internet.

- The People's Liberation Army (PLA) views cyberspace operations as an important component of information warfare in concert with space, electronic, and psychological warfare capabilities. The Strategic Support Force (SSF) is at the forefront of China's strategic cyberwarfare operations and plans to target both U.S. military assets and critical infrastructure in a crisis or in wartime.
- China's cyberespionage activities are increasingly sophisticated and use advanced tactics, techniques, and procedures (TTPs) such as vulnerability exploitation and third-party compromise to infiltrate victims' networks. China's premier spy agency, the Ministry of State Security (MSS), conducts most global cyberespionage operations and targets political, economic, and personally identifiable information to achieve China's strategic objectives.
- Military-civil fusion underpins China's development of cyber capabilities and conduct of cyber operations. To advance China's military aims, the SSF can mobilize civilian information technology (IT) resources, such as data centers, as well as militias composed of technically competent civilians working in the domestic telecommunications industry, cybersecurity firms, and academia. For its cyberespionage operations, the MSS exploits vulnerabilities submitted to the Chinese government and often employs contractors to carry out state-sponsored cyber operations.
- China's cybersecurity legislation weaponizes the country's cybersecurity industry and research by requiring companies and researchers to submit all discovered software and hardware vulnerabilities to the government before providing them to the vendors that can patch them. This policy, leveraged in combination with domestic hacking competitions and cooperative agreements with Chinese universities, provides China's security services with a steady stream of vulnerabilities to exploit for state-sponsored operations.

Recommendations

- Congress direct the Office of the U.S. Trade Representative to create an updateable list of Chinese firms operating in critical sectors and found to have benefited from coercive intellectual property transfer, including theft. Such a list would enable the U.S. Department of the Treasury to ban investment in and the U.S. Department of Commerce to deny export licenses to these firms and related parties for a rolling period of five years to prevent Chinese beneficiaries from further gaining from U.S. intellectual property loss. If additional authorities are needed, such requests should be made to Congress on an expedited basis.

- Congress direct the U.S. Department of Homeland Security to catalog Chinese-sourced surveillance equipment, first responder communication systems, and smart cities systems used by state and local governments. The Department of Homeland Security shall further identify:
  - Levels of risk from these systems as a result of foreign interference or malicious cyber activity;
  - Plans to remove and replace such equipment to protect U.S. interests; and
  - The necessary resources to implement these plans.
- Congress pass legislation codifying the concept of "systemically important critical infrastructure" (SICI) and requiring SICI-designated entities, defense contractors, and recipients of federal funding for research and development of sensitive and emerging technologies to undertake enhanced hardening and mitigation efforts against cyberattacks. These efforts shall follow cybersecurity standards and guidance as determined by the U.S. Department of Defense and Cybersecurity and Infrastructure Security Agency. Congress should provide appropriate legal liability "safe harbor" provisions to compliant SICI operators and appropriate support as necessary for SICI-designated small- and medium-sized companies to address the cost of compliance. Such legislation would also require that cybersecurity risk mitigation plans be a condition for the Small Business Administration (SBA) to award grants such as those under the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs. As part of the regular audit process, SBA and any relevant agencies should ensure implementation of these plans and require certification of compliance.
- Congress direct the U.S. Secretary of the Treasury to prohibit investment in and other financial transactions with any Chinese entities that have been involved in cyber-enabled intelligence collection or theft of intellectual property sponsored by the People's Republic of China against U.S.-based persons or organizations under authorities pursuant to Executive Order 13694 on "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (amended as EO 13757), including any individuals, research institutes, universities, and companies that have been affiliated with Chinese state-sponsored advanced persistent threat (APT) groups or served as contractors for China's Ministry of State Security or People's Liberation Army.

Introduction

In early March 2021, U.S. technology corporation Microsoft publicly disclosed that a Chinese state-sponsored threat actor called HAFNIUM had exploited multiple previously unknown vulnerabilities in its Exchange email server software to attack customer networks.[1] The intrusions left a door wide open to tens of thousands of vulnerable email servers that had not yet implemented Microsoft's patch, allowing hackers unaffiliated with HAFNIUM to opportunistically

infiltrate organizations ranging from municipal governments and small businesses to healthcare providers and manufacturers.[2] Cybersecurity experts estimated that the systems of at least 30,000 victims in the United States and up to 250,000 victims worldwide had been compromised within a matter of days.[3] Four months later, the United States and a coalition of allies* released an unprecedented joint statement attributing the initial breach by HAFNIUM to hackers affiliated with the MSS.[4] China's "pattern of irresponsible behavior in cyberspace is inconsistent with its stated objective of being seen as a responsible leader in the world," the statement said, highlighting the "major" threat Chinese state-sponsored cyber operations pose to U.S. and allied security.[5]

The Microsoft Exchange hack, while historic in scale, is just one of many high-profile Chinese cyberattacks in recent years that reflect the country's ongoing efforts to transform itself into a "cyber superpower." Whereas a decade ago U.S. analysts ridiculed Chinese state-sponsored cyber operations for their simplicity and sloppiness, Beijing's cyber operators today make use of advanced tactics such as vulnerability exploitation† and third-party compromise‡ to subtly, effectively, and extensively infiltrate victims' networks.[6] In its 2022 *Global Threat Report*, U.S. cybersecurity firm CrowdStrike assessed that China is a global leader in vulnerability exploitation, highlighting the substantial exploitation development talent within China's domestic hacker community.[7] The astounding improvement in Chinese cyber capabilities since 2013 is the product of sustained attention at the highest levels of China's political leadership, major reorganizations of its cyber-related institutions, and substantial investments in its future cybersecurity workforce. The United States faces potentially formidable challenges both in contesting China's daily cyber intrusions and in defending itself against China's offensive cyber operations during a high-end conflict.

This section assesses China's military and espionage activities in cyberspace as well as its efforts to increase its influence in global internet governance. First, the section examines the Chinese leadership's view of cyberspace as a strategic domain and its efforts to reorganize the country's cyber institutions to improve offense, defense, and intelligence collection capabilities. Next, it explores the role of cyber capabilities in Chinese doctrinal concepts of information warfare and how the SSF may execute cyberwarfare missions during a crisis or conflict. It then discusses the targets and scale of Chinese state-sponsored cyberespionage, focusing on the MSS and

---

*The coalition included the "Five Eyes" nations (Australia, Canada, New Zealand, the United Kingdom, and the United States), Japan, the EU, and NATO, and the announcement marked the first time the transatlantic alliance had condemned China's cyber activities. Martin Matishak, "White House Formally Blames China's Ministry of State Security for Microsoft Exchange Hack," *The Record*, July 19, 2021.

†Vulnerability exploitation occurs when an actor exploits flaws or vulnerabilities in software or hardware to infiltrate it for malicious purposes, such as gaining unauthorized access to a device, sabotaging a device, or executing the attacker's commands. A zero-day vulnerability is a flaw in software or hardware that is discovered before its existence becomes known to the party responsible for patching the flaw. An "n-day vulnerability" is a vulnerability that vendors have disclosed and patched. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–3.

‡Third-party compromise involves an intrusion that abuses a trusted channel, such as that between a service provider and a client. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4.

its extensive use of contractors. Finally, the section evaluates China's increasingly vigorous advocacy for its own cyber norms in international institutions. This section is based on the Commission's February 2022 hearing on the topic as well as open source research and analysis.

Defining Cyberwarfare and Cyberespionage

Academics, journalists, and members of the public often use the term "cyberwarfare" to describe how states such as China use computers and computer networks to cause harm, launch cyberattacks, or complement conventional forms of warfare waged against an adversary.* [8] There is also no widely accepted definition of "cyberwar," but many definitions emphasize the disruption or destruction of an adversary's military assets, government infrastructure, or civilian infrastructure to achieve strategic purposes.[9] Some analysts further distinguish between "operational cyberwar," which refers to wartime cyberattacks against military targets to degrade an adversary's means of fighting, and "strategic cyberwar," or cyberattacks launched against an adversary and its society to influence its will, behavior, and policy choices in peacetime or in wartime.[10] Militaries tend to use the term "information warfare," rather than cyberwarfare, to describe how they leverage cyberspace capabilities in concert with other "information-related capabilities" to accomplish military objectives.† [11]

By contrast, cyberespionage is the act of obtaining access to data from a computer system for intelligence collection purposes without the authorization of that system's owner.‡ [12] Cyberespionage may clandestinely surveil an organization's networks and exfiltrate data for economic gain, competitive advantage, political reasons, or military reasons.[13] Cyberespionage is typically carried out by the militaries or intelligence services of nation-states against foreign government, commercial, or academic targets, but independent contractors (or "hackers for hire") may also participate in state-sponsored cyberespionage.[14] Cyberespionage eliminates some of the risk associated with traditional espionage techniques, enables greater geographic reach, and massively increases the quantity of information that can be collected at a given time.[15]

*A "cyberattack" is an attack, carried out via cyberspace, that targets an organization's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure. National Institute of Standards and Technology, *Computer Security Resource Center*, *Cyberattack*.

†Examples of information-related capabilities include cyberspace operations, military information support operations (MISO), military deception operations, civil affairs operations, and electronic warfare. U.S. Department of the Army, *The Conduct of Information Operations* (ATP 3-13.1), October 4, 2018, 1-1.

‡The U.S. Department of Defense previously used the term "computer network operations" (CNO) to refer to computer network attack (CNA), computer network defense (CND), and related computer network exploitation enabling operations (CNE). CNE describes how computer networks can be used to gather data from a target's system for intelligence collection and is used as a shorthand for cyberespionage. Catherine A. Theohary, "Information Warfare: Issues for Congress," *Congressional Research Service*, March 5, 2018, 3; *National Institute of Standards and Technology,* Computer Security Resource Center, *Computer Network Exploitation (CNE)*.

Key Ideas Driving China's Cyberspace Activities

General Secretary Xi has emphasized that CCP officials implementing cyber policies must hold the "correct" view of cyberspace because "ideas determine actions."[16] Central elements of the Chinese government's official view on cyberspace include China's aspiration for cyber superpower status, the primacy of national security, and cyberspace as a venue for international strategic competition.

Aspiring to Become a Cyber Superpower

The phrase "cyber superpower" is both a political slogan and a unifying strategic concept linking cyber initiatives across sectors.[17] As a slogan invoked frequently by Xi, cyber superpower describes a goal to achieve parity with major powers like the United States in terms of cyber capability and influence on global internet governance.[18] It reflects what researchers at the New America Foundation call "an almost grandiose level of ambition attached to Chinese government and Communist Party plans and development in cyberspace fields."[19] As a unifying strategic concept, cyber superpower encompasses specific plans and initiatives related to domestic information control, national security, indigenous innovation in core technologies, the digital economy, and China's influence in global cyber governance.[20] The phrase appears in high-level policy documents like China's 14th Five-Year Plan and has been incorporated into regulatory processes at the Party, ministerial, provincial, and municipal levels of government.[21]

Controlling Cyberspace to Protect National Security

CCP officials believe that left uncontrolled, cyberspace poses grave challenges to their rule and to China's national security.[22] Xi has repeatedly emphasized this concern by declaring, "Without cybersecurity, there is no national security."[23] He and theorists from the Cyberspace Administration of China (CAC) have also publicly assessed, "If our Party cannot traverse the hurdle represented by the Internet, it cannot traverse the hurdle of remaining in power for the long term."[24]

In the CCP's view, several basic risks stem from cyberspace that must be managed differently. One type of risk is cyber operations perpetrated by foreign adversaries that undermine political and social stability by injecting information the CCP regards as threatening into the Chinese information space.[25] Likening subversive ideas conveyed through cyberspace to gunpowder, Xi has stated that "the Internet is at the forefront of the current ideological struggle" and directed his subordinates to maintain "online ideological security" through a mix of censorship and propaganda.[26] Similarly, the CCP is concerned about the transmission of negative information about the Party or its policies that could incite the Chinese public to organize against it.[27] For example, the CCP swiftly censored social media posts shared by Shanghai residents describing the dire conditions created by authorities' lockdown of the city in the spring of 2022, even denying citizens' allegations of loved ones dying after struggling to access medical care or starving amid food shortages.[28] Another type of risk is foreign adversary cyber operations that disrupt, damage, or destroy computers, networks, critical infrastruc-

ture, or data the Chinese government regards as important.[29] Xi has argued that mitigating these threats requires increased cyber defense, attribution, and incident response capabilities.[30] He has also called for new cyber threat information-sharing mechanisms and new cybersecurity standards, among other measures.[31]

Shaping the Competitive Strategic Domain of Cyberspace in China's Favor

Top Chinese leaders view cyberspace as an arena of fierce strategic competition between countries that China must shape in its favor.[32] Xi has stated that a country's ability to master the internet determines its rise or fall and that "those who win the internet win the world."[33] He has also expressed the concern that China lags behind the world's most advanced cyber powers and called for accelerating efforts to enhance its strategic influence in cyberspace.[34] China's 2016 *National Cyberspace Security Strategy* sums up these efforts in nine "strategic tasks" underscoring the multidimensional way in which Chinese leaders aspire to shape cyberspace within and beyond their borders (see Table 1).[35]

Table 1: Strategic Tasks Outlined in China's 2016 *National Cyberspace Security Strategy*

No.	Strategic Task	Summary
1	Defend cyberspace sovereignty	Uphold China's sovereignty in cyberspace by managing domestic online activities, protecting domestic IT infrastructure, and "resolutely oppos[ing] all actions to subvert our country's national regime" through IT networks.
2	Safeguard national security	Prevent, curb, and punish any acts that use IT networks to engage in treason, separatism, subversion of the CCP, or the theft or leakage of state secrets.
3	Protect critical information infrastructure*	Protect critical information infrastructure and the data it contains from attacks and destruction. Strengthen risk assessment and information-sharing mechanisms pertinent to critical information infrastructure.
4	Strengthen online culture	Use the internet to disseminate socialist values, promote "positive energy,"† prevent the spread of harmful information, and foster traditional Chinese culture.
5	Combat cyberterrorism and crime	Prevent the use of the internet for terrorism, espionage, fraud, drug trafficking, hacking, invasion of citizens' privacy, infringement of intellectual property (IP) rights, dissemination of obscene or sexual materials, or other unlawful activities.

*The strategy defines critical information infrastructure as IT infrastructure that "affects national security, the national economy and the people's livelihood." Sectors involving what the Chinese government considers critical information infrastructure include telecommunications, energy, finance, transportation, education, scientific research, hydropower, manufacturing, and healthcare. Cyberspace Administration of China, *National Cyberspace Security Strategy*, December 27, 2016. Translated by China Copyright and Media.

†"Positive energy" is a propaganda term the CCP uses to describe the need for messages that are uplifting and portray the Party in a flattering light. *China Media Project*, "Positive Energy," April 16, 2021.

Table 1: Strategic Tasks Outlined in China's 2016 *National Cyberspace Security Strategy—Continued*

No.	Strategic Task	Summary
6	Improve cyber governance	Promulgate and enforce domestic cybersecurity laws and regulations. Interpret and revise existing laws to make them suitable for cyberspace.
7	Reinforce the foundation of cybersecurity	Encourage technological innovation. Support the growth of cybersecurity enterprises, promote the cybersecurity industrial base, and increase the talent pool of cybersecurity professionals.
8	Enhance cyberspace defense capabilities	Build cyber forces "commensurate with our country's international standing and suited to a strong cyber power." Invest in cyber detection and defense.
9	Strengthen international cooperation	Reform the global cyber governance system, promote norms acceptable to all countries, and support the leading role of the UN in cyber governance decision-making. Internationalize the management of internet resources. Craft an international treaty on cyberterrorism. Disseminate internet technology globally.

Source: Cyberspace Administration of China, *National Cyberspace Security Strategy*, December 27, 2016. Translated by China Copyright and Media.

Under General Secretary Xi, China Overhauls Its Domestic Cybersecurity Ecosystem

In a series of internal speeches and meetings from 2013 onward, top CCP officials called attention to foreign and domestic challenges in cyberspace that demanded an urgent policy response. The discovery of the Stuxnet computer worm in 2010 and Edward Snowden's allegations of U.S. government surveillance activities in 2013 likely contributed to concern within the CCP that it was highly vulnerable to U.S. intelligence collection.[36] China's dependence on U.S. and European IT hardware and software exacerbated fears that foreign technology could be exploited or choked off in a crisis.*[37] China's critical infrastructure, which top leaders viewed as the "nerve center of economic and social operation," was extremely vulnerable to disruptive cyberattacks.[38] Moreover, cyberspace offered a channel through which China's enemies could transmit subversive ideas to undermine internal stability, and China had limited influence on the global institutions that shaped cyberspace norms.[39] China's own cyber policymaking process was fragmented, opaque, and dominated by bureaucratic turf wars, giving rise to a situation that state media under General Secretary Xi characterized as "nine dragons managing the flood."[40]

To resolve these challenges, the CCP embarked on a sweeping reorganization of its cyber governance system around new ideas, in-

*For example, Chinese users were outraged when Microsoft decided to end technical support for the Windows XP operating system in 2014. At the time, more than 70 percent of Chinese personal computers ran the operating system. A poll conducted six years prior on the Chinese digital platform QQ found that 73 percent of respondents said they were using pirated versions of XP. Steven Millward, "Support for Windows XP Is Over, but China Still Has 200 Million PCs Using It," *Tech in Asia*, April 9, 2014; Ma Yujia, Pang Li, and Keen Zhang, "Microsoft Accused of Hacking Attack," *China Internet Information Center*, October 21, 2008.

stitutions, and laws.[41] Xi personally led the new system through his role as chair of the Central Cybersecurity and Informationization Leading Small Group, a body he established in 2014 and ultimately elevated to a Central Commission for Cybersecurity and Informationization (CCCI) in 2018.[42] This top-down design streamlined the policymaking process, enabling Beijing to wield its new cyber governance system for expeditious and far-reaching changes to its military, espionage, and diplomatic activities in cyberspace.[43] (For more on Xi's centralization of China's bureaucracy through Party leading small groups and commissions, see Chapter 1, "CCP Decision-Making and Xi Jinping's Centralization of Authority").

China Streamlines Its Cyber Institutions

China's cyber governance system today reflects Xi's decade-long efforts to centralize and optimize the policymaking process for cyberspace around several key institutions. Prior to 2014, responsibility for various cyber-related tasks was fragmented across the Ministry of Public Security (MPS), the Ministry of Industry and Information Technology (MIIT), the Ministry of Propaganda, the PLA, and the intelligence services.[44] Now, the cyber governance system is led from the top by Xi through his chairmanship of the CCCI.[45] The CCCI coordinates and oversees the cyber-related activities of numerous Party and state bodies, technical entities, and industry associations (see Figure 1).

New Legal Measures Advance Cybersecurity Standards and Cyberespionage

China has enacted dozens of laws, regulations, and technical standards related to cybersecurity since 2013 (see Appendix I). Taken collectively, these measures strengthen the Chinese government's ability to monitor and control cyberspace in numerous areas, from cross-border data flows to the software and hardware underpinning industrial control systems.[46] Adam Kozy, CEO and founder of the boutique consulting firm SinaCyber, testified before the Commission that China's legal system also gives the intelligence services "unfettered access to Chinese firms" and allows them to "cherry pick high value vulnerabilities, which can be turned into exploits for use in cyberespionage campaigns."[47] China's 2017 Cybersecurity Law and recent regulations on vulnerability disclosure illustrate how Chinese laws and regulations may facilitate cyberespionage in tandem with legitimate efforts to defend the Chinese public and businesses from malicious cyberattacks.

The Cybersecurity Law imposes new security requirements on all China-based operators of networks and critical information infrastructure, representing a major effort by the Chinese government to better protect systems and information it deems essential to national security.*[48] Under the Cybersecurity Law, network operators must maintain network security protections, backups of important data, and encryption in addition to formulating and implementing emergency response plans for cybersecurity incidents.[49]

*"Network operators" is a broad term referring to any entity that owns or administers a network or provides network services. Traditional telecommunications operators, internet firms, financial institutions, providers of cybersecurity products and services, and enterprises that have websites and provide network services all conceivably fall within the definition of a network operator. Susan Ning and Han Wu, "Cybersecurity 2022," *Chambers and Partners*, March 17, 2022; KPMG China IT Advisory, "Overview of China's Cybersecurity Law," February 2017, 9.

Operators of critical information infrastructure must also meet a stringent set of cybersecurity standards, such as regular risk reviews as well as mandatory testing and certification of computer equipment.[51] Notably, the Cybersecurity Law requires network operators to store some types of data domestically* and cooperate with China's law enforcement and security services upon request.[52] Violations of the law may lead to stiff penalties, ranging from fines to the suspension of business activities.[53] These provisions, together with the law's vague language, have prompted some observers to argue that the Cybersecurity Law facilitates government censorship, surveillance, and theft of foreign IP.[54] Since taking effect in 2017, the Cybersecurity Law has become the legislative centerpiece from which more granular cybersecurity regulations flow.[55]

In a similar vein, China's 2021 Regulations on the Management of Security Vulnerabilities in Network Products require vendors and individuals to report all discovered software and hardware vulnerabilities to the MIIT within two days.†[56] The regulations obligate vendors to promptly patch known vulnerabilities, prohibit the public disclosure of vulnerabilities until they are assessed by Chinese authorities, and restrict sharing vulnerabilities with anyone overseas unless the affected vendor itself is based overseas.[57] "The Chinese government, therefore, is to be given access to information on vulnerabilities before any other interested party," China cybersecurity researchers Devin Thorne and Samantha Hoffman wrote in a 2021 analysis.[58] "There's also a real likelihood that the regulations will facilitate China's cyber espionage efforts opportunistically in the gaps between reporting, patching and disclosure."[59] Dakota Cary, a former research analyst at Georgetown University's Center for Security and Emerging Technology, agreed in testimony before the Commission, noting that such a policy "effectively weaponizes the cybersecurity researcher ecosystem in China."[60]

Workforce and Education Policies Invest in China's Future Cyber Power

China faces a deficit of about 1.4 million skilled cybersecurity professionals.[61] CAC deputy director Zhao Zeliang told state media in 2018 that the country has "more than 751 million netizens, but only produces around 8,000 cybersecurity graduates every year."[62] A 2019 report commissioned for the China Information Technology Security Evaluation Center (CNITSEC), also known as the MSS's 13th bureau, confirmed that Chinese cybersecurity professionals are in short supply and found that many handle additional tasks unrelated to cybersecurity in the course of their day jobs.[63] Likening the deficit to a "stubborn disease," Chinese experts predict that the

*Article 37 of the Cybersecurity Law requires that "critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China." It is unclear what types of personal and business data the Chinese government regards as "important." Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina,* June 29, 2018.

†More specifically, the regulations apply to "network product vendors" (potentially any developer of network hardware or software, including servers, web applications, and websites) that operate in China, including Chinese companies with an international footprint and foreign companies with operations in China. Devin Thorne and Samantha Hoffman, "China's Vulnerability Disclosure Regulations Put State Security First," *Australian Strategic Policy Institute*, August 31, 2021.

Figure 1: Selected Key Institutions in China's Cybersecurity Ecosystem

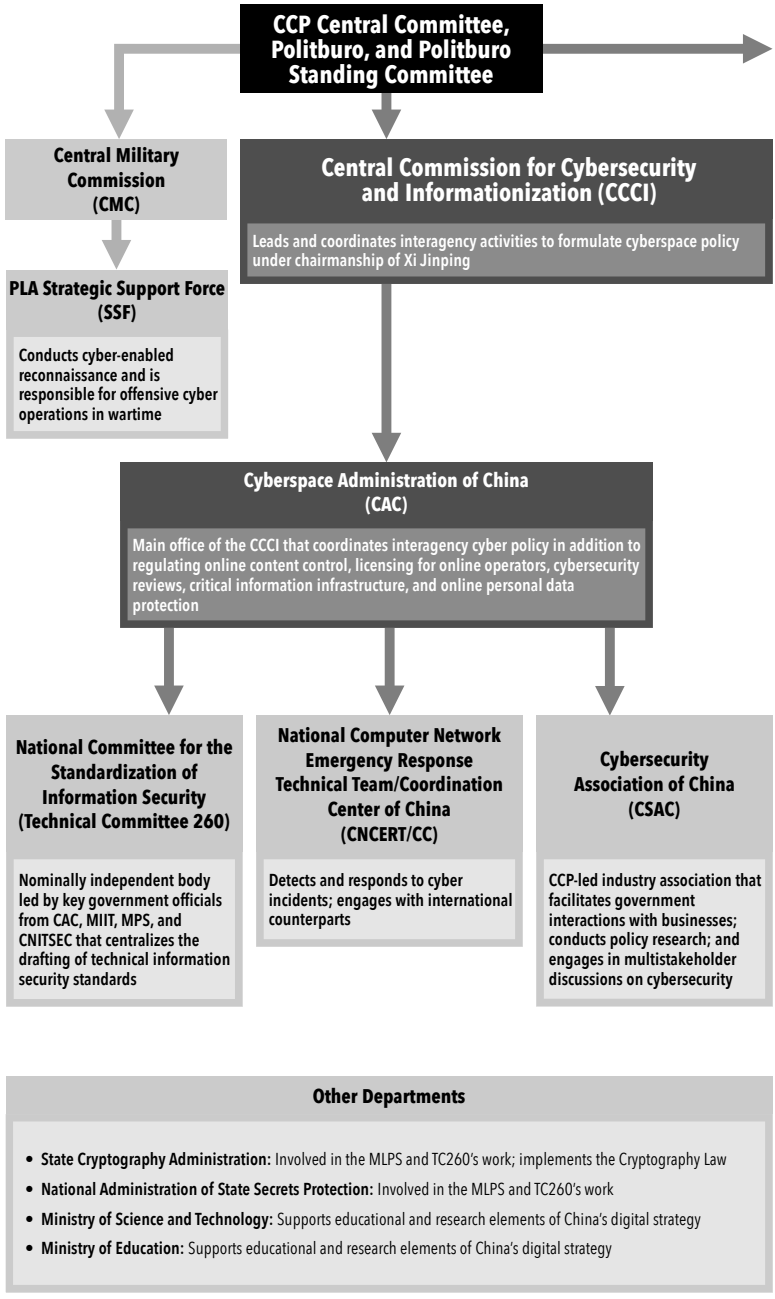
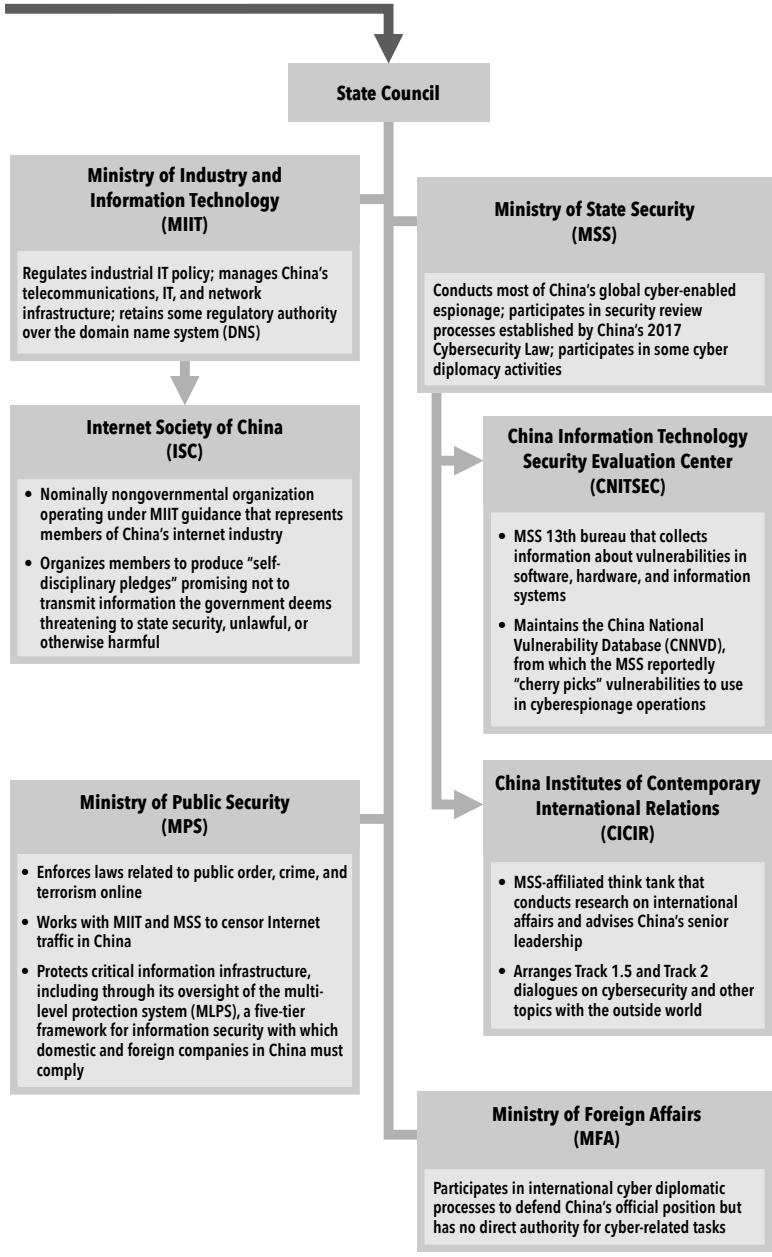


Figure 1: Selected Key Institutions in China's Cybersecurity Ecosystem—*Continued*



Note: This graphic displays a selection of key institutions in China's cybersecurity ecosystem; it is not exhaustive.
Source: Various.[50]

personnel shortage will be exacerbated in the future by growing demand for cybersecurity talent as society more widely adopts IT.[64]

The Chinese government has accordingly unveiled a raft of workforce development and education policies in recent years to grow the domestic talent pool of cyber operators on an expedited timeline.[65] It has also identified a number of "strategic tasks" required to build its cybersecurity innovation base in documents such as the 2016 *National Cyberspace Security Strategy*.[66] The strategy calls for strengthening academic education in information security by standardizing cybersecurity degree programs and "forg[ing] first-rate cybersecurity academies."[67] The establishment of a cybersecurity school at the new Wuhan-based National Cybersecurity Center, which aspires to produce more than 2,500 graduates annually, exemplifies this high-level push to build more high-quality cybersecurity institutions.[68] CAC and the Ministry of Education announced plans in 2017 to build four to six "world-famous" cybersecurity schools between 2017 and 2027.[69]

The Chinese government has also set standards for degree accreditation and created a cybersecurity skill certification system. In 2017, Beijing launched a program to certify academic institutions as World-Class Cybersecurity Schools, a designation similar to Centers of Academic Excellence programs in U.S. universities.*[70] According to Mr. Cary, China has fashioned other components of its certification regime after U.S. models as well.[71] For example, Chinese universities offering cybersecurity degree programs have implemented standards criteria based on those devised by the National Initiative for Cybersecurity Education, a branch of the U.S. National Institute of Standards and Technology, to measure the quality of curricula and set performance benchmarks.[72]

China's Way of Cyberwarfare

China's views on the military use of cyberspace are rooted in its leadership's conviction that the Gulf War (1990–1991) transformed the nature of modern warfare.[73] Senior Chinese military leaders were impressed by U.S.-led coalition forces' use of IT to support ground, sea, and air combat against the Iraqi military, which collapsed more quickly than anticipated.[74] They concluded that future wars would be local, joint, and reliant on high technology, but they worried China was unprepared to win such wars.[75] U.S. interventions in the Balkans, Afghanistan, and Iraq reinforced the sense of urgency Chinese leaders felt to modernize the PLA and integrate IT on a massive scale, a process they referred to as "informationization."[76] Influenced by the U.S. military's "network-centric warfare" concept, PLA strategists developed a theory of "integrated network-electronic warfare" (INEW) in the early 2000s that similarly emphasized information superiority and the fusion of computer and electronic operations to disrupt the enemy's military operations (see Appendix II for a table of Chinese terms related to information

*Eleven universities have received this designation since the program's establishment. China Net, *The Number of First-Class Network Security College Construction Demonstration Projects Has Increased to 11 Universities* (一流网络安全学院建设示范项目高校增至11所), September 17, 2019. Translation.

warfare).*[77] New cyberspace-related organizations and capabilities sprang up within the PLA throughout the mid-2000s, but they did not advance the INEW vision in a coherent or systematic way.†

Under General Secretary Xi, however, China has aligned its warfighting apparatus with the INEW concept and publicly emphasized the strategic importance of cyberspace. The SSF, established on the last day of 2015 amid a wider reorganization of the PLA, aims to employ space, electronic, cyber, and psychological warfare capabilities in unified and innovative ways.[78] A 2015 defense white paper described space and cyberspace as the "new commanding heights in strategic competition," acknowledging for the first time that China was building a military force capable of offensive cyber operations.[79] In a speech the following year, Xi argued that China must enhance both offensive and defensive cyber capabilities to better protect itself and bolster deterrence.[80] A 2019 defense white paper signaled great ambition in the cyber domain, stating that the PLA would accelerate its cyber capability development in a manner "consistent with China's international standing and its status as a major cyber country."[81]

Cyber Underpins China's Information Warfare Strategy

Like their U.S. counterparts, Chinese defense planners view cyberspace capabilities as a supporting component of "information warfare." Information warfare involves the use and management of information for competitive advantage, including both offensive and defensive operations.[82] Militaries implement strategies of information warfare by carrying out "information operations," which utilize various information-related capabilities to create effects and desirable operational conditions on the battlefield.[83] The battlefield spans not just the physical domains of land, air, and sea but also space, cyberspace, the electromagnetic spectrum, and the human mind.‡[84] Both the U.S. and Chinese militaries view cyberspace op-

*According to the U.S. Department of Defense, "information superiority" is "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." The United States' network-centric warfare concept aims to translate information advantages enabled by IT into competitive advantages through the robust computer networking of dispersed friendly forces. Joint Chiefs of Staff, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, November 8, 2010 (as amended through February 15, 2016), 111; Timothy L. Thomas, "Chinese and American Network Warfare," *Joint Force Quarterly* 38 (2005): 77, 79–80.

†According to publicly available reports, China stood up an elite corps for cyber operations in 1997 and established a battalion-sized information warfare unit in 2000. The (now defunct) third department of the PLA's General Staff Headquarters (3PLA, focused on signals intelligence) assumed network defense and cyber-enabled intelligence collection missions, while the fourth department (4PLA, focused on electronic countermeasures) assumed network attack missions. The PLA reportedly developed and field tested a variety of capabilities for cyber-enabled information warfare from the early 2000s onward, including software for network scanning; obtaining and cracking passwords; stealing data; and paralyzing, blocking, or deceiving information systems. The PLA conducted more than 100 military exercises involving some aspect of information warfare between the early 1990s and 2005 and a similar number likely occurred between 2005 and 2010. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, Phillip Saunders et al., eds., National Defense University Press, 2019, 444, 446; Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* (Spring 2018): 108; Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges* 7:2 (Winter 2011): 81, 82, 84; Steven A. Hildreth, "Cyberwarfare," *Congressional Research Service*, June 19, 2001, 12.

‡Both the Chinese and U.S. militaries view cyberspace as a warfighting domain existing within a broader information-based context. The PLA uses the term "information domain" to encompass operations conducted in space, cyberspace, and the electromagnetic spectrum and against the human mind. The U.S. military explicitly includes cyberspace within the "information environ-

erations as but one type of information operation to be employed in a multifaceted assault on an adversary's decision-making process during peacetime, competition, and wartime.[85]

Chinese strategic texts have described the integration of cyber, space, and electromagnetic operations as an operational necessity because such integrated operations can paralyze an adversary's decision-making and generate profound strategic effects.[86] Some PLA theorists have argued that the SSF's cyber and other information operations should affect an adversary's political system, economy, scientific and technological base, culture, and foreign policy, a practice roughly aligning with the U.S. concept of "strategic cyberwarfare."[87] Because strategic cyberwarfare ultimately aims to degrade an adversary's will, behavior, and policy choices, these theorists argue that cyber operations should target governmental, economic, and societal networks as well as civilian critical infrastructure.[88] The 2020 edition of the *Science of Military Strategy*, one of the PLA's leading textbooks on strategy, similarly states that the "key targets" of integrated cyber, space, and electronic operations are an adversary's "national and military decision-makers, strategic early warning systems, military information systems, and information systems in national information infrastructure such as finance, energy, and transportation."[89] More broadly, the text notes that such integrated information warfare operations are superior to traditional computer network warfare precisely because they transcend multiple domains and can be employed at any point in the continuum between peace and war.[90]

Cyber operations are also foundational to China's information warfare strategy because they enable rapid victory over an adversary in the information domain. Chinese information warfare aims to defeat an adversary in a military engagement by establishing "information dominance," or the ability to gain the initiative by collecting, managing, and employing information more quickly and precisely than the adversary.[91] The *Science of Military Strategy* notes that cyberspace is the "basic platform for information warfare" because blinding cyberattacks on an adversary's computer networks can paralyze its combat processes at the outset of a conflict, thereby ensuring one's own information dominance.[92] "The victory of the war begins with the victory of cyberspace," the text states.[93] "Whoever holds the dominance in cyberspace will win the initiative in the war; whoever loses this center will fall into strategic passivity."[94]

Network Warfare: The Best Equivalent to Cyberwarfare in Chinese Strategic Thought

Chinese strategists use the term "network warfare" to describe a variety of operations that states undertake in cyberspace, also known as the "network space," throughout the peace-war continuum.[95] The purpose of network warfare is to establish "network dominance" whereby a state's own networks operate smoothly while its adversary's networks cannot.[96] A state achieves network dominance through a mixture of

---

ment." The information environment has three components: the "physical dimension" (command and control systems, and associated infrastructure), the "informational dimension" (networks and systems where information is stored), and the "cognitive dimension" (the minds of people who transmit and respond to information). Edmund J. Burke et al., "People's Liberation Army Operational Concepts," *RAND Corporation*, 2020, 4; Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, November 27, 2012, I-2, I-3.

network reconnaissance, offense, defense, and support operations (see Table 2).[97] "Among them, the attack force is the leader, the defensive force is the main body, and the reconnaissance force is the cornerstone," the authors of the 2020 *Science of Military Strategy* write.[98]

Table 2: Forms of Network Warfare Outlined in the *Science of Military Strategy*

Form	Summary
Network reconnaissance	The use of various methods to surveil an adversary's networks.[99] Network reconnaissance aims to exploit an adversary's data and information for intelligence purposes rather than to sabotage those information systems.[100] The difference between network reconnaissance and network attack, however, may simply be a few commands entered into a computer terminal.[101] "Network reconnaissance often is preparation for future possible network attack and defense operations; network reconnaissance thus very easily transforms into attack in network space," the authors of the 2013 edition of the *Science of Military Strategy* note.[102] The authors of the 2020 edition state that network reconnaissance is the most common type of military cyber operation in peacetime.[103]
Network attack	Offensive operations against an adversary's information networks and the data within those networks to disrupt or destroy combat capability.[104] Network attacks can include "soft sabotage" and "hard destruction."[105] "Soft sabotage" involves using malicious code to disrupt an adversary's networks, while "hard destruction" destroys the components in computer facilities, equipment, and network systems through means such as electromagnetic pulse weapons.[106] The authors of the 2013 edition note that network attack weapons have numerous advantages: they are inexpensive to develop and easy to deploy quickly, and "the risk of being punished when executing network attacks is relatively low."[107]
Network defense	Efforts to secure one's own network systems, facilities, and the information that flows through them against adversary attacks.[108] Network defense methods include building firewalls to prevent unauthorized entry into network systems, encrypting data so they cannot be tampered with, requiring identify verification to access systems, and using antivirus software.[109] The authors of the 2013 edition acknowledge that network defense is hard because "it is difficult to take initiative to resolve those security problems not yet detected."[110]
Network support (operation, maintenance, and recovery)	Capabilities to operate, maintain, and repair one's own networks in the face of adversary attacks.[111] Network operation and maintenance capabilities enable real-time situational awareness, data sharing, and coordination among commanders on the battlefield.[112] Data backup and recovery methods should be implemented quickly to repair hardware, software, and data damaged by an adversary attack.[113]

Source: Various; compiled by Commission staff.

Chinese strategists envision waging network warfare against a wide range of military and civilian targets. These include the networks involved in Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), air defense networks, and civilian infrastructure.[114] Dean Cheng, a former senior research fellow in Asian studies at the Heritage Foundation, confirmed in testimony before the Commission that the PLA views U.S. military and economic networks as attractive targets during a military conflict.[115]

Chinese Strategists Argue Deterrence Works in Cyberspace

While the question of whether deterrence is possible in cyberspace remains hotly contested among U.S. academics, authoritative Chinese writings on the subject reflect no such qualms.[116] Rather, Chinese strategists believe cyber capabilities can be used both to deter an adversary from engaging in malicious cyber behavior and to achieve Chinese political objectives beyond the cyber realm.

The first concept, known as "network deterrence," aims to deter a hostile state from carrying out cyberattacks by displaying one's own cyber capabilities and expressing the resolve to retaliate.[117] According to the 2020 *Science of Military Strategy*, network deterrence can be practiced at the strategic and tactical levels to respond to threats of varying scale and seriousness.[118] Strategic network deterrence works by showing an adversary that one can damage some of its most important strategic assets, such as its C4ISR and transportation systems, thereby persuading it to abandon planned large-scale cyberattacks.[119] By contrast, tactical network deterrence may prevent "scattered and small-scale cyberattacks and cyber infiltration behaviors," though the authors do not explain how these methods differ from those involved in strategic cyber deterrence.[120]

The second concept, known as "information deterrence," refers to the use of cyber and other information operations to compel an adversary to act in ways that further China's political goals.[121] Mr. Cheng noted that information deterrence entails both dissuasion and coercion; it also embodies the idea of deterring an adversary's unwanted action in a conventional, physical domain through information operations rather than deterring operations in the information domain itself.[122] For example, China could threaten or conduct information operations against the United States in an effort to deter U.S. military intervention on behalf of Taiwan.[123] Mr. Cheng stated that Chinese strategists were closely observing the United States' reaction to Russian threats to conduct cyberattacks against the U.S. government and businesses in retaliation for assistance to Ukraine.*[124] (For more on China's reaction to Russia's war on Ukraine, see Chapter 3, Section 1, "Year in Review: Security and Foreign Affairs.")

According to Mr. Cheng, Chinese strategists may envision a "deterrence ladder" for information operations similar to those developed in the space and nuclear domains.[125] This ladder would progress gradually: publicizing experimentation with capabilities for network warfare at the lowest rung; publicly demonstrating plans, prototype development, and equipment production for network warfare; conducting operational exercises; and finally, executing actual offensive network operations at the highest rung.[126] The highest rung could involve a direct attack against key adversary networks for the purpose of preempting that adversary's attack or in response to an adversary's probe for the purpose of retaliating and demonstrat-

*U.S. experts debate the impact of Russia's cyber operations on Ukraine. A June 2022 report by Microsoft found that the Russian military had launched multiple waves of destructive cyberattacks against 48 distinct Ukrainian agencies and enterprises since the conflict began. Recent advances in cyber defenses (such as threat intelligence and end-point protection) have helped Ukraine withstand a high percentage of these destructive Russian cyberattacks, however. Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," *Microsoft*, June 22, 2022; David Cattler and Daniel Black, "The Myth of the Missing Cyberwar," *Foreign Affairs*, April 6, 2022.

ing capability.[127] In a news article about information deterrence, one expert from the PLA's Academy of Military Sciences noted that disrupting telecommunications networks, spamming the public's phones with propaganda messages, and attacking the power grid could all produce a deterrent effect.[128]

China's Approach to Cyber Operations Heightens Escalation Risks

The chances that an engagement between China and the United States in cyberspace could escalate to higher levels of violence is higher today than in the past due to China's increasingly aggressive cyber activities. Three risks are especially prominent.

First, inadvertent escalation could result from differing Chinese and U.S. understandings about appropriate behavior in cyberspace. Adam Segal, director of the digital and cyber program at the Council on Foreign Relations, testified before the Commission that military interactions between China and the United States in cyberspace could spill over into a kinetic conflict because the two countries lack a shared understanding of appropriate thresholds, escalation ladders, and signaling.[129] Without shared understanding of these matters, one party may deliberately take an action in cyberspace that it does not believe is escalatory but that the other party to the conflict interprets as escalatory.[130] For example, Chinese beliefs about the deterrent effect of cyberspace operations may rely on erroneous assumptions about an adversary's psychology. Using actual offensive cyberspace operations against an adversary in a crisis or the early stages of a conflict could serve to provoke rather than deter that adversary.[131] Moreover, a Chinese cyberattack on the United States' co-located conventional and nuclear assets, such as satellites that enable both conventional and nuclear command and control, would be viewed by U.S. leaders as highly escalatory—even if they were intended simply to disable conventional military operations—because such an attack would appear to threaten nuclear capabilities. Indeed, the *Science of Military Strategy* explicitly describes "strategic early warning systems" as a potential target of integrated cyber operations.[132]

Second, escalation could result from Chinese leaders' apparent tolerance for risk and lack of concern about potential escalation. Mr. Cheng argued that the PLA's extended incursions into Indian territory in 2021 reflect a view of crisis stability fundamentally at odds with that held by the United States precisely because it is so dangerous to provoke a nuclear-armed neighbor.[133] According to research conducted by Georgetown University assistant professor of political science Ben Buchanan and University of Pennsylvania assistant professor of political science Fiona Cunningham, Chinese strategic writings do not scrutinize the escalation risks associated with using cyber intrusions for operational preparation of the environment, and there is no evidence the PLA has practices in place to manage inadvertent cyber escalation.[134]

Finally, Chinese military leaders might be willing to carry out a crippling cyberattack on the United States if they believe attribution will be difficult or impossible.[135] But the United States may be more capable of attributing cyberattacks than China understands,

noted Mr. Cheng and Winnona DeSombre, a fellow at Harvard University's Belfer Center.[136] This capability creates the potential for a situation in which Chinese leaders must choose either to escalate further in the face of U.S. retaliation for the initial attack or to back down and risk "losing face" before a domestic audience.[137]

China's Formidable Cyberwarfare Capabilities: A Significant Threat Today

There is a robust debate among experts about whether China is a peer of the United States in cyberspace. Major studies conducted by the Belfer Center and the International Institute for Strategic Studies (IISS) within the past two years have found that the United States remains the world's leading cyber power but that China is a noteworthy second due to the rapid progress it has made in developing its cyber capabilities over the past decade.[138] According to the IISS, the United States exceeds China on most metrics of cyber power and stands apart from all other countries based on its "ability to employ a sophisticated, surgical [offensive] capability at scale."[139] For these reasons and others, the IISS assesses that China is likely to remain second for at least the next ten years.[140]

Some analysts believe China is already a peer or near-peer adversary in cyberspace, however.[141] Ms. DeSombre testified before the Commission that China is a peer in cyberspace because its offensive cyber capabilities "rival or exceed" those of the United States, its cyber operations have successfully compromised U.S. targets, and Chinese cybersecurity firms have claimed to detect some U.S. state-sponsored cyber operations.*[142] She judged that the United States does not presently have adequate cyber defenses, personnel, or supply chain security to "rival China long-term in cyberspace," though it does enjoy several "first mover" advantages.†[143]

Assessing Cyber Power

Assessing cyber power is difficult for many reasons. Most states shroud their cyber capabilities in secrecy to preserve the efficacy of their TTPs and the broader strategic advantages they may confer.[144] A small number of disruptive cyber operations have been publicly attributed to state actors, but these probably reflect only

*Ms. DeSombre pointed to Antiy Labs and Qihoo 360 as examples of two Chinese cybersecurity firms that have published analyses of what they claim to be U.S. National Security Agency and Central Intelligence Agency cyber operations. She argued that in some cases, Chinese cyber operators are able to "turn our own tools against us," citing cybersecurity firm reporting that the Chinese state-sponsored threat group APT3, which contracts for the MSS, used hacking tools allegedly developed by the National Security Agency a full year before those tools were publicized in the Shadow Brokers leak. According to Ms. DeSombre, the incident suggested "that the contractor observed the hacking tools being used against Chinese targets and recreated the tool from those observations." Winnona DeSombre, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 10; Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6; Symantec, "Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak," May 6, 2019.

†These include U.S. companies' ownership of large portions of international fiber optic cable; U.S. companies' dominance of the largest online platforms and most popular technological products; the global U.S. network of intelligence-sharing alliances and partnerships; and the fact that the United States still attracts much of the world's best technical talent. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6.

Assessing Cyber Power—*Continued*

a fraction of all state-sponsored cyber activities and therefore provide limited insight into the totality of a state's cyber capabilities.[145] Some indicators of cyber power are better assessed through qualitative methods while others are best measured quantitatively, and sometimes the indicators chosen to represent a particular aspect of cyber power offer a poor proxy.[146] Ms. DeSombre noted that some studies also exhibit the "fallacy of sophistication," inferring that a country such as China is a lesser cyber power because it makes use of unsophisticated techniques like phishing or infected USBs* to facilitate its cyber operations.[147] Despite these complications, existing studies compare countries' cyber power across several categories. These include military strategy and doctrine, offensive cyber capability, cyberespionage capability, dependence on foreign IT and high-tech exports, the scale and quality of the domestic cybersecurity industry, the supply of skilled employees in the IT sector, the percentage of the population that uses the internet, and leadership roles in global cyber governance venues.[148] In the specific case of China, additional insight into the status and future of direction of China's cyber capabilities can come from publications produced by SSF-affiliated researchers, reports about military exercises and training facilities, real-world operations experience attributed to the SSF, and scholarly discussions of the force's potential weaknesses.

Whether or not one believes China is a peer, the country clearly excels in certain aspects of cyber capability, and its offensive cyber operations create considerable dangers for the United States.†[149] According to the U.S. Office of the Director of National Intelligence's *2021 Annual Threat Assessment*, China "possesses substantial cyberattack capabilities" and "can launch cyberattacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States."[150] The IISS similarly assesses that China has likely "developed effective offensive cyber tools for

*A universal serial bus, more commonly known as a USB, is an industry standard for short-distance digital data communication involving a plug and play interface that allows a computer to communicate with other devices. There are many types of USB-connected devices, including flash drives, keyboards, external drives, printers, and may others.

†Offensive cyber capabilities encompass the technologies, people, and organizations that enable offensive cyber operations to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems, or networks. According to a study by researchers at the Atlantic Council, there are at least five aspects of offensive cyber capabilities relevant to analyses of state capability: vulnerability research and exploit development, malware payload development, technical command and control, operational management, and training and support. Vulnerability research and exploit development refers to the programs that facilitate the proliferation of discovered vulnerabilities and written exploits. Malware payload development refers to the programs that facilitate the development or use of malware or tool by attacks to conduct offensive cyber operations, or any forum that encourages the exchange of malware. Technical command and control refers to the technologies that support offensive cyber operations, such as domain name registration, server side command and control software, or virtual personal network (VPN) services that are vital to the initial creation of an offensive operation. Operational management refers to the functions required to effectively manage an organization conducting cyber operations, such as operations management, teams and resource management, and targeting decisions. Training and support refers to the training or education provided to personnel on the offensive cyber process that facilitates the growth of offensive cyber operations. Winnona DeSombre et al., "A Primer on the Proliferation of Offensive Cyber Capabilities," *Atlantic Council*, March 1, 2021; Tom Uren et al., "Defining Offensive Cyber Capabilities," *Australian Strategic Policy Institute*, July 4, 2018.

combat use" based on the content of its cyber doctrine and evidence that it has successfully stolen classified and sensitive information from U.S. government and commercial networks on numerous occasions.[151] To take one metric relevant to offensive capability, reporting from multiple cybersecurity firms indicates China is a global leader in vulnerability exploitation and that it exploited more zero-day vulnerabilities than any other nation in the period between 2012 and 2021.[152] More broadly, the PLA reportedly has as many as 60,000 cyber personnel that could support cyberwarfare missions, dwarfing the number of cyber operators associated with U.S. Cyber Command's Cyber Mission Force by a factor of ten.[153] China also devotes a greater proportion of its cyber personnel to offensive operations than the United States does. According to the IISS's *Military Balance*+ database, 18.2 percent of the units in China's SSF focus on offensive operations,* compared to only 2.8 percent of the units commanded by U.S. Cyber Command.† [154]

China's chief challenge in cyberspace may stem from inadequate domestic cybersecurity, which official Chinese government sources portray as a problem requiring immediate attention.‡ [155] The IISS similarly assesses that "China's core cyber defenses remain relatively weak, [as] evidenced by its continued reliance on U.S.-based corporations for core internet technology and its shortage of cyber-security professionals."[156] China has tried to alleviate its dependence on foreign technology and talent by cultivating a domestic cybersecurity industry, but that industry is relatively new and considerably smaller than its U.S. counterpart.[157] In fact, China's domestic cybersecurity industry constituted less than 7 percent of the global cybersecurity industry in 2019, and in general Chinese cybersecurity firms have both lower revenues and smaller global footprints than their U.S. equivalents.[158] The Chinese government has also issued directives to reduce foreign technology in government and corporate settings as part of its broader efforts to mitigate foreign espionage threats and soften the impact of U.S. export controls on advanced technologies.[159] In late 2021, for example, Beijing tasked a quasi-governmental committee to vet and approve local suppliers in

---

**The Military Balance*+ refers to these offensive operations in terms of generating "effects," or actions to deny, degrade, disrupt, or destroy adversaries' networks, computers, or devices or the information they contain. International Institute for Strategic Studies, "Chapter Ten: Military Cyber Capabilities," in *The Military Balance*+ 122:1 (2022): 507.

†The IISS bases these percentages on the distribution of roles across the units within the principal cyber forces of each country, which have their own components. The Network Systems Department is the relevant component of the SSF, China's principal cyber force. By contrast, the relevant components of U.S. Cyber Command, the United States' principal cyber force, are Army Cyber Command, Air Forces Cyber, Fleet Cyber Command, Marine Corps Forces Cyberspace Command, Coast Guard Cyber Command, and cyber units within the National Guard. International Institute for Strategic Studies, "Chapter Ten: Military Cyber Capabilities," in *The Military Balance*+ 122:1 (2022): 508.

‡Chinese government sources describe domestic cybersecurity as lacking. A 2020 report by the China Internet Network Information Center, an administrative agency subordinate to CAC, documented a 57 percent increase in hacks of Chinese government websites between 2019 and 2020. More recently, a 2021 report released by the National Computer Network Emergency Response Technical Team/Coordination Center of China noted that "organized and purposeful network attacks" were becoming a more prominent challenge to the country's cybersecurity, and it highlighted the threat posed by overseas advanced persistent threat (APT)) actors' long-term, latent intrusions in party, government, and commercial networks. China's National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), *2020 China Internet Network Security Report (*2020年中国互联网网络安全报告*)*, July 21, 2021, 15, 16–17. Translation; Rogier Creemers, "China's Cyber Governance Institutions," *Leiden Asia Centre*, January 2021, 11; China Internet Network Information Center, *Statistical Report on Internet Development in China*, September 2020, 71.

sensitive areas from banking to data centers storing government information.[160] In May 2022, the Chinese government ordered central government agencies and state-backed corporations to replace foreign-branded personal computers (PCs) with local alternatives that run on domestically developed software within two years.[161] According to Bloomberg News, the campaign will likely replace at least 50 million PCs on the central government level alone and eventually extend to provincial governments.[162]

Exercises and Training Rehearse Cyberattacks on Adversary Targets

Reporting on Chinese military exercises and training involving cyber capabilities is minimal, but the reporting that does exist demonstrates that the PLA and its militias are rehearsing cyberattacks on military and civilian targets. For example, the PLA's Tibet military command reportedly held a field training exercise in 2020 that integrated "live-fire" offensive cyber operations* into joint air-ground combat drills.[163] Recent research by Mr. Cary also reveals that China has a number of national- and provincial-level cyber ranges that the PLA's cyber militias are likely using to practice attacking and defending electrical grids, water treatment plants, and industrial control systems.[164] China Aerospace Science and Industry Corporation, a defense state-owned enterprise, also maintains a cyber range that allows civilians who would likely be mobilized by the PLA in wartime to practice attacking and defending space assets.[165] Both types of ranges help simulate the kinds of Chinese cyberattacks on U.S. military assets and critical infrastructure that experts expect in a wartime scenario.[166]

Suspected Operations Gain Experience Preparing the Battlefield

Several publicly known examples of Chinese state-sponsored cyber operations suggest the country's cyberwarfare operators are gaining experience in conducting both disruptive cyberattacks and preconflict reconnaissance.[167] For instance, in 2020 Taiwan's government attributed cyberattacks against the state-owned petroleum, gasoline, and natural gas company CPC Corporation and ten other organizations involved in Taiwan's critical infrastructure to the Chinese state-sponsored advanced persistent threat (APT)† group APT41.[168] The attacks shut down these companies' computer systems, prevented gas stations from accessing the digital platforms used to manage revenue records, and rendered customers unable to pay for their gas with certain types of electronic payments.[169] To take another

*According to the IISS, live-fire cyber exercises can entail the injection of malicious code into networks by 'adversary' role players and real-time incident response by a defensive team against either an automated or human opponent. International Institute for Strategic Studies, "Chapter Ten: Military Cyber Capabilities," in *The Military Balance*+ 122:1 (2022): 509.

†APT is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to steal sensitive data. Different cybersecurity vendors use different naming conventions for APTs, meaning that a given APT can go by a number of names. For example, "APT41" is also known by the names "BARIUM," "Winnti," "Wicked Panda," and "Wicked Spider." *CrowdStrike*, "What Is an Advanced Persistent Threat?" June 15, 2021; U.S. Department of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection with Computer Intrusion Campaigns against More than 100 Victims Globally*, September 16, 2020; Florian Roth, "The Newcomer's Guide to Cyber Threat Actor Naming," *Medium*, March 25, 2018.

example, a 2021 report by the cybersecurity firm Recorded Future found that a Chinese state-sponsored threat actor group known as RedEcho had extensively penetrated the Indian power grid amid heightened border tensions between China and India in 2020.[170] The report's authors concluded that RedEcho's prepositioning on India's energy assets "may support several potential outcomes, including geostrategic signaling during heightened bilateral tensions . . . influence operations, or as a precursor to kinetic escalation."[171] As of 2021, Chinese hackers continued their reconnaissance activities on parts of the Indian electrical grid, strengthening the argument that they are collecting information useful for future attacks.[172]

Recent reports of cyber-enabled disinformation campaigns emanating from China also suggest the country is gaining experience conducting psychological warfare (for more, see "Psychological Warfare Units Amplify the Impact of Offensive Cyber Operations" later in this section). Fake news reports originating from China proliferated throughout Taiwan's online information environment before and during military exercises carried out by the PLA in response to U.S. Speaker of the House of Representatives Nancy Pelosi's visit to Taiwan in August 2022 (see Chapter 4, "Taiwan" for more on the Pelosi visit).[173] Taiwan's Ministry of National Defense attributed to China's government at least 272 attempts to spread disinformation between August 1 and August 8, which the ministry said reflected themes of "creating an atmosphere of unification by force," "attacking the [Taiwan] government's authority," and "disturbing the morale of the military and citizens."[174] Examples of fake news circulated during this period include reports of a PLA warship entering territorial waters on Taiwan's east coast, a photo of three U.S. B-52 bombers hovering over Taipei, a video of a low-flying missile allegedly shot by the PLA directly over the island, and a video of the PLA transporting rocket launchers to Fujian Province for imminent attacks on Taiwan.[175] The flood of disinformation emanating from China coincided with a number of cyberattacks on the websites of Taiwan's presidential office, Ministry of National Defense, and Ministry of Foreign Affairs, though some experts concluded that the attacks were carried out by Chinese activist hackers not directly affiliated with China's government.[176]

Weaknesses Could Undermine China's Cyber Superpower Ambitions

Despite these indications of strength, China's cyberwarfare forces still face several obstacles in their efforts to develop military capabilities commensurate with superpower status. The PLA lacks warfighting experience and has not tested its own theories about the strategic use of cyber operations on the battlefield, making success uncertain.[177] The fact that the SSF channels information from strategic reconnaissance and sensors to the Central Military Commission (CMC) rather than to the theater commands reinforces peacetime control of the military but risks creating persistent delays in wartime for theater commanders, who will have to "call Beijing" to receive coordinates for assets they intend to shoot.[178] Commanders may not understand how to make best use of the SSF reserve units at their disposal, and neither these reserves nor the cyber militias

have been effectively integrated into operational-level exercises.[179] Finally, China's domestic cybersecurity practices in both government and corporate settings remain weak, leaving many exposed targets for a determined adversary.[180]

The SSF Is China's Primary Cyberwarfare Agent

China has substantially improved its capabilities for cyberwarfare over the past decade and tasked several organizations inside and outside the PLA with carrying out these missions.[181] The most important actor is now the SSF, which is mandated to conduct strategic cyber operations to defeat an adversary in wartime.[182] In addition to active-duty SSF personnel, SSF reserves, cyber militias, and Chinese civilian agencies may all participate in Chinese cyberwarfare activities on a permanent or ad hoc basis.[183] While little information about the SSF's cyberwarfare capabilities is publicly available, China's competency in certain areas of cyber research suggest the country is a formidable competitor in the cyber domain.[184]

The SSF creates synergies between space, cyber, and electronic warfare capabilities in order to execute strategic missions Chinese leaders believe will win future major wars.[185] Like the PLA Rocket Force, the SSF reports directly to the CMC for operations, reflecting its status as a strategic force to be employed only by officials at the highest levels of the CCP.*[186] John Chen, a lead analyst at Exovera's Center for Intelligence and Research Analysis, testified before the Commission that the SSF would "likely prosecute more sensitive missions against political or infrastructural targets at the sole behest of Xi Jinping through the CMC, in keeping with the desire for tight, centralized control over these capabilities."[187] In addition to its primary mission of securing the information domain, the SSF supports other PLA services to execute regional and global military missions.†[188]

Network Systems Department Carries Out Reconnaissance and Offensive Cyberwarfare Missions

The SSF's operational forces are split into the Space Systems Department and the Network Systems Department, with the latter responsible for strategic cyber, electronic, and psychological warfare operations.‡[189] The cyber forces subordinate to the Network Systems Department carry out reconnaissance and offensive missions, while the CMC's Joint Staff Department oversees cyber defense through the Information and Communications Bureau Information

*By contrast, other PLA services are under the operational control of the five theater commands. Ziyu Zhang, "China's Military Structure: What Are the Theatre Commands and Service Branches?" *South China Morning Post*, August 15, 2021.

†The SSF supports other PLA services by providing strategic intelligence support from its space-based communications and reconnaissance assets to the theater commands, thereby facilitating power projection and operations. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms,* Phillip Saunders et al., eds., National Defense University Press, 2019, 476.

‡The SSF also has an administrative structure with four departments: the Staff Department, the Equipment Department, the Political Work Department, and the Logistics Department. The Space Systems Department and Network Systems Department each have their own officer corps, train their own personnel, and prioritize their specific needs for capabilities, but the two departments' operations are integrated through the Staff Department. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, Phillip Saunders et al., eds., National Defense University Press, 2019, 449–451.

Support Base.*[190] Some of the Network Systems Department's most capable cyber personnel are organized within technical reconnaissance bureaus and bases that report directly to SSF leadership and the CMC, potentially bearing responsibility for carrying out strategic cyberwarfare missions against priority targets like the United States and Taiwan.[191] Other technical reconnaissance bases with regional affiliations roughly corresponding to the PLA's five theater commands oversee lower-level brigades and detachments, potentially carrying out less sensitive cyber operations against countries in their areas of responsibility (AORs).[192]

Chinese APTs Linked to the SSF

PLA units now consolidated under the SSF have been linked to Chinese APTs carrying out espionage against military and diplomatic targets (see Appendix III for a list of selected APT groups associated with Chinese state-sponsored espionage). Cybersecurity firms have established these links by examining technical indicators, such as the use of malware or command and control infrastructure known to be employed by the PLA.[193] The information targeted by these APTs is of clear value to the PLA, which is developing indigenous defense technologies and searching for vulnerabilities within foreign military platforms that could be exploited in a conflict for operational advantage. In some cases, APT activity aligns with AORs corresponding to specific PLA theater commands.[194]

- *Tonto Team:* An APT possibly corresponding to Unit 65017 that operates in the Northern Theater Command's AOR and currently focuses on targets in South Korea, Russia, and Japan.[195] It reportedly hacked several South Korean entities involved in the deployment of the Terminal High Altitude Air Defense (THAAD) missile system in 2017.[196]
- *Naikon Team:* An APT possibly associated with Unit 78020 that operates in the Southern Theater Command's AOR and currently focuses on military and government targets in Southeast Asia.[197] Naikon Team has hacked international bodies such as the UN Development Program and ASEAN.[198]
- *RedFoxtrot:* An APT potentially linked to Unit 69010 that operates in the Western Theater Command's AOR and currently focuses on military technologies and defense targets in Central and South Asia.[199] Over the first half of 2021, RedFoxtrot allegedly hacked Indian aerospace and defense contractors as well as telecommunications companies in Afghanistan, India, Kazakhstan, and Pakistan.[200]

*The Network Systems Department absorbed several notable PLA units that existed prior to the 2015 military reforms, including the General Staff Department Third Department (3PLA), formerly responsible for cyberespionage, and the General Staff Department Fourth Department (4PLA), formerly responsible for electronic warfare and network attacks. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, Phillip Saunders et al., eds., National Defense University Press, 2019, 461–462.

Psychological Warfare Units Amplify the Impact of Offensive Cyber Operations

The SSF has also incorporated psychological warfare units into its structure, enabling it to carry out a "three warfares" (psychological, legal, and public opinion) strategy to influence an adversary's perceptions and erode its will to resist.*[201] These units exist under the 311 Base, the only organization within the PLA known to focus exclusively on psychological warfare.[202] The 311 Base's operational forces have reportedly been absorbed into the Network Systems Department, meaning that the psychological operations can be integrated with cyber or electronic warfare missions to maximize impact on an adversary's cognition.[203] These forces' operations likely require consensus within the PLA's political work apparatus and therefore answer to the highest levels of command.[204] Mr. Cheng emphasized in his testimony that manipulating and undermining an adversary's confidence in its perception of a cyberattack on its networks is essential to China's information warfare strategy.[205] "It is not simply computers. It is the human element of interpreting what is on the screen," he said.[206] "Do you believe the emails on your screen? Do you believe that your email went to the right place and conversely that the tweet, the Instagram, the TikTok actually is a reflection of reality?"[207]

The combination of network and psychological warfare units within the SSF gives China a "boosted" cyberwarfare capability the PLA hopes can trigger a chain reaction of political and social effects resulting from fear or uncertainty caused by the initial cyberattack.[208] Mr. Chen argued that the 2021 ransomware attack on Colonial Pipeline,† which resulted in fuel shortages across the East Coast and panic buying at gas stations, illustrates the type of attack the SSF could hypothetically pursue in peacetime, a crisis, or a conflict.[209] To undermine confidence in Taiwan's government, for example, the SSF could launch intermittent cyberattacks against the Taipei subway amid a sustained online influence campaign to accuse public transit officials of corruption during election season.[210] Such a campaign would damage both infrastructure and public confidence, potentially resulting in political repercussions at the polls.[211] "In examples like these, human cognition and responses are more important targets for SSF cyber operations than any network infrastructure," Mr. Chen observed.[212]

---

*According to Mr. Cheng, the "three warfares" strategy is an approach to political warfare that uses different types of information to win the political initiative and seize a psychological advantage over the adversary. "Psychological warfare" involves the application of psychological methods and principles to attack an opponent's perceptions and mindset, erode its will to fight, and protect one's own will. "Legal warfare" involves the passage and enforcement of laws to depict an adversary's actions as unlawful and bolster support for one's own behavior on the grounds that it is legal, virtuous, and just. "Public opinion warfare" uses information propagated through mass channels to shape public and decisionmaker perceptions of the overall balance of strength between oneself and one's opponent. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 44, 48, 51.

†The Federal Bureau of Investigation attributed the attack on Colonial Pipeline to DarkSide, a Russian criminal group, in May 2021. Two months later, the Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency issued a notification jointly attributing a spearphishing and cyber intrusion campaign targeting U.S. oil and natural gas pipeline companies between 2011 and 2013 to Chinese state-sponsored actors, in what some observers interpreted as a reminder that China's cyber capabilities remain a significant threat to U.S. pipeline infrastructure. Christian Vasquez and Blake Sobczak, "China Hacking Threat Prompts Rare U.S. Pipeline Warning," *Energy Wire*, July 21, 2021; Zachary Cohen, Geneva Sands, and Matt Egan, "What We Know about the Pipeline Ransomware Attack: How It Happened, Who Is Responsible and More," *CNN*, May 10, 2021.

SSF Reserves Supplement Active-Duty SSF Personnel

The SSF can also call up reserve units to supplement cyberwarfare operations.[213] These units are drawn from the PLA's standing Reserve Force and constitute a relatively small number of personnel. As of 2018, reservists serving specialized technical functions in the PLA Navy, PLA Air Force, PLA Rocket Force, and SSF combined made up less than 10 percent of the largely ground-centric force.[214] In wartime, SSF reserve units will be commanded through a military chain of command and are organized by mission set, such as network attack or defense.[215]

Military Cyberwarfare Research

Militaries like that of the United States often rely on in-house engineers and tool developers to create capabilities for cyber missions.[216] Similarly, the SSF's own personnel and researchers appear to develop some of the tools it requires for cyberwarfare operations.

The SSF's In-House Capabilities Development

While public information about the SSF's in-house capability development is limited, personnel in SSF units and researchers at the Information Engineering University (IEU), a military academy subordinate to the Network Systems Department, have authored technical papers on a variety of subjects relevant to information warfare (see "Dual-Use Research Advances Cyberwarfare Capabilities" later in this section for more).[217] There is also evidence that SSF units have procured foreign antivirus software, likely for the purposes of testing malware or discovering zero-day vulnerabilities that can be exploited in cyberwarfare operations.[218]

Dual-Use Research Advances Cyberwarfare Capabilities

SSF-affiliated researchers have written papers exploring cybersecurity methods that are inherently dual use, meaning they could be used for both defensive and offensive purposes amid an information warfare campaign.[219] For example, a 2019 Ph.D. dissertation submitted by an IEU researcher specializing in industrial control systems examined defensive methods for detecting intrusions in electrical power infrastructure, dual-use knowledge that could easily be used to attack an adversary's systems.[220] Others at IEU have studied the application of adversarial machine learning to cyber intrusion techniques.[221] Similarly, IEU and 311 Base researchers have published papers and dissertations on topics such as spambot detection, user identification across different social media networks, and automated models for disseminating propaganda—methods that are useful both for controlling domestic information and for conducting psychological warfare or influence campaigns against an adversary.[222]

PLA Leverages Civilian and Commercial Resources for Cyberwarfare

The CCP views military-civil fusion* as an important way to develop the tools and human talent needed to defend against foreign

*The Chinese government's military-civil fusion policy aims both to spur innovation and economic growth through an array of policies and other government-supported mechanisms and to leverage the fruits of civilian innovation for China's defense sector. For more, see U.S.-China

adversaries' cyber operations and prevail on the battlefield.[223] Accordingly, the PLA looks to militias, Chinese government agencies, universities, research institutes, and domestic hacking competitions for sources of technically competent civilians. Some of these avenues enable the SSF to commandeer personnel who can execute cyberwarfare operations, while others contribute to the research and development (R&D) enterprise that "trains" and "equips" the country's cyber operators.

Cyber Militias Bring Civilian Resources to Bear in Cyberwarfare Operations

The SSF can mobilize cyber militias composed of technically competent civilians to supplement cyberwarfare operations.[224] Militias are formal, permanent groups that operate at the direction of the PLA but are distinct from the official reserves.*[225] Militias vary in terms of composition and domain focus, but those specialized for information warfare have existed since the late 1990s.[226] Since 2017, however, China has formalized a "new-type militia force system" to better support informationized warfare and military operations other than war (such as disaster relief).†[227] Cyber militias are one of 20 kinds of new-type militias listed in a classification table maintained by the CMC's National Defense Mobilization Department.‡[228] Their responsibilities likely include network attack, network security and defense, public opinion monitoring and guidance, psychological warfare, and legal warfare.[229] China's cyber militias could participate in military operations alongside the PLA in times of war.[230]

Cyber militias exemplify military-civil fusion because their personnel are drawn from Chinese cybersecurity enterprises and academic institutions.[231] Qihoo 360 Technology Corporation has stood up at least one cyber militia unit in Beijing that reportedly ensures local network security, trains personnel, and conducts research on offensive and defensive network operations.[232] Since 2003, the Southwest University of Science and Technology has operated a cyber militia in partnership with the China Academy of Engineering Physics—China's premier nuclear weapons developer—that trains cybersecurity personnel and members of other militias.[233] The number of cyber militia units within China remains unknown, but there could be thousands or even tens of thousands.[234]

Economic and Security Review Commission, Chapter 3, Section 2, "Emerging Technologies and Military-Civil Fusion: Artificial Intelligence, New Materials, and New Energy," in *2019 Annual Report to Congress*, November 2019.

*In general, Chinese militias train for warfare-oriented support roles (such as logistics, intelligence, and defense operations) and participate in disaster relief, emergency response, and social stability missions. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 13.

†According to Insikt Group, China's new-type militias are intended to carry out emergency response tasks, support the needs of modern warfare, and help China project military power in new strategic spaces. These militias rely on well-educated, skilled professionals from China's civilian economy. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 1.

‡The 20 militia categories listed in the classification table are: emergency response, stability maintenance, special search and rescue, duty support, maritime militia, border/coastal defense militia, air defense militia, special assistance/support, engineering rapid repair, chemical defense/rescue, transportation and shipping, transport/road protection, communications support, reconnaissance/intelligence support, logistics support, equipment support, service and branch support, network (cyber), intelligence and information, and sentry posts. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 16–17.

Ad Hoc Arrangements Enable SSF to Call Up Chinese Government Agency Personnel

During wartime, the SSF may call up personnel within Chinese government agencies like the MSS and MPS to participate in cyberwarfare missions on an ad hoc basis.[235] Little information about these arrangements is available, but both agencies are likely to have operational roles during a conflict.[236] Mr. Kozy speculated that the MSS could turn over to the PLA both targeting recommendations and the access the MSS and its contractors have already gained to adversary networks.[237] The MSS could also instruct its various contractors to engage in "patriotic hacking" of less sensitive targets in order to deconflict with potential SSF operations while sowing chaos within the adversary's society.[238] More broadly, PLA texts outline a series of support and coordination mechanisms between the SSF and central- and local-level CAC, MSS, and MPS organizations that carry out cyber activities.[239] "These support and coordination mechanisms are meant to ensure that [China's] various cyber actors act in concert when strategic cyberwarfare is underway," Mr. Chen observed.[240]

Chinese government agencies can also mobilize cyber resources owned by civilian organizations for use in wartime. A draft survey used by the National Defense Mobilization Department to identify civilian assets that can be requisitioned in wartime identified several types of "mobilization instruments" relevant to cyber operations.[241] These include large-scale cybersecurity enterprises, authority for which lies with CAC, the MIIT, and the MPS; large and super-large data centers, authority for which lies with CAC and the MIIT; and cyber ranges, authority for which lies with CAC, the MPS, and the MIIT.[242]

A Pipeline for Offensive Research between Chinese Universities and the SSF

According to Mr. Chen, the MIIT and its State Administration of Science, Technology, and Industry for National Defense (SASTIND) together "orchestrate a vast effort to equip the PRC's [People's Republic of China's] cyber agencies with leading-edge technology and supply them with elite talent."[243] Both entities advance this effort through their supervision of a web of research universities with close ties to China's defense industry.[244] The most visible are the so-called "Seven Sons of National Defense," but there are at least 60 Chinese universities subordinate to both the MIIT and SASTIND.[245] Many of these universities conduct cybersecurity research with potential applications to information warfare, generating knowledge the PLA can consume even in the absence of formal collaboration.*

*According to the China Defense Universities Tracker, at least 23 universities conduct cybersecurity-related research. These include Beijing Electronic Science and Technology Institute, Beijing University of Posts and Telecommunications, Hangzhou Normal University, Harbin Institute of Technology, Harbin University of Science and Technology, Heilongjiang University, Information Engineering University, Nanjing Institute of Information Technology, Nanjing University, National University of Defense Technology, Northwestern Polytechnical University, People's Public Security University of China, Shandong University, Shanghai Jiao Tong University, Sichuan University, Southeast University, Tsinghua University, University of Electronic Science and Technology of China, Wuhan University, Xi'an Jiaotong University, Xidian University, Zhejiang University, and Zhengzhou University. China Defense Universities Tracker, "Cyber," *Australian Strategic Policy Institute*.

Other Chinese universities contribute directly to the PLA's offensive and defensive cyber capabilities through joint research facilities and research grants, embodying China's military-civil fusion approach.[246] Southeast University jointly operates the Purple Mountain Network Communication and Security Laboratory with the SSF, where researchers work together to fulfill "important strategic requirements" and conduct interdisciplinary cybersecurity research.[247] Shanghai Jiao Tong University (SJTU) co-locates its School of Information Security Engineering on a PLA information engineering base in Shanghai.[248] SJTU's Cyberspace Security Science and Technology Research Institute also runs a program that conducts APT attack testing and defense, which Mr. Cary framed as "bold admission of their own APT work and their perceived value to the PLA's cyber capabilities."[249] Both universities have been implicated in state-sponsored hacking operations and received funding from multiple Chinese government grant programs with potential ties to the PLA that support information warfare-related research.*[250] Mr. Cary noted that in examples such as these, "the lab-to-field pipeline is clear and direct."[251]

Some universities even have formal agreements with the SSF or provincial governments to institutionalize research collaboration that benefits the military. The SSF signed an agreement with six Chinese universities and three defense industry enterprises in 2017 to facilitate academic exchange and "train high-end talents for new combat forces."[252] The schools are the University of Science and Technology of China, SJTU, Xi'an Jiaotong University, Beijing University of Technology, Nanjing University, and Harbin Institute of Technology.[253] Both Zhejiang University and Huazhong University of Science and Technology have partnered with the Zhejiang provincial government to operate Zhejiang Labs.[254] Zhejiang Labs' oversight board includes representation from the PLA's National University of Defense Technology, and the laboratory is conducting research with various partners on topics such as artificial intelligence for software vulnerability discovery as well as attack and defense of industrial control systems.[255]

National Research Centers Leverage Academia and Industry to Enhance China's Cyber Capabilities

National research centers focused on cybersecurity are another part of the R&D ecosystem that equips China's cyberwarfare forces. Endorsed by the top bodies of the CCP and military, these centers bring together government, industry, and academia to develop cyber technologies that will advantage China in future wars and reduce its dependence on foreign technologies.[256] The National Cybersecurity Center† (NCC) in Wuhan and the Cybersecurity Civil-Military Fusion Innovation Center in Qingdao are among the most import-

*Southeast University allegedly hacked the healthcare insurance company Anthem in 2015. SJTU allegedly hacked Google and other U.S. technology companies in 2009. China Defense Universities Tracker, "Shanghai Jiao Tong University," *Australian Strategic Policy Institute*, November 18, 2019; China Defense Universities Tracker, "Southeast University," *Australian Strategic Policy Institute*, November 12, 2019; David Barboza, "Hacking Inquiry Puts China's Elite in New Light," *New York Times*, February 21, 2010.

†The NCC is formally known as the National Cybersecurity Talent and Innovation Base. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 6.

ant, though there are smaller cybersecurity parks and industrial bases in Chengdu, Shanghai, Tianjin, and Shanxi Province.[257]

The NCC is overseen by a guidance committee subordinate to the CCCI, and its research zone hosts two laboratories that likely conduct cybersecurity research for government use.[258] The Offense-Defense Laboratory is a network simulation center that applies and tests network security tools in addition to carrying out "practical combat drills."[259] While details are scarce, the laboratory may correspond to or be connected with the similarly named Cyber Offense-Defense Center jointly operated by the PLA and Wuhan University.[260] The Combined Cybersecurity Research Institute, by contrast, focuses on the initial development of new cybersecurity technologies.[261] The institute grew out of a joint effort between Wuhan University and Qihoo 360 and now partners with 12 Chinese companies.[262] Mr. Cary observed that two of these companies, Qihoo 360 and Beijing TopSec, are known to train PLA cyber operators.[263] Both companies have also moved or assigned hundreds of their research staff to the NCC.[264]

The Cybersecurity Civil-Military Fusion Innovation Center was established in 2017 under the guidance of the Central Commission for Integrated Military and Civilian Development and the CMC to enhance the PLA's cyber capabilities.*[265] The center's operations are shrouded in secrecy, but Chinese media reported that the center plans to build cyber defense systems and a threat-intelligence-sharing mechanism for military users, encourage companies to cooperate on R&D projects addressing combat requirements, conduct a pilot study on cyber militia construction, and provide emergency response and APT analysis services to the PLA and local governments.[266] Qihoo 360 is responsible for daily operations of the center, reportedly marking the first time a military-civilian fusion center supervised by the military has been operated by a private company.[267] A 2021 article on a tourism-oriented WeChat account called *Qingdao Local Treasure* mentioned that the center is located in a smart city complex built by Qihoo 360 in Qingdao, not far from a "network security confrontation base" and "network security talent training base."[268] A 2018 commentary in *PLA Daily* argued that the center's establishment reflects "an urgent need to deal with the severe situation of global network security, but also [constitutes] a practical measure for our military to use military-civilian integration development to strengthen the construction of network security capabilities."[269]

Talent Competitions Uncover Vulnerabilities for Military Use

The PLA also holds hacking competitions that encourage researchers in the commercial and academic sectors to identify vulnerabilities for use in cyberwarfare operations.[270] Mr. Cary noted that China's Robot Hacking Games are modeled on the U.S. Defense Advanced Research Projects Agency's 2016 Cyber Grand Challenge.[271] The games are intended to spur innovation in automated software vulnerability discovery, patching, and exploitation technology, tools

*The Central Commission for Integrated Military and Civilian Development was established in 2017 and is chaired by General Secretary Xi. The commission leads decision-making and coordinates policy implementation for matters related to civil-military integration. Brian Lafferty, "Civil-Military Integration and PLA Reforms," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, Phillip Saunders et al., eds., National Defense University Press, 2019, 648.

that can be used in the development of both offensive and defensive capabilities.[272] He observed that while the United States has not hosted any new iterations of the Cyber Grand Challenge since 2016, China has staged more than a dozen rounds of the Robot Hacking Games since their inception in 2017.[273] Specific entities within the PLA, such as the Equipment Development Department, have organized their own hacking competitions to identify and develop tools that can automate vulnerability discovery.[274]

China's Cyberespionage Goals and Capabilities

China's cyberespionage operations have grown stealthier, more technically sophisticated, and more agile over the past decade.[275] Analysts studying China's cyberespionage operations in the early 2010s used to describe Chinese tradecraft as rudimentary and "sloppy."[276] One Shanghai-based PLA unit carrying out a massive, multiyear cyberespionage campaign took so few precautions against detection, for example, that cybersecurity firm Mandiant released a landmark report in 2013 that thoroughly documented its operations.[277] Since that time, however, Chinese cyberespionage operations have grown more covert, incorporated more advanced TTPs, infiltrated a wider range of targets, and leveraged a more diverse workforce of hackers beyond the PLA.[278] This improvement largely reflects the reassignment of responsibility for most global cyberespionage operations from the PLA to the MSS in recent years.*[279] According to Mr. Kozy, the MSS is a "unique cyber adversary that has in many ways surpassed the smash-and-grab PLA intrusions of the past and created a much more dangerous environment globally" for victims of Chinese cyberespionage.[280]

The MSS Leverages Special Advantages in Its Global Cyberespionage Operations

The MSS excels at cyberespionage because of its competence and its unique access to other elements of China's cybersecurity ecosystem.[281] As a professional intelligence service, the MSS combines human intelligence operations with cyber campaigns, synthesizes big data for targeting operations, and attracts top-level technical talent with generous benefits.†[282] Though top-ranking MSS officials were early targets of General Secretary Xi's anticorruption campaign, the agency now enjoys the confidence of China's top leadership and is headed by Chen Wenqing, one of General Secretary Xi's close associates.[283] But the MSS's most consequential advantages stem from its empowered position in the Chinese legal system, its deep ties to the MPS, and its oversight of technical bodies responsible for vulnerability testing and software reliability assessments.[284]

---

*According to Mr. Kozy, the Chinese leadership elevated the MSS around 2015 to take advantage of the agency's greater technical competence, to move beyond embarrassing exposures of PLA cyber operations, to buy time for the PLA's various cyber units to be absorbed into the SSF, and to provide an "off ramp" in negotiations with the United States over an agreement to restrict cyberespionage. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 84; Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–3.

†Big data analytics enable the rapid processing of vast amounts of data in ways that can facilitate cyber offense and cyber defense.

Vast Legal Authorities Enhance MSS Collection

China's legal system empowers the MSS to compel virtually any individual or organization within China to assist its cyberespionage operations. Specific provisions of the Cybersecurity Law and National Intelligence Law require all Chinese citizens, companies, and government agencies to comply with the MSS's requests for support to intelligence operations.[285] Such support can take the form of providing MSS officers intelligence cover, allowing the use of one's organization as a recruiting platform, or granting the MSS access to one's premises, networks, or data.[286] The MSS also benefits from security regulations that require all individuals and vendors operating within China to submit discovered vulnerabilities in software to the government within two days.[287]

For example, some large Chinese technology companies have reportedly lent their data-processing capabilities to the MSS, ostensibly because they are required to do so by law. A 2020 report in *Foreign Policy* magazine found that Alibaba and Baidu have previously assisted the MSS and other elements of the security services with requests to analyze large amounts of data collected in its intelligence operations.[288] The report noted that large Chinese technology companies have likely synthesized data Chinese state-sponsored hackers stole from Marriot, Equifax, the U.S. Office of Personnel Management, and other organizations for the purpose of identifying U.S. intelligence personnel.[289] Mr. Cary argued that large Chinese technology firms may comply with such one-off requests from the MSS "begrudgingly," viewing them as "a cost of doing business, not another profitable venture for the firm."[290] More broadly, experts have raised concerns that China's intelligence services could access data about U.S. users from the popular video platform TikTok after *BuzzFeed* reported in June 2022 that China-based employees of TikTok's parent company ByteDance had repeatedly accessed nonpublic data about U.S. users.*[291]

MPS Provides Cover, Office Space, Recruitment Help

The MSS derives significant operational advantages from its longstanding and intimate relationship with the MPS, a law enforcement agency.†[292] MSS offices are frequently co-located with MPS

*The Biden Administration's EO 14034 effectively revoked and replaced the Trump Administration's EO 13942 and 13943 on TikTok and WeChat, respectively. Released in August 2020, the Trump Administration orders would have required both apps to cease services provision in the United States and prompted TikTok's parent ByteDance to enter into negotiations with Walmart and Oracle over the sale of TikTok to allow the app's continued operation in the United States. Negotiations over the buyout languished alongside multiple lawsuits against the executive orders on First Amendment grounds, and implementation of these orders was postponed with the Biden Administration's review of policies. In June 2022, TikTok and Oracle announced they had completed the migration of TikTok's collection of U.S. user data into Oracle-owned data centers in the United States. It is not clear whether the Committee on Foreign Investment in the United States will pursue additional mitigation measures with TikTok to secure U.S. users' "sensitive personal data." Richard C. Sofield, John M. Satira, and Olivia Hinerfeld, "TikTok and Oracle Ink Data-Storage Agreement in Apparent Effort to Avoid Further CFIUS Scrutiny," *Vinson & Elkins*, June 24, 2022; Robert Chesney, "TikTok, WeChat, and Biden's New Executive Order: What You Need to Know," *Lawfare*, June 9, 2021; White House, *Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries*, June 9, 2021.

†The MSS was created in 1983 by combining the CCP's Investigation Department with the MPS departments responsible for intelligence and counterintelligence. The MSS's first minister was a former MPS vice minister. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.

offices, which provide convenient cover for intelligence operations.[293] The MSS likely accesses data collected by the MPS through domestic surveillance and censorship mechanisms such as the Great Firewall.[294] Finally, the two agencies may work together to secure the cooperation of convicted criminals who possess hacking skills that can be leveraged for the state. "New laws during the late 2000s gave new powers to the MPS and MSS to pursue cyber criminals domestically, and it is believed that many of these same individuals came under legal scrutiny or were arrested," Mr. Kozy observed.[295] "It is suspected several were released in exchange for rendering their skills to the state for cyber espionage purposes, and subsequently allowed to continue their criminal activities as long as they targeted victims outside China."[296] He pointed to the example of infamous hacker Tan Dailin (a.k.a. Wicked Rose), who was arrested by the MPS in 2009 but likely received a commuted sentence in exchange for an agreement to contract for the MSS just two years later.[297]

MSS Mines Vulnerabilities through Its Control of Technical Organizations

The MSS also derives exploits from its control of technical bodies responsible for assessing vulnerabilities in software and hardware. The most important is CNITSEC, which appears to outside observers as an independent agency but in actuality belongs to the MSS's 13th bureau.[298] CNITSEC reviews software for government use, conducts "national security reviews" of foreign technology that will be sold on the Chinese market, interfaces with domestic cybersecurity firms pursuing government contracts, and collects information about vulnerabilities in software, hardware, and information systems.[299] It also maintains China's National Vulnerability Database (CNNVD), which catalogues and provides advisories for vulnerabilities discovered in software.[300]

The MSS uses its oversight of CNITSEC to evaluate high-value vulnerabilities in software or hardware for operational utility before they are published in CNNVD.[301] A 2017 analysis by researchers at *Recorded Future* found that CNNVD tended to publish high-threat vulnerabilities substantially later than low-threat vulnerabilities (a discrepancy ranging from 21 to 156 days later) and that the U.S. government's National Vulnerability Database beat CNNVD to publication on 97 percent of vulnerabilities commonly exploited by malware linked to Chinese APT groups.[302] A year later, the same researchers found that CNNVD had altered the dates corresponding to initial publication of high-value vulnerabilities identified by the 2017 report in an apparent attempt to cover up evidence of the MSS's vulnerability evaluation process.[303] Mr. Kozy stated in his testimony that one example of this process can be seen in the use of zero-day vulnerability by APT40 (a.k.a. Kryptonite Panda) a month before it was publicly reported as being discovered by Qihoo 360.[304]

The MSS also leverages resources beyond CNNVD to acquire vulnerabilities and exploits for its cyberespionage operations. While details are scarce, the MSS may have access to a common, centralized development and logistics infrastructure that enables its own cyber operators, contractors associated with APTs, and SSF personnel to access the same pool of malware and other tools.[305] A common infra-

structure could explain why multiple APTs associated with the MSS often use the same malware.[306] The MSS also buys datasets and tools from underground marketplaces that it subsequently customizes.[307] Mr. Kozy argued that such purchases on the black market "may account for the variety of tools seen in use by MSS operators and explain why many of them are more advanced than tools typically seen in the domestic Chinese underground marketplaces."[308]

Separately, the MSS may run its own domestic hacking competitions to identify vulnerabilities from talented civilian hackers. Mr. Cary noted that CNITSEC has hosted talent competitions in the past to identify and develop tools for vulnerability discovery.[309] The MSS also appears to benefit from the Tianfu Cup, one of China's largest and most important hacking competitions, though the nature of the MSS's relationship with the competition is unclear.[310] Modeled after the premier international hacking competition Pwn2Own, the Tianfu Cup hosts three concurrent tournaments focused on identifying vulnerabilities, hacking devices, and compromising operating systems, often taking aim at products produced by the world's largest technology companies.[311] Reporting from cybersecurity firms and media outlets over 2020 and 2021 revealed that China's intelligence services had made use of an award-winning vulnerability discovered at the Tianfu Cup to hack the iPhones of Uyghur Muslims.[312]

China's Cyberespionage Operators

Multiple Actors Perpetrate China's State-Sponsored Cyberespionage

While the MSS is the lead agency responsible for global cyberespionage, it does not rely solely on its own technical experts to conduct operations. Rather, the MSS supplements its in-house talent through contracting arrangements with hackers at small firms—some of whom moonlight as cyber criminals—as well as researchers at universities. The PLA also conducts some cyberespionage operations, but most of its cyberespionage portfolio has been transferred to the MSS.[313]

In-House Talent Conducts Operations Spanning the Globe

The MSS has substantial in-house talent it draws on to conduct global cyberespionage operations, thanks to an earlier drive to recruit capable hackers by offering attractive benefits and more career flexibility relative to the PLA.[314] Little public information is available about the MSS's cyber operators, but they are likely located in provincial or functional branches of CNITSEC, serving in penetration tester and tool developer roles.[315]

Some of the most active and notorious Chinese APTs appear to involve MSS cyber operators directly, though it is difficult to ascertain when MSS officers have cyber training and to distinguish between actions of the MSS working through front companies and its contractors, respectively (see Appendix III). For example, APT26 (a.k.a. Turbine Panda), a threat actor run by the MSS's Jiangsu provincial bureau, targeted U.S. and European commercial airliners between 2010 and 2015 for trade secrets related to turbofan engines that ultimately contributed to the design of China's C919 aircraft.[316] According to Mr. Kozy, APT26's cyber operations were overseen by a

chief of the MSS's cyber bureau, who probably had technical training.[317] Many of APT26's cyber operations were perpetrated by the hacker Liu Chunliang, who oversaw the work of other hackers and likely worked directly at the Jiangsu bureau.[318]

Outside Contractors Enhance Capability and Offer Plausible Deniability

The MSS also pays contractors to conduct state-sponsored cyberespionage operations while overlooking the collateral damage created by their criminal activities. According to Mr. Kozy, contractors act as both a "force multiplier and alternative tradecraft for the MSS."[319] Using contractors allows the MSS to easily terminate operations, add an extra layer of operational security between the victim and the MSS, leverage various technical methods for fulfilling intelligence requirements, create plausible deniability in the event attacks are discovered, and acquire technical expertise that may not exist in house.[320]

There is substantial variety across the MSS's contracting relationships, depending on the agency's needs. Some contracting relationships may be formalized through a government contract supervised by CNITSEC, such as those with companies like Qihoo 360 and NSFOCUS.[321] Other contracting relationships may be informal, flexible, and characterized by minimal MSS direction regarding collection requirements.[322] An additional benefit of using contractors is that the MSS has a ready scapegoat if an operation goes awry. Mr. Kozy explained that the MSS can rely on its partners within the MPS to "make arrests if they feel like they need to trot out some victims or [assign] some blame."[323]

In addition to monetary compensation, the MSS may also provide its contractors a kind of "immunity" by turning a blind eye to criminal activities conducted off the job.[324] Mr. Kozy noted that such willful blindness is likely temporary and context dependent rather than constituting any kind of formal or lifelong guarantee.[325] "This makes the relationship between black hat contractors and the MSS a tenuous one, based mostly on those criminals conducting their activities outside of China to prevent a conflict of interest where the MSS and MPS need to protect Chinese citizens from their own operators," he observed.*[326]

There is some public evidence that hackers themselves believe their work with the MSS confers legal protection. According to a 2020 U.S. Department of Justice (DOJ) indictment of hackers associated with APT41, a state-sponsored threat actor that Mandiant has observed using nonpublic malware typically reserved for espionage campaigns in criminal activities for personal gain, hacker Jiang Lizhi boasted of his close connections to the MSS.[327] The indictment noted, "Jiang and his associate agreed that Jiang's working relationship with the Ministry of State Security provided Jiang protection, because that type of association with the Ministry of State Security provided such protection, including from the Ministry of Public Security, 'unless something very big happens.'"[328] Mr. Kozy noted that such a dynamic probably accounts for the recent surge

*"Black hat" hackers exploit weaknesses in an organization's network for malicious purposes, while "white hat" hackers are typically hired to look for vulnerabilities in an organization's system so that they can be patched. Norton, "What Is the Difference between Black, White and Gray Hat Hackers?" February 25, 2022.

in state-sponsored APT groups using tactics like ransomware and cryptojacking* against foreign targets.[329]

Some aggressive Chinese APTs have been outed as contractors for the MSS. For example, cybersecurity researchers discovered in 2017 that activity associated with APT3 (a.k.a. Gothic Panda), a threat actor that stole trade secrets from Siemens AG, Moody's Analytics, and Global Positioning System (GPS) technology company Trimble between 2011 and 2016, was carried out by Guangzhou Boyu Information Technology Company (a.k.a. Boyusec).[330] Boyusec is a contractor working with the MSS's Guangzhou provincial bureau.[331] Similarly, activity associated with APT10 (a.k.a. Stone Panda), a threat actor that stole trade secrets from managed service providers and more than 45 technology companies between 2006 and 2018, has been tied to two hackers who worked for Huaying Haitai Science and Technology Development Company, a contractor for the MSS's Tianjin provincial bureau.[332]

Universities Sometimes Collaborate on Cyber Operations

Some Chinese universities help the MSS and PLA conduct state-sponsored cyberespionage operations in a way that simply has no analogue in the United States. Mr. Cary assessed that most Chinese universities probably do not directly participate in PLA and MSS hacking campaigns, instead advancing China's cyber capabilities in a more traditional educational capacity, but those that do constitute a significant threat to U.S. interests.[333] SJTU allegedly hacked Google and other U.S. technology companies as part of a broader PLA cyberespionage campaign in 2009.[334] More recently, in 2018 U.S. authorities arrested an intelligence officer working for the MSS's Jiangsu provincial bureau who allegedly coordinated with a top-ranking academic official at Nanjing University of Aeronautics and Astronautics to cultivate overseas targets who could facilitate the theft of engine technology from GE Aviation.[335]

Other Chinese universities may engage with the MSS through educational and career development activities that result in technical solutions the agency can exploit in cyberespionage operations. At Hainan University, for example, a professor working with the MSS's Hainan provincial bureau allegedly recruited students from on-campus hacking competitions in 2013 and 2016, offering bounties of up to $73,000 to students and faculty who procured software vulnerabilities that ultimately facilitated hacking operations.[336] Xidian University reportedly operates a jointly administered graduate degree program with the Guangdong Bureau of CNITSEC (known as Guangdong ITSEC), which brings students and graduate students together to solve technical problems that facilitate the MSS's work.[337]

Characteristics of China's State-Sponsored Cyberespionage Operations

Like other countries, China uses cyberespionage campaigns to acquire information that advances its national interests. Yet Chinese cyberespionage activity can often be distinguished from espionage

*Cryptojacking is a type of cybercrime that involves the unauthorized use of victims' devices by cybercriminals to mine for cryptocurrency. *Kaspersky*, "What Is Cryptojacking?—Definition and Explanation."

activities perpetrated by other nation-states based on its distinctive collection requirements and its scale.[338] According to Kelli Vanderlee, a senior manager for strategic analysis at Mandiant's threat intelligence division, some of Beijing's intelligence targets—such as those in Hong Kong, Tibet, and the Uyghur diaspora—reflect the CCP's unique priorities and therefore can be easily distinguished from the intelligence collection activities of other countries.[339] Even though the volume of Chinese cyber threat activity Mandiant has observed declined by at least 50 percent from 2013 to 2016, Ms. Vanderlee noted there are more Chinese state-sponsored threat groups conducting more compromises and exploiting more zero-days than any other nation.[340]

Victims Possess Information Related to China's Key State Priorities

China's cyberespionage operations target political, military, economic, and technical information that advances national priorities, wherever it may be found. According to a 2019 presentation by cybersecurity firm FireEye, between 2016 and 2019 Chinese cyberespionage actors most frequently targeted the telecommunications, government, high-technology, and media/entertainment sectors.[341] The same report found that Chinese cyberespionage actors most frequently targeted the United States, South Korea, Hong Kong, Germany, Japan, India, and Taiwan.[342]

MSS activity can be distinguished from PLA activity based on geographic scope and the identity of the victim.[343] According to Ms. Vanderlee, MSS-affiliated cyberespionage operators generally target the United States and regions outside of the Indo-Pacific, such as Europe, Latin America and the Caribbean, and North America, and their victims align with the agency's mandate to conduct nonmilitary foreign intelligence, carry out domestic counterintelligence, and support aspects of political security.[344] By contrast, PLA cyberespionage operations typically correspond to AORs of the theater commands and focus on military intelligence or defense targets.[345]

Enhanced Collection of Traditional Diplomatic, Political, and Military Intelligence

China's security services have leveraged cyber operations in recent years to enhance traditional espionage campaigns against adversaries, friendly countries, and ethnic minorities of interest. Reflecting the importance Chinese intelligence places on insight into the United States, suspected MSS affiliate APT41 used vulnerable internet-facing web applications to breach the government networks of six U.S. states between 2021 and 2022.*[346] MSS affiliate APT40 reportedly carried out an extensive 2018 cyberespionage campaign in Cambodia, a close ally of China, to acquire intelligence about the country's election commission, opposition politicians, and human rights activists ahead of the general

*There are numerous examples of Chinese cyberespionage operations that have targeted the federal government, such as the 2015 hack of the Office of Personnel Management, as well as U.S. political figures, such as the governor of Alaska in the leadup to a trade delegation visit to China in 2018. Insikt Group, "Chinese Cyberespionage Originating from Tsinghua University Infrastructure," *Recorded Future*, August 16, 2018; Ellen Nakashima, "Chinese Breach Data of 4 Million Federal Workers," *Washington Post*, June 4, 2015.

election.[347] Chinese APT groups also hacked telecommunications networks and Facebook in 2019 and 2021, respectively, to spy on Uyghur activists living in the United States, Central Asia, and Southeast Asia.[348] Numerous Chinese cyberespionage operations have targeted U.S. defense contractors conducting sensitive research in aviation and maritime technologies, successfully stealing designs for advanced U.S. weapons systems such as aircraft carriers and the F-35 fighter jet.[349]

Pilfered Commercial IP Fills Key Technology Gaps

Chinese state-sponsored groups have aggressively targeted commercial IP that aligns with the requirements identified in the country's various industrial plans.*[350] Mr. Kozy contended that Chinese leaders view cyberespionage "as a way to bridge key technology gaps and rapidly gain parity with advanced adversaries like the U.S. in a variety of dual-use technologies . . . that would otherwise be unattainable without years of research and billions spent on development."[351] He pointed to China's first domestic airliner, the C919, as a direct beneficiary of cyberespionage campaigns perpetrated by the MSS-affiliated group APT26 to steal U.S. and European proprietary technology.[352] Ms. Vanderlee concurred, noting Mandiant had observed that Chinese state-sponsored cyberespionage groups regularly targeted organizations where commercial IP theft was a plausible objective, such as those in the technology, engineering, construction, transportation, and biotechnology sectors.[353]

Theft of Personal Information Could Enable Future MSS Targeting

Chinese cyberespionage operators have also stolen personally identifiable information the MSS could potentially use for blackmail or recruitment purposes. For example, DOJ indictments in 2019 and 2020 alleged that contractors from the cybersecurity firm Chengdu 404—whose personnel are thought to be synonymous with APT41—had collected significant amounts of personally identifiable information in the course of their wide-ranging intrusions into more than 100 companies, research universities, and other organizations around the world.[354] Chengdu 404 subsequently constructed a "big data" repository tool known as Sonar-X that allowed users to search social media records that had been collected for individuals of interest, presumably for use by Chinese intelligence.[355] The defendants used Sonar-X to find records related to individuals linked to various Hong Kong democracy and independence movements, a U.S. media outlet that reported on China's repression of Uyghurs, and a specific Tibetan Buddhist monk.[356] According to Mr. Kozy, "This proves the MSS is likely capable of using data gleaned from other breaches such as 2015's OPM [Office of Personnel Management] breach to create targeting packages for both future cyber and HUMINT [human intelligence] operations."[357]

---

*Relevant Chinese industrial plans include the 863 and 973 Plans, five-year plans, Made in China 2025, and the *Space Science & Technology in China: A Roadmap to 2050* report. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 12.

Technical Tradecraft Is More Stealthy, Agile, and Complex than Before

While Chinese state-sponsored cyberespionage operators exhibit varying levels of skill and employ TTPs common to many APTs, Ms. Vanderlee assessed that on the whole their technical tradecraft has "steadily evolved to become stealthier and more agile," and featured efforts to complicate attribution.[358] In her view, three tactics Chinese cyberespionage operators use to gain initial access into a victim's system exemplify trends toward greater efficiency and impact.[359] These include vulnerability exploitation, third-party compromise, and software supply chain compromise.[360] Chinese cyberespionage operators' use of malware is also becoming more varied and focused on concealing malicious activity.[361]

Chinese Cyberespionage Operators Exploit N-Days and Zero-Days

Vulnerability exploitation occurs when an actor exploits flaws or vulnerabilities in software or hardware to infiltrate it for malicious purposes, such as gaining unauthorized access to a device, sabotaging a device, or executing the attacker's commands.[362] These flaws may be "n-day vulnerabilities," which are vulnerabilities that vendors have disclosed and patched, or "zero-day vulnerabilities," which are unknown to the software developer or hardware manufacturer.[363] Vulnerability exploitation is a powerful tactic because once threat actors know a particular software flaw exists, they can target any internet-accessible device running that software, either in targeted or mass campaigns.[364] Ms. Vanderlee testified that Chinese cyberespionage actors made frequent use of both n-day and zero-day vulnerabilities in 2020 and 2021.[365] Moreover, she noted that Mandiant analysis of all attributed zero-day exploits between 2012 and 2021 revealed that Chinese state-sponsored cyberespionage groups had utilized more zero-days than any other nation-state.[366] Both the Microsoft Exchange hack and the Pulse Secure virtual private network (VPN) hack reported in 2021 occurred in part as a result of Chinese cyberespionage actors leveraging zero-day exploits.[367] Ms. Vanderlee stated that several clusters of Chinese cyber threat activity, including one with likely ties to APT5, had exploited Pulse Secure VPN zero-days and n-days to deploy at least 16 families of malware.[368] Notably, the actors "took steps to preserve operational security and stymie forensic investigations, such as clearing logs, cleaning up evidence of data staged for exfiltration, and changing file timestamps."[369]

Third-Party Compromise Illustrates "Upstream" Movement of Collection Efforts

Third-party compromise involves an intrusion that abuses a trusted channel, such as that between a service provider and a client.[370] Chinese cyberespionage operators' use of this tactic is best exemplified by APT41's 2019 hack of a telecommunications company to search its users' text messages, though APT10's breach of nine managed service providers to gain access to client information as part of the Cloudhopper campaign is a more well-known example.[371] Ms. Vanderlee explained that APT41's deployment of MESSAGETAP malware into the network of a telecom-

munications provider enabled it to filter and copy specific users' SMS messages for topics China deems sensitive in a way that left no forensic evidence on users' devices.[372] More broadly, she pointed out that APT41's use of malware to collect SMS messages from a telecommunications provider demonstrates that Chinese intelligence collection efforts are moving "upstream," collecting information closer to the backbone of global communications.[373] That means instead of targeting individual devices, APT41 collected the information at the telecommunications company itself, many degrees removed from the end user.[374]

Supply Chain Compromise

Software supply chain compromise is a type of third-party compromise that occurs when attackers implant malicious code within programs or updates that are distributed via the same trusted channels users normally employ to obtain legitimate hardware, software, packages, or updates.[375] According to Mandiant's analysis of software supply chain compromise incidents successfully attributed to state-sponsored actors between 2013 and 2020, Chinese cyberespionage groups conducted nearly double the number of supply chain compromises carried out by Russian and North Korean groups combined.[376] APT41's large-scale supply chain compromises of common enterprise software offer a good example of this tactic.[377] For example, APT41's 2018 attack leveraged Taiwan-based computer maker ASUS's live update utility to install malicious backdoors on more than 50,000 systems, though the victims targeted and broader goal of the attack remain unclear.*[378] Ms. Vanderlee also highlighted several cases of Chinese software supply chain compromises from 2019 and 2020 that involved software recommended or in some cases required by government authorities, explaining that these breaches likely enabled the collection of intelligence about foreign businesses operating in China as well as Chinese citizens.[379]

Chinese Cyberespionage Groups Change Malware to Conceal Operations

Finally, Chinese cyberespionage operators are changing the types of malware they use to more effectively evade detection by their victims. "Chinese cyber espionage malware use appears to have evolved to operate on a wider variety of operating systems, focus on modular code families, and increasingly incorporate malware only executed in memory,"† Ms. Vanderlee observed.[380] She explained that Chinese cyberespionage threat groups use a combination of publicly and nonpublicly available tools to accomplish operations but that they are increasingly leveraging publicly available malware to blend in with other threat activity.[381]

*The live update utility was distributed to about a million users but only installed by around 57,000. The hackers did not appear to target all of those who installed the backdoor, however. According to the cybersecurity firm Kaspersky, "The goal of the attack was to surgically target an unknown pool of [around 600] users, which were identified by their network adapters' MAC addresses." A MAC address, or Media Access Control address, is a unique hardware identifier used by computers, game boxes, and other devices that access the internet. *SecureList by Kaspersky*, "Operation ShadowHammer," March 25, 2019.

†Malware that exists in a computer's memory, rather than as a file or other artifact on a computer's hard drive, is difficult to detect because most digital forensics discover malware by examining alterations to the hard drive.

China Strives to Remake Global Cyber Governance

China's leadership seeks to shape the norms* and institutions underpinning a global cyber governance system it perceives as unfair and disadvantageous to Chinese interests. According to Dr. Segal, Chinese leaders and analysts have long believed the United States unfairly controls the internet due to its historical management of the Internet Assigned Numbers Authority (IANA), its previous contract with the Internet Corporation for Assigned Names and Numbers (ICANN), and the fact that it once hosted most of the world's original root servers.†[382] More recently, General Secretary Xi and his top officials have criticized the global cyber governance system as "unsound" and "unreasonable" on the grounds that the United States, its allies, and its partners promote norms China opposes and monopolize the policy discourse within institutions making up that system.[383] In response to these perceived injustices, over the past decade Chinese diplomats have become increasingly proactive in promoting cyber norms conducive to CCP interests while opposing norm-building processes led by the United States, its allies, and its partners in existing cyber governance institutions.[384] At the same time, China's leaders have sought to embed China's preferred cyber norms in regional frameworks and create alternative venues for global internet discussions that promote its competing vision of a state-centric cyberspace order.[385]

United States and China Differ on Norms of Responsible State Behavior in Cyberspace

The United States and China diverge sharply on the norms that should guide responsible state behavior in cyberspace during peacetime. The main points of contention are whether espionage conducted for economic advantage is more or less legitimate than espionage conducted for national security purposes, the appropriate extent of state control over the internet, and how international law applies to state activities in cyberspace.

---

*A "norm" is a collective expectation for the proper behavior of actors with a given identity. In the context of international relations, for example, it is a norm that all states conduct espionage, though they may not all agree on the specific types of espionage that are appropriate. The global cyber governance system refers to the rules, policies, standards, and practices that shape global cyberspace. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 157–158; Martha Finnemore, "Cybersecurity and the Concept of Norms," *Carnegie Endowment for International Peace*, November 30, 2017; Internet Governance Project, "What Is Internet Governance?" *Georgia Institute of Technology*, 2017.

†IANA is a standards organization that oversees global Internet Protocol (IP) addresses, internet domain names, and protocol parameters. Prior to 1998, IANA was operated by a component of the University of Southern California under a contract with DOD. Between 1998 and 2016, IANA was operated by the U.S. nonprofit ICANN under a contract with the U.S. Department of Commerce's National Telecommunications and Information Administration. ICANN oversees the central repository of IP addresses and manages the domain name system. After 2016, IANA functions were transferred to the global multistakeholder community through ICANN affiliate Public Technical Identifiers (PTIs), ending U.S. government stewardship of IANA. Historically, most of the world's 13 domain name system (DNS) infrastructure root servers were based in the United States, but today there are hundreds of root servers at more than 130 locations around the world. Sarah Jelen, "DNS Root Servers: What Are They and Are There Really Only 13?" *Security Trails*, July 30, 2021; Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution, Aegis Paper Series No. 1703*, June 2, 2017, 3; ICANN, "Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends," October 1, 2016; Joel Snyder et al. "The History of IANA: An Extended Timeline with Citations and Commentary," May 9, 2016; Internet Society, "IANA Functions: The Basics," August 12, 2014; Digital Guide IONOS, "IANA: Admins of the Internet," 2022.

The (Il)Legitimacy of Economic Espionage

While the United States and many other countries assert that states should not conduct or knowingly support cyber-enabled theft of IP, Dr. Segal testified that Beijing has never embraced the distinction Washington draws between legitimate and illegitimate state operations.* [386] Some have argued that China's theft of IP will decline as its economy becomes more innovative and less reliant on foreign knowledge and technology.[387] Instead, China's burgeoning cyber capabilities have enhanced its widescale cyber-espionage campaigns to steal U.S. and foreign IP for economic and technological advantage in violation of its commitments under a 2015 cyber policy agreement reached between the United States and China.[388] Dr. Segal argued that China is unlikely to accept a norm against economic espionage or cease its widespread theft of IP in the future unless the United States imposes greater costs for its activities.[389] Ms. Vanderlee concurred that Chinese leaders apparently believe the benefits of continuing to engage in economic espionage over U.S. objections outweigh the risks of persisting. "I don't think that it is that they do not understand our preferences or how we would define acceptable or unacceptable behavior," she said.[390] "I think it is simply that they have more to gain by continuing to do the activity that we would prefer they not do than lose."[391]

An Open Internet versus "Cyber Sovereignty"

The United States and many of its allies support a multistakeholder approach† to internet governance and believe cyberspace should be free, open, interoperable, secure, and resilient.‡ [392] By contrast, the Chinese government emphasizes the security of the state over the importance of openness, resilience, and decentralization in cyber governance.[393] China rejects the multistakeholder model of cyber governance, arguing instead that national governments and certain technical standards bodies should be the primary makers of governance decisions.[394] The intellectual lynchpin of China's cyber diplomacy is "cyber sovereignty," which Xi has defined as "respect[ing] the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and internet public policies, and participate in international cyberspace governance on an equal footing."[395] Cyber sovereignty asserts that national governments should be free to erect borders in cyberspace just as they do in the physical world, effectively legitimizing Beijing's internal censorship and surveillance policies.[396]

---

*The United States is one of many countries that oppose commercial cyberespionage. Following the agreements of the 2015 UN's Group of Governmental Experts consensus report, for example, both the G7 and G20 released statements urging member states to take "decisive and robust measures" to increase protections against various forms of cybercrime, including "theft of intellectual property" or other forms of proprietary business information. G20, "*G20 Leaders' Communiqué*," November 15–16, 2015, 6; U.S. Department of State, *G7 Principles and Actions on Cyber*, March 13, 2016.

†The "multistakeholder governance model" envisions the governance of the internet implemented through a coordinated structure distributed across many actors, including governments, international organizations, the private sector, civil society, and international technical institutions.

‡Other members of the G7 (Canada, France, Germany, Italy, Japan, and the United Kingdom) also support the free, open, interoperable, secure, and resilient internet. U.S. Department of State, *G7 Principles and Actions on Cyber*, March 13, 2016.

Chinese diplomats argue that governments should not use the internet to interfere in other countries' internal affairs, reflecting the CCP's broader concern that information from the outside world transmitted through cyberspace poses a threat to domestic stability and regime legitimacy.[397] China's official rhetoric about noninterference in cyberspace is not consistent with its actions, however.[398] Ms. DeSombre noted that China "espouses ideals of cyber sovereignty while abusing the free and open Internet to sow disinformation in the United States."[399] For example, Chinese intelligence operatives reportedly spread fake text messages and social media posts in April 2020 claiming the Trump Administration was planning to lock down the country, instigating public panic in the early days of the novel coronavirus (COVID-19) outbreak.[400]

Varying Applications of International Law

The United States and China agree on the basic application of international law and the UN charter to cyberspace, but they differ substantially in their interpretations of certain provisions that would be relevant to cyber operations in a military context.[401] The United States and many allies and partners hold that international law and the UN Charter's provisions relating to self-defense, the use of force, and armed conflict apply to cyberspace.*[402] From the U.S. perspective, malicious cyber activities may constitute a use of force or "armed attack" that triggers a sovereign state's right to defend itself through proportionate offensive operations, cyber or otherwise, as appropriate.[403] By contrast, China opposes the idea that the principle of self-defense can be invoked to respond to malicious cyberactivity on the grounds that such an interpretation "militarizes" cyberspace and gives powerful states carte blanche to conduct cyberwarfare.[404] Instead, Beijing calls on states to observe the principle of sovereign equality enshrined in article 2 of the UN Charter and refrain from carrying out military cyber operations against other states.[405]

China (and Russia) argues that the current framework of international law is unsuitable for regulating the uniqueness and complexity of the cyber domain, requiring the international community to negotiate a binding multilateral treaty for cyberspace instead of continuing to build consensus around common, nonbinding norms.[406] According to Nikolay Bozhkov, a cyber threat analyst at NATO's cyber defense section, China's reluctance to apply international law to cyberspace reflects concerns about curtailing its own cyber capabilities and providing the United States with a pretext to conduct disruptive cyberattacks during an armed conflict.[407]

U.S.-China Normative Competition Occurs across Cyber Governance Venues

U.S.-China competition over the norms shaping cyberspace spans a variety of formats and venues. According to Dr. Segal, China can now assert that it too has a governance model for data and cyber-

*For example, ASEAN similarly supports the application of international law to cyberspace. Singapore's Ministry of Foreign Affairs, *Statement on Behalf of the Members of Southeast Asian Nations Delivered by Deputy Permanent Representative of Singapore to the United Nations Joseph Teo at the Thematic Debate on Cluster 5: Other Disarmament Measures and International Security of the First Committee, 23 October 2017*, October 23, 2017.

security in addition to those already offered by the United States and Europe.[408] "This model offers an alternative to the balance between individual rights and state authority, privacy and security, and regulation and innovation that liberal democracies emphasize," he observed.[409] "It also explicitly rejects the idea that the balance offered in the other governance models is universal."[410] With this alternative vision of norms for cyberspace, Chinese diplomats advocate for their preferred norms in international institutions and regional groupings devoted to cyberspace issues. At the same time, China has created or proposed new organizations and conventions to supplant existing cyber governance mechanisms in favor of a Chinese alternative.

China Helps Fracture the UN's Premier Cyber Governance Body

China has participated in the UN's Group of Governmental Experts (GGE) process for developing norms of responsible state behavior in cyberspace since 2004, but its recent coordination with Russia has effectively split the global consensus-building process into two separate tracks.[411] In the first decade after the GGE's creation, China joined the United States as a signatory of two major consensus reports in 2013 and 2015.[412] The 2013 report asserted the basic relevance of international law and the UN Charter to cyberspace, while the 2015 report included several U.S.-favored norms related to state responsibility, the duty to assist, not intentionally damaging or impairing other states' critical infrastructure in peacetime, and not targeting another state's computer emergency response teams during peacetime.[413] Despite supporting U.S. positions within these consensus documents, China and Russia jointly opposed U.S. efforts to include a reference to article 51 of the UN Charter's self-defense provision at the 2015 GGE meeting and criticized the United States' "naming and shaming" of state-sponsored hackers.[414]

After the 2017 meeting of the GGE failed to produce a consensus, China supported a Russian resolution to create a new working group of states, known as the Open-Ended Working Group (OEWG), to develop cyber norms in parallel with the GGE.[415] The two groups produced largely similar reports in 2021, though the OEWG's report omitted the term "international humanitarian law," the body of law that protects civilians during armed conflict.[416] In response to comments submitted by the International Committee for the Red Cross, the OEWG's chair acknowledged that "certain questions on how international law applies to the use of ICTs [information and communications technologies] have yet to be fully clarified."[417] Dr. Segal noted in his testimony that the OEWG's opposition to the incorporation of international humanitarian law probably stems from the argument that its inclusion would legitimize cyberattacks against it.[418]

Regional Cyber Diplomacy Bolsters China's Leadership and the Appeal of Its Internet Model

China's cyber diplomacy initiatives aim to promote its preferred norms and bolster its leadership profile in regional and developing country groupings.[419] For example, China has used the Shanghai

Cooperation Organization (SCO) to incubate and socialize its cyber sovereignty norm, described in SCO documents as a component of the "information security" concept.[420] In 2015, the SCO countries submitted (but did not successfully pass) a revised version of the International Code of Conduct for Information Security to the UN General Assembly that attempted to limit states' cyber activities in a way consistent with the cyber sovereignty concept.[421] Under the auspices of the BRICS, China has worked with Brazil, Russia, India, and South Africa to promote norms conducive to cyber sovereignty.[422] More broadly, China's 2017 international cyberspace strategy notes other examples of regional frameworks in which it plays a role, such as the China-Japan-Korea cyber policy consultation mechanism, the ASEAN Regional Forum, the Boao Forum for Asia, the Forum on China-Africa Cooperation, the China-Arab States Cooperation Forum, the Forum of China and the Community of Latin American and Caribbean States, and the Asian-African Legal Consultative Organization.[423]

Chinese regional diplomacy promotes China's technical and normative model for cyberspace. For example, in 2021 China and the League of Arab Nations announced the Initiative on China-Arab Data Security Cooperation that invoked the Chinese concept of "community with a shared future in cyberspace" and promised multifaceted data security collaboration, though details about the substance of the agreement are scarce.[424] Chinese state media hailed the initiative as a "model" for global cyber governance, while Chinese Deputy Foreign Minister Ma Zhaoxu said the initiative aimed to provide a global solution to "the prominent risks and challenges on data security posed by personal information infringement and massive cyber-surveillance on other countries."[425] Some countries have also proposed or passed cybersecurity laws with provisions on website blocking, real name registration, data sharing, and content removal that are similar to China's.[426] These include Egypt, Laos, Pakistan, Tanzania, Uganda, Vietnam, and Zimbabwe.[427]

Competing Venues and Conventions Attempt to Supplant Existing Governance Platforms

Finally, China has launched initiatives intended to replace existing platforms for global cyber governance, though the success of these efforts to date has been limited.[428] The most prominent example is China's creation of the World Internet Conference (WIC) in 2014, which is hosted annually in the city of Wuzhen.[429] The WIC aims to communicate China's cyber sovereignty vision to an international audience and garner support against perceived Western encroachments on China's cyber sovereignty.[430] According to Dr. Segal, however, the WIC's prestige has declined over time.[431] Though Apple CEO Tim Cook, Cisco CEO Chuck Robbins, and Google CEO Sundar Pichai all spoke at the 2017 WIC meeting, in the years afterward most attendees from foreign technology companies have sent country heads, while the United States and its allies have sent representatives from embassies in Beijing rather than heads of state.[432] High-level officials from countries friendly to China, such as Russia, Pakistan, Kazakhstan, Kyrgyzstan, and Tajikistan have attended the WIC.[433]

Another example of China's efforts to supplant existing cyber governance platforms is its cooperation with Russia to replace the Budapest Convention on Cybercrime with a new global treaty. The Budapest Convention is a binding, global treaty that harmonizes national laws and procedural law tools relevant to defining, investigating, and handling evidence of cybercrime.[434] Originally developed by the Council of Europe, the Budapest Convention entered into force in 2004 and currently lists 67 parties to the treaty within and beyond Europe.[435] China is not a party to the Budapest Convention on the grounds that the treaty's provisions encroach on national sovereignty and are unsuitable for non-European countries.[436] In 2019, however, China backed a Russian resolution in the UN General Assembly to draft a new global treaty that would replace the Budapest Convention.[437] The UN General Assembly approved the resolution later that year, allowing the drafting of the treaty to move forward.[438] Negotiations on the Russian draft treaty began in 2022, and the draft treaty will be presented to the UN General Assembly during its 78th session from 2023 to 2024.*[439] According to researchers at Human Rights Watch, this draft treaty "has the potential to expand government regulation of online content and reshape law enforcement access to data in a way that could criminalize free expression and undermine privacy."[440]

Implications for the United States

China's activities in cyberspace pose a fundamentally different, more complex, and more urgent challenge to the United States today than they did a decade ago. General Secretary Xi has broken from his predecessors by framing cyber capabilities as a component of China's superpower status, prioritizing cyber capability development, and centralizing the institutions tasked with cyber policy implementation. The SSF offers Chinese leaders a warfighting apparatus that integrates cyber, electronic, space, and psychological warfare in a way that was once purely aspirational. Sophisticated Chinese cyberespionage campaigns in recent years have compromised greater numbers of sensitive targets within the U.S. government and the private sector than ever before, raising questions about CCP insight into U.S. vulnerabilities that could be exploited for coercion or disruption during a crisis or a war. Whereas ten years ago China cooperated with the United States in many policy areas, today Chinese leaders engage in confrontational behavior toward the United States that increases the chances of miscalculation and escalation. The upshot of these changes is that the United States now faces a mature and capable adversary in cyberspace that is hostile to U.S. interests.

China's cyberwarfare capabilities threaten U.S. society, critical infrastructure, and military operations both in peacetime and during a conflict scenario. The SSF's growing capabilities to manipulate social media and disseminate false information enable it to carry

*The war in Ukraine has cast a shadow over negotiations for the treaty. During the initial negotiations convened by the Ad-Hoc Committee Secretariat from the UN Office on Drugs and Crime in March 2022, several member states expressed solidarity with Ukraine and questioned whether Russia could constructively debate potential provisions within the treaty defending state sovereignty in cyberspace while unleashing cyberattacks against Ukraine. Katitza Rodriguez and Karen Gullo, "Negotiations over UN Cybercrime Treaty Under Way in New York, with EFF and Partners Urging Focus on Human Rights," *Electronic Frontier Foundation*, March 3, 2022.

out "boosted" cyber operations against the United States that could spark panic and undermine public trust in institutions. China's regular cyber forces and militias plan and train to carry out cyberattacks on power grids, water supplies, and transportation networks, demonstrating that China's cyber operators are ready to turn off the lights—or do something much worse—when the CCP directs them to act. In a war over Taiwan, for example, the PLA will likely attempt to blind and paralyze U.S. forces in the region through cyberattacks on U.S. C4ISR and logistics. The PLA may also launch cyberattacks against targets on the U.S. mainland, such as the U.S. military's domestic force generation and sustainment capability.

The U.S. Department of Defense (DOD) has taken steps in the right direction but is limited by manpower and resources. Under its new strategy of "persistent engagement," U.S. Cyber Command is prepared to impose costs on China for malicious cyberactivity, contest its cyber forces in wartime, and disrupt cyber intrusions into U.S. and allied networks in peacetime.* Yet as Hoover Institution fellow Jacquelyn Schneider noted in testimony before the Commission, PLA cyber operators outnumber those of U.S. Cyber Command's Cyber Mission Force by a factor of nearly ten to one.†[441] This quantitative advantage could give the PLA an edge over U.S. cyber forces if a surge in malicious Chinese cyberactivity overwhelms limited U.S. personnel.

Chinese cyberespionage also undermines the integrity of the U.S. political system and undercuts U.S. innovation. China's intelligence services are likely making use of personal information stolen in the hacks on the Office of Personnel Management, Marriott, and Equifax to target U.S. officials and others for blackmail and recruitment. The country's systematic, wide-ranging industrial espionage campaigns have stolen trillions of dollars' worth of U.S. IP, enabling China to circumvent substantial and time-consuming investments in R&D that would otherwise be required to develop advanced technologies for its military and commercial sector.[442] With illicit access to U.S. and foreign trade secrets, China is also able to flood U.S. and global markets with cheap copies of foreign products, driving non-Chinese competitors out of business.

China's formidable cyber capabilities call into question the U.S. government's preparedness to protect its networks from a major

---

*Persistent engagement aims to thwart an adversary's cyberspace operations by continuously anticipating and exploiting its vulnerabilities while simultaneously denying its ability to exploit U.S. vulnerabilities. U.S. cyber forces prevent the exploitation of U.S. vulnerabilities—and sustain U.S. strategic advantage more broadly—by conducting operations that increase resiliency, "defend forward," and continually engage the adversary in cyberspace. "Defending forward" involves proactively observing and countering adversary operations "as close as possible to the origin of adversary activity" and imposing costs (retaliation) in day-to-day competition to disrupt ongoing cyber campaigns. David Vergun, "'Persistent Engagement' Strategy Paying Dividends, Cybercom General Says," *DOD News*, November 10, 2021; Erica D. Lonergan, "Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior," *Lawfare*, March 12, 2020; U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*, 2018, 2, 4, 6.

†The Cyber Mission Force (CMF) executes U.S. Cyber Command's mission to direct, synchronize, and coordinate cyberspace operations in defense of U.S. national interests. The CMF's tasks include defensive operations to protect the use of friendly cyberspace capabilities, data, and networks; offensive operations to project power in and through cyberspace; and operations to secure and maintain the DOD Information Network. The CMF currently has 133 cyber mission teams, but more will be created in the coming years. C. Todd Lopez, "Cyber Mission Force Set to Add More Teams," *DOD News*, April 6, 2022; U.S. Army Cyber Command, *DOD FACT SHEET: Cyber Mission Force*, February 10, 2020.

Chinese cyberattack. Cyber defenses are inconsistent across U.S. civilian government agencies, which have continually struggled to meet their targets for improving cybersecurity best practices.*[443] Marked variation in cybersecurity practices also exists across the U.S. military, since each service tends to have its own networks and teams dedicated to the defense of those networks.[444] Dr. Schneider also argued that DOD employs "byzantine and arcane" network architectures and IT processes that do not align with commercial best practices.[445] According to media reports, slightly more than half of the 133 Cyber Mission Force teams originally set up by U.S. Cyber Command are focused on defending DOD networks, though this proportion may change as the command stands up additional teams.[446] Dr. Schneider argued that too few cyber protection teams are dedicated to the defense of old, insecure DOD systems.[447]

U.S. critical infrastructure is vulnerable to Chinese cyberattacks and poorly regulated by the federal government. According to Microsoft's 2021 *Digital Defense Report*, China-based threat actors displayed the strongest interest in targeting critical infrastructure among all nation-state threats the firm observed that year.[448] In the United States, the private sector owns and operates the majority of critical infrastructure.[449] Neil Jenkins, chief analytic officer at the Cyber Threat Alliance, testified before the Commission that the federal government has little directive authority over most of this infrastructure and is generally limited to providing information that helps manage risk and fostering cross-sector collaboration.[450] Participation by critical infrastructure operators in federal cybersecurity activities is voluntary, and existing regulations for critical infrastructure pertains only to a small number of sectors, such as energy and finance.[451] While the U.S. government has historically favored less cybersecurity regulation on the private sector, Dr. Jenkins argued that the ransomware attack on Colonial Pipeline and other cybersecurity incidents have sparked public concerns that "the market has not been able to keep up with the threat."[452]

More broadly, public-private sector cooperation on cybersecurity is insufficient to meet the challenge posed by China's cyber capabilities. The U.S. government has expanded information sharing and operational collaboration with the private sector over the past 15 years, most notably through the Cybersecurity and Infrastructure Security Agency's public alerts about malicious cyberactivity and the newly created Joint Cyber Defense Collaborative.[453] Challenges remain because federal information sharing is often slow and because the fundamental interests of the government and the private sector are sometimes at odds.[454] Dr. Jenkins noted that private sector organizations may be unwilling to share information with the government due to concerns about the potential usage and reputational consequences of the shared information becoming public, increased regulations on them or their sector, and exposure to legal liability.[455] New cybersecurity incident reporting requirements for

*A January 2022 report by the U.S. Government Accountability Office (GAO) evaluated agencies' inconsistent implementation of federal cybersecurity policies and practices. Since 2010, GAO has made about 3,700 recommendations to agencies aimed at remedying cybersecurity shortcomings. The report found that about 900 of these recommendations were not yet fully implemented as of November 2021. Jennifer R. Franks, testimony for the U.S. House of Representatives Committee on Oversight and Reform, U.S. Government Accountability Office, January 11, 2022, i.

public and private companies in the Securities and Exchange Commission's March 2022 rules and the Cyber Incident Reporting for Critical Infrastructure Act of 2022, also signed into law in March, constitute initial steps to address the vulnerability of U.S. critical infrastructure.

On the global stage, China continues to promote cyberspace norms that suit its authoritarian political system while undermining institutions where the United States historically builds consensus around norms of responsible state behavior in cyberspace. China's creation of the WIC and its push to replace the Budapest Convention with a new cybercrime treaty exemplify its efforts to supplant existing venues for global governance with Chinese alternatives it can manipulate for its own interests.

China enjoys an asymmetric advantage over the United States in cyberspace due to the CCP's unwillingness to play by the same rules. China does not fully accept the applicability of international law to its cyber operations, commits cyber-enabled industrial espionage on a massive scale, uses its domestic law to compel researchers and companies in China to supply it with vulnerabilities, and plans to exploit its commercial IT sector for cyber operations in wartime. By contrast, the United States accepts the rights and constraints imposed by international law on its cyber operations, does not use its professional intelligence services to commit industrial espionage, does not legally compel its researchers or the private sector to supply it with vulnerabilities, allows its adversaries access to U.S. society and markets, and will not exploit the entirety of its civilian economy to wage wartime cyber operations on its adversaries. "This means that during the last decade, given its different doctrinal approach and greater regard for legal and ethical constraints, the U.S. is more likely to have been the victim of an offensive cyberattack than the perpetrator," the IISS observed.[456] "The U.S. may be the most powerful cyber state, but arguably other countries are making greater use of their cyber capabilities in order to exert power."[457] To prevail in the long-term competition with China, policymakers must find ways to impose greater costs for malicious cyberactivity and strengthen domestic cyber defenses while upholding the liberal values the United States has historically championed.

Appendix I: Select Chinese Measures Related to Cybersecurity

Title	Summary	Date
National Security Law	• Requires all "core network and information technologies" to be secure and controllable.[458] • Criminalizes for cyber-enabled hacking, theft of secrets, dissemination of illegal and harmful information, and other cyber-enabled crimes.[459]	Effective July 2015
Ninth amendment of the Criminal Law	• Criminalizes the cyber-enabled dissemination of "false" information that disrupts social order.[460] • Mandates penalties for network service providers that fail to comply with national cybersecurity regulations or provide deliberate assistance to those breaking laws.[461]	Effective November 2015
Counterterrorism Law	• Requires telecommunications operators and internet service providers to provide technical interfaces, decryption, and other technical assistance to the security services conducting investigations of terrorist activities.[462] • Requires telecommunications operators and internet service providers to halt the dissemination of, delete, and report any information involving terrorist or extremist content.[463]	Effective January 2016
Cybersecurity Law	• Requires network operators to implement network security protections, backups of important data, and encryption.[464] • Requires network operators to formulate and implement emergency response plans for cybersecurity incidents.[465] • Requires operators of critical information infrastructure to meet stringent cybersecurity standards, such as annual risk reviews and mandatory testing and certification of computer equipment.[466] • Requires network operators to store sensitive data domestically.[467] • Requires network operators to cooperate with China's law enforcement and security services upon request.[468]	Effective June 2017
National Intelligence Law	• Requires individuals, organizations, and institutions to assist the security services in carrying out intelligence work, including by lending their "communications tools, premises and buildings."[469]	Effective June 2017
Informal prohibition on participation in foreign cybersecurity events	• Media reporting indicates that the Chinese government has prohibited Chinese security researchers from sharing their knowledge at some foreign cybersecurity events, such as Pwn2Own and Capture the Flag competitions.[470]	Reported March 2018

Appendix I: Select Chinese Measures Related to Cybersecurity—*Continued*

Title	Summary	Date
Cryptography Law	• Requires critical information infrastructure operators to conduct a security assessment of their use of commercial encryption.[471] • Requires critical information infrastructure operators to apply for a national security review led by the Cyberspace Administration of China and the State Cryptography Administration.[472]	Effective January 2020
National Defense Law	• Asserts that the Chinese government will take necessary measures to protect its activities, assets, and other interests in cyberspace.[473]	Effective January 2021
Data Security Law	• Establishes a system of data classification and obligations for organizations handling data, including security requirements and assessments for data protection, collection, use, and transfer internally and overseas.[474]	Effective September 2021
Critical Information Infrastructure Protection Regulations	• Clarifies the obligations of critical information infrastructure operators in performing cybersecurity duties.[475] • Clarifies that the MPS is the national lead for the protection of critical information infrastructure.[476] • Clarifies that the Cyberspace Administration of China will coordinate an interagency cybersecurity information-sharing mechanism and receive mandatory reports on cybersecurity incidents.[477]	Effective September 2021
Regulations on the Management of Security Vulnerabilities in Network Products	• Requires vendors and individuals to report all vulnerabilities discovered to the MIIT within two days.[478] • Bans sharing data about vulnerabilities with overseas organizations, except for vendors selling the affected product.[479] • Prohibits security researchers from releasing details about vulnerabilities before vendors had an opportunity to develop a patch.[480] • Criminalizes the sale of vulnerabilities for profit.[481]	Effective September 2021
Cybersecurity Review Measures	• Outlines security procedures for operators of critical information infrastructure and organizations handling data sensitive to national security, including initial public offerings and organizations handling data of more than one million users.[482]	Effective February 2022

Source: Various; compiled by Commission staff.

Appendix II: Chinese Concepts Relevant to Information Warfare and Cyberspace Capabilities

Information warfare	A form of warfare in which the PLA seeks to secure information dominance over the adversary's military forces and contest the information domain as a warfighting domain.[483] Chinese writings conclude information warfare is the "main operational form" of informationized warfare.[484]
Informationization	The process by which militaries are moving toward greater collection, systematization, distribution, and utilization of information.[485] "Informationized warfare" applies IT to all domains and aspects of military operations to increase precision, lethality, and tempo by networking together weapons and C4ISR systems.
Network warfare	A range of offensive, defensive, and intelligence collection activities undertaken by opposing states within the network space.[486] The purpose of network warfare is to establish "network dominance" whereby a state's own networks operate smoothly while its adversary's networks cannot.[487]
Three warfares	A political warfare strategy that calls for the coordinated use of psychological warfare, public opinion warfare, and legal warfare to control perceptions and shape narratives that advance Chinese interests and undermine those of an opponent.[488]
Integrated joint operations	In informationized warfare, the services and branches achieve higher levels of interoperability and synergy by merging together to form a unified "system of systems" rather than coordinating operations by single services.[489]
Systems warfare	The main form of conflict in informationized war is a confrontation between opposing complex networks ("systems of systems") rather than by force-on-force or platform-on-platform combat.[490] The PLA may target critical elements of an adversary's system of systems (such as command and control centers, leadership institutions, and information hubs) via cyberattacks and other means to paralyze its decision-makers.[491]
Integrated Network and Electronic Warfare (INEW)	An approach to warfare that leverages both network and electronic warfare capabilities to disrupt an adversary's networked information systems and, by extension, to secure information dominance.[492]
Peacetime-wartime integration	Maoist idea that victory in war depends on the preparations made in peacetime, which has influenced the organization of China's contemporary information warfare units into permanent operational groupings designed to transition seamlessly from peacetime into wartime command structures.[493]

Source: Various; compiled by Commission staff.

Appendix III: Selected APT Groups Likely Associated with China's State-Sponsored Espionage

Different cybersecurity firms use different naming conventions to refer to APTs* that are likely affiliated with nation-states such as China. Some popular naming conventions include CrowdStrike's use of animal names associated with geography; Mandiant and Mitre's use of numbered groups; Microsoft's use of elements; Recorded Future's use of colors and the phonetic alphabet; Secureworks' use of elements plus a nickname; and Symantec's use of species of insects.[494] Cybersecurity firms may employ different names for what appears to be the same threat actor group in accordance with their naming conventions and what they observe in the particular slice of the overall cyber threat landscape they monitor through their customer base.†[495] Generally speaking, cybersecurity firms identify a threat actor group by analyzing the telemetry‡ gathered by the security threat monitoring product used by their customers for signs of malicious activity.[496] Analyzing multiple instances of malicious activity for distinguishing characteristics, such as particular families of malware or TTPs, may allow cybersecurity firms to identify a "cluster of activity" and attribute it to a single entity.[497] Tracking APT groups can be confusing in part because one cybersecurity firm may track a single threat actor group in connection with a given cluster of activity while another cybersecurity firm may track multiple groups in connection with that same cluster (for example, the same cluster of threat activity is tracked by CrowdStrike as Vixen Panda and by FireEye/Mandiant§ as two groups, APT15 and APT25).[498] The facts that APTs may merge, split, or share their toolsets with others, and that cybersecurity firms may sometimes name APT groups after types of malware or particular cyber campaigns, all complicate attribution and tracking.[499] The table below provides a select list of Chinese APTs that may be state-sponsored and makes extensive use of Mandiant's nomenclature and reporting because of the relative completeness and accessibility of the firm's publicly available resources on APT groups.¶ The table presents alternative nomenclatures and reporting when possible.

*An APT is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to steal sensitive data.

†Because their customer bases and the types of attacks observed on these customer bases may differ, different cybersecurity firms may see different aspects of the same malicious cyber activity (such as different types of TTPs). No one firm has a comprehensive view of all the malicious threat activity occurring in cyberspace at one time.

‡In the cybersecurity context, telemetry refers to the automated communication processes from multiple data sources. Data collected by telemetry is used to monitor the security of networks and detect malicious cyber threats.

§FireEye acquired Mandiant in 2014, but the two companies parted ways in 2021, and Google announced its plans to acquire Mandiant in 2022.

¶The table does not list *individual* Chinese hackers who have been implicated in cyberespionage activities or charged by DOJ.

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
APT41 (a.k.a. Wicked Panda, Wicked Spider, BARIUM, BRONZE ATLAS, Winnti)[500]	A prolific cyber threat actor likely associated with the MSS that conducts state-sponsored espionage as well as financially motivated activity for personal gain.[501] APT41's campaigns have targeted organizations in at least 14 countries, stealing IP from the healthcare, telecommunications, technology, and videogame sectors.[502] The group's operations have also targeted political dissidents in Hong Kong.[503] In March 2022, Mandiant reported that APT41 had compromised six U.S. state government networks.[504]	*Vectors:* Uses spear-phishing, SQL injection, followed by more sophisticated TTPs.[505] *Malware:* Known to use at least 46 different malware families, including backdoors, credential stealers, keyloggers, and rootkits; ransomware; cryptojacking.[506]	2019 & 2020: DOJ charges hackers from APT41 in connection with computer intrusions affecting over 100 victims globally.[507]
APT40 (a.k.a. Kryptonite Panda, GADOLINIUM, BRONZE MOHAWK, TEMP. Periscope, Leviathan)[508]	A cyber threat actor associated with Hainan Xiandun Technology Development Co., Ltd, a front company for the MSS's Hainan branch, that conducts state-sponsored espionage likely facilitating China's naval modernization program.[509] APT40 has targeted governments, companies, and universities for IP spanning a wide range of industries—including maritime research—across the United States, Canada, Europe, the Middle East, and Belt and Road Initiative countries.[510] APT40 may be connected to or overlap with HAFNIUM.[511]	*Vectors:* Uses spear-phishing, often posing as a prominent individual of interest to the target.[512] *Malware:* Known to use at least 51 different malware families, including 37 that are nonpublic and seven of which (BADSIGN, FIELDGOAL, FINDLOCK, PHOTO, SCANBOX, SOGU, and WIDETONE) are associated with other Chinese state-sponsored groups.[513]	2021: DOJ charges members of APT40 in connection with a global computer intrusion campaign between 2011 and 2018 targeting IP, including infectious disease research.[514]
HAFNIUM (a.k.a. Operation Exchange Marauder)[515]	A cyber threat group associated with the MSS that exploited multiple zero-day vulnerabilities in Microsoft's Exchange Server email software to carry out a massive hack affecting thousands of organizations around the world in early 2021.[516] The U.S. government and a number of allied governments jointly attributed the hack to the MSS in July 2021.[517]	*Vectors:* Exploits zero-day vulnerabilities in the internet-facing and vulnerable Microsoft Exchange servers for initial access; then uploaded web shells using these vulnerabilities and executed malicious commands.[518] *Malware:* Backdoor.Hafnium web shells[519]	

*The numbered APT presented first in every entry follows Mandiant's nomenclature and reporting.

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
APT31 (a.k.a. Judgment Panda ZIRCONIUM)[520]	A cyber threat group associated with the MSS that has conducted cyberespionage against government, financial, and defense organizations and attempted cyberattacks against individuals involved in the 2020 U.S. presidential elections.[521] In March 2022, Google's Threat Analysis Group warned multiple Gmail users associated with the U.S. government that they were targeted in phishing attacks conducted by APT31.[522]	*Vectors:* Exploits vulnerabilities in applications such as Java and Adobe Flash; SQL injection.[523] *Malware:* SOGU, LUCKYBIRD, SLOWGYRO, and DUCKFAT[524]	
APT30 (a.k.a. Override Panda BRONZE GENEVA)[525]	A cyber threat group that targets government and commercial organizations in Southeast Asia and India.[526] According to Mandiant, APT30 "is particularly interested in regional political, military, and economic issues, disputed territories, and media organizations and journalists who report on topics pertaining to China and the government's legitimacy."[527] It shares many characteristics with the cyber threat group Naikon, but they are not exact matches.[528]	*Vectors:* Uses a variety of tools including downloaders, backdoors, a central controller, and several components designed to infect removable drives and cross air-gapped networks to steal data.[529] *Malware:* SHIPSHAPE, SPACESHIP, and FLASHFLOOD[530]	
Naikon Team	A cyber threat group associated with PLA Unit 78020 that operates in the Southern Theater Command's area of responsibility and currently focuses on military and government targets in Southeast Asia.[531] Naikon has been active since 2010 and has attacked government agencies as well as civil and military organizations in the Philippines, Malaysia, Cambodia, Indonesia, Vietnam, Myanmar, Singapore, Nepal, Thailand, Laos, and China.[532] Naikon Team has also hacked international bodies such as the UN Development Program and ASEAN.[533]	*Vectors:* Uses social engineering and spearphishing emails with crafted lures containing malicious attachments.[534] *Malware:* Aria-Body remote access trojan, RARSTONE, BACKSPACe, NETEAGLE, XSControl[535]	
Tonto Team (a.k.a. Karma Panda, BRONZE HUNTLEY, Earth Akhlut, CactusPete)[536]	A cyber threat actor associated with PLA Unit 65017 that operates in the Northern Theater Command's AOR and currently focuses on targets in South Korea, Russia, and Japan.[537] It reportedly hacked several South Korean entities involved in the deployment of the THAAD missile system in 2017.[538]	*Vectors:* Uses phishing websites, spearphishing emails with malicious attachments, and vulnerabilities in software.[539] *Malware:* Bisonal, ShadowPad[540]	

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
RedFoxtrot	A cyber threat group potentially linked to PLA Unit 69010, now part of the SSF's Network Systems Department, that operates in the Western Theater Command's AOR and currently focuses on military technologies and defense targets in Central and South Asia.[541] Over the first half of 2021, RedFoxtrot allegedly hacked Indian aerospace and defense contractors as well as telecommunications companies in Afghanistan, India, Kazakhstan, and Pakistan.[542]	*Vectors:* Unclear.[543] *Malware:* PCShare RAT, QUICKHEAL, PlugX, Icefog, RoyalRoad, PoisonIvy[544]	
RedEcho	A cyber threat group that has targeted Indian critical infrastructure.[545] Cybersecurity firm Recorded Future notes that RedEcho shares some common infrastructure TTPs with APT41 and Tonto Team.[546]	*Vectors:* Unclear.[547] *Malware:* ShadowPad[548]	
RedAlpha (a.k.a. Deepcliff, Red Dev 3)[549]	A cyber threat group likely composed of contractors associated with the Chinese intelligence services that targets humanitarian, think tank, and government organizations globally as well as members of the Tibetan and Uyghur communities.[550] According to Recorded Future, in recent years RedAlpha has displayed a particular interest in spoofing political, government, and think tank organizations in Taiwan for the apparent purpose of gathering political intelligence.[551]	*Vectors:* Registering domains to spoof organizations, credential phishing activity imitating webmail login portals.[552] *Malware:* NjRAT[553]	
APT27 (a.k.a. IronPanda, Emissary Panda, Lucky Mouse, Iron Tiger, ZipToken, Group 35, TEMP.Hippo, TG 3390, BRONZE UNION, Threat Group 3390)[554]	A cyber threat group that conducts cyberespionage to acquire political and military intelligence as well as IP from organizations in the aerospace, government, defense, technology, energy, manufacturing, and gambling/betting sectors around the world.[555] In 2015, the cybersecurity firm TrendMicro reported that the group had stolen "trillions of bytes of data from defense contractors in the United States, including emails, IP, and strategic planning documents."[556] APT27 has been active for over a decade but has conducted financially motivated cybercrime activities since 2021, sometimes using ransomware.[557] In January 2022, Germany's domestic intelligence service said APT27 is engaged in an ongoing hacking campaign against German commercial organizations.[558]	*Vectors:* Uses unauthorized access, spearphishing, watering hole attacks (strategic web compromises), remote code execution, living off the land attack, rootkit attack, supply chain attack[559] *Malware:* PANDORA, SOGU, ZXSHELL, GHOST, WIDEBERTH, QUICKPULSE, FLOWERPOT, and others[560]	

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
APT26 (a.k.a. Turbine Panda)[561]	A cyber threat group associated with the MSS's Jiangsu branch that has conducted cyberespionage campaigns targeting the aerospace, defense, and energy sectors.[562] In 2019, CrowdStrike revealed that the group, which it calls Turbine Panda, had stolen IP from multiple foreign companies that manufactured components for China's domestic C919 airliner between 2010 and 2015.[563] The hackers were overseen by MSS Jiangsu intelligence officers and successfully breached the systems of suppliers like Ametek, Honeywell, Safran, Capstone Turbine, GE, and others.[564]	*Vectors:* Uses watering hole attacks (strategic web compromises) and custom backdoors once inside a victim's network.[565] *Malware:* SOGU, HTRAN, POSTSIZE, TWOCHAINS, BEACON, PlugX[566]	2018: DOJ charges two intelligence officers from MSS's Jiangsu branch with conspiring to steal sensitive data, IP, and confidential business information, including information related to a turbofan engine used in commercial airliners.[567]
APT25 (a.k.a. Uncool, Vixen Panda, Ke3chang, Sushi Roll, Tor)*[568]	A cyber threat group that targets organizations in the defense industrial base, media, financial services, and transportation sectors in the United States and Europe for their data.[569]	*Vectors:* Uses spearphishing and publicly available zero-day vulnerabilities.[570] *Malware:* LINGBO, PLAYWORK, MADWOFL, MIRAGE, TOUGHROW, TOYSNAKE, SABERTOOTH[571]	
APT24 (a.k.a. Pitty Tiger)[572]	A cyber threat group that has targeted organizations in the government, healthcare, construction and engineering, mining, nonprofit, and telecommunications industries, often headquartered in the United States and Taiwan.[573] According to Mandiant, APT24 has documents with "political significance," suggesting that "its intent is to monitor the positions of various nation states on issues applicable to China's ongoing territorial or sovereignty dispute."[574] The cybersecurity firm FireEye reports that Pitty Tiger has likely been active since 2008.[575]	*Vectors:* Uses phishing, often relying on military, renewable energy, or business strategy themes as lures.[576] *Malware:* PITTYTIGER, ENFAL, TAIDOOR[577]	

*Mandiant's current webpage on APTs describes APT25 as synonymous with threat groups that other cybersecurity firms track as VixenPanda and Ke3chang; however, other cybersecurity firms have linked VixenPanda and Ke3chang with the APT designated by FireEye as APT15.

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
APT23 (a.k.a. Pirate Panda, KeyBoy, Tropic Trooper, BRONZE HOBART, G0081)[578]	A cyber threat group that has targeted information of political and military significance from media and government organizations in the United States, the Philippines, Vietnam, and Taiwan.[579] Mandiant observes that APT23 may perform data theft in support of more traditional espionage operations.[580] Cybersecurity firm Anomali reported in 2020 that Pirate Panda had carried out a spearphishing campaign targeting Vietnamese government officials located near the Paracel Islands in the South China Sea, which both China and Vietnam claim.[581]	*Vectors:* Uses spear phishing, often relying on education-related themes as lures; occasionally leverages public zero-day vulnerabilities.[582] *Malware:* NONGMIN[583]	
APT22 (a.k.a. Barista, BRONZE OLIVE)[584]	A cyber threat group that has targeted public sector entities, private sector entities, and dissidents in East Asia, Europe, and the United States since 2014.[585] According to Secureworks, BRONZE OLIVE conducted a long-running espionage campaign against Indian government and commercial organizations between 2014 and 2015.[586]	*Vectors:* Uses strategic web compromises; identifies vulnerable public-facing web servers on victim networks, and uploads webshells to gain access to the victim network.[587] *Malware:* PISCES, SOGU, FLATNOTE, ANGRYBELL, BASELESS, SEAWOLF, LOGJAM, DestroyRAT, PlugX, TCP/ICMP RAT[588]	
APT21 (a.k.a. Zhenbao, Hammer Panda)[589]	A cyber threat group that targets government organizations in Russia with information about state security as well as dissident groups seeking greater independence from China, such as those in Tibet or Xinjiang.[590] According to Mandiant, APT21 leverages strategic Russian-language attachments themed with national security issues in lure documents.[591] According to CrowdStrike, Hammer Panda was likely associated with the PLA's first Technical Reconnaissance Bureau in the former Lanzhou Military Region and may have been incorporated into the SSF.[592]	*Vectors:* Uses spear phishing emails with malicious attachments, links to malicious files, or web pages; strategic web compromises; frequently uses the TRAVELNET and TEMPFUN backdoors.[593] *Malware:* SOGU, TEMPFUN, Gh0st, TRAVELNET, HOMEUNIX, ZEROTWO[594]	

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
APT20 (a.k.a. Twivy)[595]	A cyber threat group that targets organizations in the construction, engineering, healthcare, nonprofit, defense industrial base, and chemical sectors in order to steal data and IP.[596] According to Mandiant, APT20 also steals data from or monitors the activities of individuals with particular political interests. Mandiant believes APT20 may be a freelancer group with some state sponsorship.[597] In 2019, cybersecurity firm FOX-IT reported that APT20 had carried out a campaign dubbed Wocao that bypassed two-factor authentication used by businesses and governments in ten countries to protect their networks.[598]	*Vectors:* Uses strategic web compromises, often hosted on websites that deal with issues such as democracy, human rights, freedom of the press, ethnic minorities in China, and other matters.[599] *Malware:* QIAC, SOGU, Gh0st, ZXSHELL, Poison Ivy, BEACON, HOMEUNIX, STEW[600]	
APT19 (a.k.a. Deep Panda, C0d0s0, Pupa, BRONZE FIRESTONE)[601]	A cyber threat group that targets organizations in the defense, finance, energy, pharmaceutical, telecommunications, high-tech, education, manufacturing, legal and investment sectors, likely composed of freelancers with some degree of state sponsorship.[602] In 2017, FireEye observed APT19 carry out a phishing campaign targeting at least seven global law and investment firms.[603] Some analysts believe APT19 and Deep Panda are the same group, but this is not clear from open source reporting.[604]	*Vectors:* Phishing emails with malicious attachments.[605] *Malware:* BEACON, COBALT-STRIKE[606]	
APT18 (a.k.a. Wekby, Dynamite Panda, TG-0416)[607]	A little-known cyber threat group that targets the manufacturing, health and biotechnology, aerospace, defense, construction, engineering, education, high-tech, telecommunications, and transportation sectors as well as human rights groups.[608] Some sources link APT18 to the PLA Navy, but this cannot be confirmed with open source research.[609]	*Vectors*: Uses spearphishing, develops or adapts previously known zero-day vulnerabilities.[610] *Malware:* Gh0st RAT, HTTP-Browser, Pisloader[611]	
APT17 (a.k.a. Deputy Dog, Tailgator Team)[612]	A cyber threat group associated with the MSS's Jinan bureau that targets the U.S. government, international law firms, IT companies, mining companies, and nongovernmental organizations.[613] Among the more memorable campaigns attributed to APT17 was a 2017 spearphishing attack that used a *Game of Thrones*-themed lure purporting to contain spoilers for the current season to convince victims to download a remote access trojan.[614]	*Vectors:* Uses spearphishing; creates profiles and posts in forums to embed encoded command and control infrastructure for use with a variant of the malware it uses.[615] *Malware:* BLACKCOFFEE[616]	

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
APT16	A cyber threat group that has targeted Japanese and Taiwanese organizations in the high-tech, government services, media, and financial services industries.[617] In late 2015, FireEye attributed to APT16 a cyber operation targeting Taiwan media organizations through a modified version of a known vulnerability in the Microsoft Encapsulated Postscript.[618] In some cases, the webmail addresses from which the emails were sent seemed intended to appear as though they were legitimate communications from Taiwan's Democratic Progressive Party.[619]	*Vectors:* Uses spearphishing emails from fake webmail addresses containing malicious attachments; uses compromised VPN credentials to maintain persistent access.[620] *Malware:* IRONHALO, ELMER[621]	
APT15 (a.k.a. Vixen Panda, NICKEL, Ke3chang)*[622]	A cyber threat group potentially associated with Chinese defense contractor Xi'an Tianhe Defense Technology that targets organizations in the trade, economic, financial, energy, and military sectors in Europe, the United States, and South Africa.[623] In 2020, cybersecurity firm Lookout attributed a years-long hacking campaign targeting Uyghurs and Tibetans living in China with Android malware to APT15 and stated that its members may be contractors at Xi'an Tianhe Defense Technology.[624] In late 2021, Microsoft seized dozens of malicious sites used by APT15, which it calls NICKEL, to compromise the servers of governments, diplomatic entities, and nongovernmental organizations across 29 countries, mainly in Europe and Latin America.[625]	*Vectors:* Spearphishing; watering hole attacks distributing malware for Android.[626] *Malware:* ENFAL, BALDEAGLE, NOISEMAKER, MIRAGE, and others[627]	
APT14 (a.k.a. Anchor Panda)[628]	A cyber threat group associated with the PLA Navy that targets government, telecommunications, construction, and engineering organizations for data relevant to military and maritime equipment, operations, and policies.[629] CrowdStrike notes that Anchor Panda has heavily targeted companies in the United States, Germany, Sweden, the UK, and Australia that provide maritime satellite systems, aerospace companies, and defense contractors.[630] Mandiant believes the stolen data, especially encryption and satellite communication equipment specifications, are used to enhance China's military operations.[631]	*Vectors:* Uses spearphishing, exploits zero-days once they have been made public.[632] *Malware:* Gh0st, POISONIVY, CLUBSEAT, GROOVY[633]	

*Many cybersecurity firms and media organizations state that the FireEye-designated APT15 is synonymous with groups known as NICKEL, VixenPanda, and Ke3chang. However, Mandiant's webpage on APTs currently associates VixenPanda and Ke3chang with APT25.

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
APT12 (a.k.a. Calc Team, Numbered Panda, IXESHE, JOYRAT, DynCalc, DyncCalc, DNSCALC, BRONZE GLOBE)[634]	A cyber threat group associated with the PLA that frequently targets journalists, governments, and the defense industrial base.[635] In 2012, APT12 hacked the *New York Times* as it worked on a story about the multibillion-dollar fortune accumulated by relatives of then Prime Minister Wen Jiabao.[636] In 2014, Mandiant reported that APT12 had conducted a cyberespionage campaign targeting organizations in Japan and Taiwan.[637]	*Vectors:* Uses phishing emails from valid but compromised accounts.[638] *Malware:* RIPTIDE, HIGHTIDE, THREBYTE, WATERSPOUT[639]	
APT10 (a.k.a. Menupass Team, Stone Panda, POTASSIUM, Red Apollo, Cicada, CVNX)[640]	A cyber threat group associated with the MSS that has historically targeted construction and engineering, aerospace, and telecom firms as well as foreign governments in support of China's national security goals.[641] Mandiant assesses that these goals include acquiring military and intelligence information as well as confidential business data to benefit Chinese corporations.[642] APT10 perpetrated Operation Cloud Hopper, a global cyberespionage campaign that compromised a number of managed service providers in the United States and other countries to obtain the information of their clients in the engineering, industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government industries.[643] APT10 has also historically targeted Japanese corporations and media organizations, though reporting by Symantec in April 2022 indicated the group is now targeting government-related institutions and nongovernmental organizations in North America, the Middle East, and Europe.[644]	*Vectors:* Uses spearphishing and access to victims' networks through managed service providers.[645] *Malware:* HAYMAKER, SNUGRIDE, BUGJUICE, QUASARRAT[646]	2018: DOJ charges two members of APT10 in connection with a campaign of global computer intrusions over a decade that targeted managed service providers and more than 45 technology companies for IP and confidential information.[647] The indictment alleged that the defendants worked for a company called Huaying Haitai Science and Technology Development Company (Huaying Haitai) and acted in association with the MSS's Tianjin State Security Bureau.[648]

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
APT9 (a.k.a. Nightshade Panda, FlowerLady, Flowershow)[649]	A cyber threat group composed of freelancers with some degree of state sponsorship that has targeted organizations in the healthcare, pharmaceuticals, construction, engineering, aerospace, and defense industries for data and IP.[650] According to the Institute for Critical Infrastructure Technology, Nightshade Panda (APT9) shares some similarities with Stone Panda (APT10).[651]	*Vectors:* Uses spearphishing, compromised valid accounts, and remote services for initial access.[652] *Malware:* SOGU, HOMEUNIX, PHOTO, FUNRUN, Gh0st, ZXSHEL, PoisonIvy, PlugX[653]	
APT8	A cyber threat group that targets organizations in the media and entertainment, construction, engineering, aerospace, and defense industries for their IP.[654]	*Vectors:* Uses spearphishing emails with malicious attachments or links, exploits vulnerable internet-facing web servers to compromise targets, sends malicious links to victims via instant messaging or chat programs.[655] *Malware:* HASH, FLYZAP, GOLFPRO, SAFEPUTT[656]	
APT7	A cyber threat group that targets organizations in the construction, engineering, aerospace, and defense industrial base industries for their IP.[657] APT7 has targeted organizations headquartered in the United States and UK.[658]	*Vectors:* Uses access to one organization to infiltrate others under the same corporate parent.[659] *Malware:* DIGDUG, TRACKS[660]	
APT6	A cyber threat group likely associated with the Chinese government that targets organizations in the transportation, automotive, construction, engineering, telecommunications, electronic, construction, and materials sectors for valuable data.[661] APT6 has targeted organizations headquartered in the United States and UK.[662] In 2016, the Federal Bureau of Investigation issued an alert about an ongoing cyber campaign that had compromised and stolen data from numerous government and commercial networks over a five-year period, which cybersecurity experts attributed to APT6.[663]	*Vectors:* Uses custom backdoors, including some used by other APT groups.[664] *Malware:* BELUGA, EXCHAIN, PUPTENT[665]	

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
APT5 (a.k.a. Keyhole Panda, MANGANESE, DPD, BRONZE FLEETWOOD, Poisoned Flight, TG-2754)[666]	A cyber threat group active since 2007 that is likely associated with the Chinese government and targets organizations in the telecommunications and technology sectors in the United States, Europe, and Southeast Asia.[667] Mandiant posits that APT5 may be a large threat group consisting of several subgroups with distinct tactics and infrastructure.[668] In 2019, media organizations reported that a subgroup of APT5 had reportedly exploited vulnerabilities in Fortinet and Pulse Secure VPN servers—which are used by a variety of government and corporate organizations—to harvest files with password information or VPN session data.[669]	*Vectors:* Uses malware with keylogging capabilities to target telecommunication companies' employees; compromises networking devices and manipulates the underlying software supporting them.[670] *Malware:* BRIGHTCREST, SWEETCOLA, SPIRITBOX, PALEJAB, WIDERIM, WINVAULT, HAPPYSAD, BIRDWORLD, FARCRY, CYFREE, FULLSILO, HELLOTHEWORLD, HAZELNUT, GIF89A, SCREENBIND, SHINYFUR, TRUCKBED, LEOUNCIA, FREESWIM, PULLTAB, HIREDHELP, NEDDYHORSE, PITCHFORK, BRIGHTCOMB, ENCORE, TABCTENG, SHORTLEASH, CLEANACT, BRIGHTCYAN, DANCEPARTY, HALFBACK, PUSHBACK, COOLWHIP, LOWBID, TIGHTROPE, DIRTYWORD, AURIGA, KEYFANG, Poison Ivy[671]	
APT4 (a.k.a. Maverick Panda, BRONZE EDISON, Sykipot Group, Wisp)[672]	A cyber threat group that targets organizations in the aerospace, defense, industrial engineering, electronics, automotive, government, telecommunications, and transportation sectors.[673] Mandiant notes that APT4 appears to target the defense industrial base more frequently than other commercial organizations.[674] Secureworks observes that BRONZE EDISON has "been linked to intrusions in the fossil fuels, defense and telecoms sectors, with a historic focus on Russia and South Korea."[675] It is not clear whether the group is still active.[676]	*Vectors:* Uses spearphishing messages involving U.S. government, DOD, or defense industrial base themes.[677] *Malware:* GETKYS, LIFESAVER, CCHIP, SHYLILT, SWEETTOOTH, PHOTO, SOGO[678]	

APT Name*	Overview and Targets	Typical Attack Vector for Initial Access/Associated Malware	Charged by U.S. Department of Justice?
APT3 (a.k.a. UPS Team, Gothic Panda, TG-0110, Boyusec, Buckeye)[679]	A cyber threat group associated with the Chinese cybersecurity firm Guangzhou Boyu Information Technology Company, Ltd ("Boyusec"), a known contractor for the MSS.[680] APT3 targets organizations in the aerospace, defense, construction, engineering, high-technology, telecommunications, and transportation sectors.[681] APT3 has carried a number of high-profile cyberespionage campaigns, including Operation Clandestine Fox and Operation Double Tap.[682] According to Symantec, since 2015 APT3 has shifted from targeting U.S.-based victims to political organizations in Hong Kong.[683]	*Vectors:* Uses phishing emails, zero-days vulnerabilities in browsers (e.g., Internet Explorer, Firefox, and Adobe Flash Player).[684] *Malware:* SHOTPUT, COOKIECUTTER, SOGU[685]	2017: DOJ charges three hackers from Boyusec for hacking corporations in the financial, engineering, and technology industries for commercial advantage.[686]
APT2 (a.k.a. Putter Panda, MSUpdater)[687]	A cyber threat group associated with PLA Unit 61486 (formerly of the 12th Bureau of the PLA's 3rd General Staff Department) that targets U.S. and European organizations in the military, satellite, and aerospace sectors for their IP.[688]	*Vectors:* Uses spearphishing emails that exploit a particular vulnerability known as CVE-2012-0158.[689] *Malware:* MOOSE, WARP[690]	
APT1 (a.k.a. Comment Crew, Comment Panda)[691]	A cyber threat group associated with PLA Unit 61398 (formerly of the Second Bureau of the PLA's 3rd General Staff Department) first revealed by Mandiant in a landmark February 2013 report.[692] APT1 has stolen hundreds of terabytes of data from at least 141 organizations in a wide variety of sectors.[693] In 2014, the U.S. government accused APT1 of stealing trade secrets and IP from Westinghouse Electric, U.S. Steel, SolarWorld, United Steel Workers Union, Allegheny Technologies Inc., and Alcoa to benefit Chinese state-owned enterprises.[694] DOJ's indictment against the hackers marked the first time the United States has leveled criminal charges against a foreign country for cyberespionage.[695]	*Vectors:* Uses spearphishing emails with malicious attachments and hyperlinks, then custom backdoors.[696] *Malware:* TROJAN.ECLTYS, BACKDOOR.BARKIOFORK, BACKDOOR.WAKEMINAP, TROJAN.DOWNBOT, BACKDOOR.DALBOT, BACKDOOR.REVIRD, TROJAN.BADNAME, BACKDOOR.WUALESS[697]	2014: DOJ charges five hackers from APT1 with conducting cyberespionage against U.S. companies in the nuclear power, metals, and solar products industries.[698]

Source: Various; compiled by Commission staff.

ENDNOTES FOR SECTION 2

1. Microsoft, "HAFNIUM Targeting Exchange Servers with 0-Day Exploits," March 2, 2021.
2. Nicole Sganga, "'Hack Everybody You Can': What to Know about the Massive Microsoft Exchange Breach," *CBS News*, March 14, 2021; Matthieu Faou, Mathieu Tartare, and Thomas Dupuy, "Exchange Servers under Siege from at Least 10 APT Groups," *We Live Security by ESET*, March 10, 2021; Frank Bajak, Eric Tucker, and Matt O'Brien, "Microsoft Server Hack Has Victims Hustling to Stop Intruders," *Associated Press*, March 8, 2021; Patrick Howell O'Neill, "Four New Hacking Groups Have Joined an Ongoing Offensive against Microsoft's Email Servers," *MIT Technology Review*, March 6, 2021.
3. Robert McMillan and Dustin Volz, "China-Linked Hack Hits Tens of Thousands of U.S. Microsoft Customers," *Wall Street Journal*, March 6, 2021; Brian Krebs, "At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software," *Krebs on Security*, March 5, 2021.
4. White House, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*, July 19, 2021.
5. White House, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*, July 19, 2021.
6. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–5; Nicole Perlroth, "How China Transformed into a Prime Cyber Threat to the U.S.," *New York Times*, July 20, 2021; James Mulvenon, "Chinese Cyber Espionage," testimony for the Congressional-Executive Commission on China, June 25, 2013, 14.
7. CrowdStrike, "*2022 Global Threat Report*," 2022, 16–17.
8. Jordan Robertson and Laurence, "Cyberwar: How Nations Attack without Bullets or Bombs," *Bloomberg*, May 12, 2018; Marie O'Neill Sciarrone, "Cyber Warfare: The New Front," *Catalyst 6 (*Spring 2017); Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38:2 (Fall 2013): 41–46; Mark Thompson, "Panetta Sounds Alarm on Cyber-War Threat," *Time,* October 12, 2012; Conn Hallinan, "Cyber War: Reality or Hype?" *Huffington Post*, March 21, 2012.
9. Andy Greenberg, "The WIRED Guide to Cyberwar," *WIRED*, August 23, 2019; *Fortinet*, "What Is Cyber Warfare?"; Paulo Shakarian, Jana Shakarian, and Andrew Ruef, *Introduction to Cyber Warfare: A Multidisciplinary Approach*, Elsevier, 2013, 2; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, Harper Collins, 2010, 6; John Arquilla and David Ronfeldt, "*Cyberwar Is Coming!" RAND Corporation*, 1993, 30.
10. Eric Heginbotham et al., *"The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power*, 1996–2017," *RAND Corporation*, 2015, 259; Martin C. Libicki, "*Cyberdeterrence and Cyberwar*," *RAND Corporation*, 2009, 8, 117, 139.
11. U.S. Department of the Army, *The Conduct of Information Operations* (ATP 3-13.1), October 4, 2018, 1–1; Catherine A. Theohary, "Information Warfare: Issues for Congress," *Congressional Research Service*, March 5, 2018, 2, 4.
12. *Kurt Baker*, "What Is Cyber Espionage?" *CrowdStrike,* June 1, 2022.
13. *Kurt Baker*, "What Is Cyber Espionage?" *CrowdStrike,* April 1, 2022.
14. National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace*, 2018, 1; Recorded Future, "The Unfortunate Many: How Nation-States Select Targets," July 13, 2017; BAE Systems, "The Nation State Actor: Cyber Threats, Methods and Motivations."
15. Jon R. Lindsay, "Introduction," in Jon R. Lindsay et al., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, 2015, 15.
16. Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informationization" (在网络安全和信息化工作座谈会上的讲话), *Xinhua*, April 19, 2016. Translation.
17. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2; Rogier Creemers et al., "Lexicon: 网络强国 Wangluo Qiangguo," *New America Foundation*, May 31, 2018; Elsa Kania et al., "China's Strategic Thinking on Building Power in Cyberspace," *New America Foundation*, September 25, 2017.

18. Rogier Creemers et al., "Lexicon: 网络强国 Wangluo Qiangguo," *New America Foundation*, May 31, 2018; Graham Webster, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on U.S. Tools to Address Chinese Market Distortions*, June 8, 2018, 5; Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informationization" (在网络安全和信息化工作座谈会上的讲话), *Xinhua*, April 19, 2016. Translation.
19. Rogier Creemers et al., "Lexicon: 网络强国 Wangluo Qiangguo," *New America Foundation*, May 31, 2018.
20. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2; Rogier Creemers et al., "Lexicon: 网络强国 Wangluo Qiangguo," *New America Foundation*, May 31, 2018; Elsa Kania et al., "China's Strategic Thinking on Building Power in Cyberspace," *New America Foundation*, September 25, 2017.
21. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2; CCP Central Commission for Cybersecurity and Informationization, *14th Five-Year Plan for National Informatization* ("十四五" 国家信息化规划), December 2021, 1, 6. Translation; Tianjin Municipal People's Government, *Tianjin Municipal People's Government Office Notice on Printing and Distributing the 14th Five-Year Plan on Smart City Construction in Tianjin* (天津市人民政府办公厅关于印发天津市智慧城市建设"十四五"规划的通知), December 28, 2021. Translation; Fujian Provincial Government's Website Portal, *Explanation of Fujian Province's Special Digital Fujian Plan for the 14th Five-Year Plan* (《福建省"十四五"数字福建专项规划》解读), November 30, 2021. Translation; China's Ministry of Industry and Information Technology, *14th Five-Year Plan Information and Communication Industry Development Plan* ("十四五" 信息通信行业发展规划) November 1, 2021, 1, 6, 8; Georgetown University *Center for Security and Emerging Technology*, "CSET Original Translation: Outline of the People's Republic of China's 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035," May 12, 2021, 38.
22. Greg Austin, *Cybersecurity in China: The Next Wave*, Springer, 2018, 7.
23. Xi Jinping, "Speech at the National Cybersecurity and Informationization Work Conference" (《在全国网络安全和信息化工作会议上的讲话》), April 20, 2018, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 97–98. Translation; Xi Jinping, "Build My Country from a Cyber Great Power into a Cyber Superpower" (习近平：把我国从网络大国建设成为网络强国), *Xinhua*, February 27, 2014. Translation.
24. Xi Jinping, "Speech at the National Cybersecurity and Informationization Work Conference" (《在全国网络安全和信息化工作会议上的讲话》), April 20, 2018, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 43. Translation; Cyberspace Administration of China's Theoretical Studies Center Group, *Deepening the Implementation of General Secretary Xi Jinping's Strategic Thinking on Building China into a Cyber Superpower: Steadily Advancing Cybersecurity and Informationization Work* (深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作), *Qiushi*, September 15, 2017. Translation; Xi Jinping, "Adhering to the Correct Political Direction of the Party's News and Public Opinion Work" (坚持党的新闻舆论工作的正确政治方向), February 19, 2016, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 3.
25. Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 12.
26. Xi Jinping, "Speech at the National Cybersecurity and Informationization Work Conference" (《在全国网络安全和信息化工作会议上的讲话》), April 20, 2018, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 55. Translation; Xi Jinping, "Resolutely Win the Online Ideological Struggle" (坚决打赢网络意识形态斗争), May 20, 2015, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 54. Translation.
27. Li Shao, "The Dilemma of Criticism: Disentangling the Determinants of Media Censorship in China," *Journal of East Asian Studies* 18:3 (November 2018): 279–280; Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows

Government Criticism but Silences Collective Expression," *American Political Science Review* 107:2 (May 2013): 1–2.

28. Sonya Yuan, "Shanghai's Censors Can't Hide Stories of the Dead," *Wired*, June 13, 2022; *Agence France-Presse*, "China's Censors Scrub Viral Shanghai Lockdown Video from Online Platforms," *France24,* April 23, 2022; Pranshu Verma, "Locked Down, Shanghai Residents Skirt Censorship to Vent Online," *Washington Post*, April 22, 2022; Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 12.

29. Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 12.

30. Xi Jinping, "Speech at the National Cybersecurity and Informationization Work Conference" (《在全国网络安全和信息化工作会议上的讲话》), April 20, 2018, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 99–100; Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informationization" (在网络安全和信息化工作座谈会上的讲话), *Xinhua*, April 19, 2016. Translation.

31. Xi Jinping, "Speech at the National Cybersecurity and Informationization Work Conference" (《在全国网络安全和信息化工作会议上的讲话》), April 20, 2018, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 99–100; Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informationization" (在网络安全和信息化工作座谈会上的讲话), *Xinhua*, April 19, 2016. Translation.

32. Xi Jinping, "Speech at the National Cybersecurity and Informationization Work Conference" (《在全国网络安全和信息化工作会议上的讲话》), April 20, 2018, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 41–42; Xi Jinping, "Speech at the 36th Collective Study Session of the 18th Politburo of the CCP" (在十八届中央政治局第三十六次集体学习时的讲话), October 9, 2016, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 39; Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informationization" (在网络安全和信息化工作座谈会上的讲话), *Xinhua*, April 19, 2016. Translation.

33. Xi Jinping, "Speech at the National Cybersecurity and Informationization Work Conference" (《在全国网络安全和信息化工作会议上的讲话》), April 20, 2018, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 41.

34. Xi Jinping, "Speech at the 36th Collective Study Session of the 18th Politburo of the CCP" (在十八届中央政治局第三十六次集体学习时的讲话), October 9, 2016, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 39; Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informationization" (在网络安全和信息化工作座谈会上的讲话), *Xinhua*, April 19, 2016. Translation.

35. Cyberspace Administration of China, *National Cyberspace Security Strategy*, December 27, 2016. Translated by China Copyright and Media.

36. *Xinhua*, "U.S. Intensified 'Hacking Empire' Behavior Threatens Global Cybersecurity" (美国变本加厉的"黑客帝国"行为威胁全球网络安全), June 17, 2022; Rogier Creemers, "China's Cyber Governance Institutions," *Leiden Asia Centre*, January 2021, 2–3; Xi Jinping, "Speech at the National Conference on Propaganda and Ideological Work" (《在全国宣传思想工作会议上的讲话》), August 19, 2013, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 50–51. Translation; Li Dianren, "Pay Attention to Online Ideological Security" (高度重视网络意识形态安全), *Qiushi*, June 15, 2014. Translation.

37. Xi Jinping, "Speech at the National Cybersecurity and Informationization Work Conference" (《在全国网络安全和信息化工作会议上的讲话》), April 20, 2018, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 42–43. Translation; Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informationization" (在网络安全和信息化工作座谈会上的讲话), *Xinhua*, April 19, 2016. Translation; Li Dianren, "Pay Attention to Online Ideological Security" (高度重视网络意识形态安全), *Qiushi*, June 15, 2014. Translation; Steven

Millward, "Support for Windows XP Is Over, but China Still Has 200 Million PCs Using It," *Tech in Asia*, April 9, 2014.

38. Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informationization" (在网络安全和信息化工作座谈会上的讲话), *Xinhua*, April 19, 2016. Translation.

39. Xi Jinping, "Speech at the National Cybersecurity and Informationization Work Conference" (《在全国网络安全和信息化工作会议上的讲话》), April 20, 2018, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 42–43. Translation; Xi Jinping, "Build My Country from a Cyber Great Power into a Cyber Superpower" (习近平：把我国从网络大国建设成为网络强国), *Xinhua*, February 27, 2014. Translation; Xi Jinping, "Speech at the National Conference on Propaganda and Ideological Work" (《在全国宣传思想工作会议上的讲话》), August 19, 2013, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 50–51. Translation.

40. Rogier Creemers, "China's Cyber Governance Institutions," *Leiden Asia Centre*, January 2021, 1–2; Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 25; *Xinhua*, "Central Committee Cybersecurity and Informationization Leading Small Group Established: From Cyber Great Power toward Cyber Superpower" (中央网络安全和信息化领导小组成立：从网络大国迈向网络强国), February 27, 2014. Translation.

41. Rogier Creemers, "China's Cyber Governance Institutions," *Leiden Asia Centre*, January 2021, 1–3; Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 25.

42. Rogier Creemers, "China's Cyber Governance Institutions," *Leiden Asia Centre*, January 2021, 4–6; Rogier Creemers et al., "China's Cyberspace Authorities Set to Gain Clout in Reorganization," *New America Foundation*, March 26, 2018; CCP Central Committee and PRC State Council, *Publication of the Full Text of the Plan for Deepening the Reform of Party and State Agencies* (中共中央印发《深化党和国家机构改革方案》), March 21, 2018. Translation; *Xinhua*, "Central Committee Cybersecurity and Informationization Leading Small Group Established: From Cyber Great Power toward Cyber Superpower" (中央网络安全和信息化领导小组成立：从网络大国迈向网络强国), February 27, 2014. Translation.

43. Rogier Creemers, "China's Cyber Governance Institutions," *Leiden Asia Centre*, January 2021, 4–6; Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 25.

44. Graham Webster, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on U.S. Tools to Address Chinese Market Distortions*, June 8, 2018, 6.

45. Rogier Creemers, "China's Cyber Governance Institutions," *Leiden Asia Centre*, January 2021, 4–6; Rogier Creemers et al., "China's Cyberspace Authorities Set to Gain Clout in Reorganization," *New America Foundation*, March 26, 2018.

46. Samm Sacks, "Beijing Wants to Rewrite the Rules of the Internet," *Atlantic*, June 18, 2018.

47. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 85.

48. Susan Ning and Han Wu, "Cybersecurity 2022," *Chambers and Partners*, March 17, 2022; Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina*, June 29, 2018; Samm Sacks, "Beijing Wants to Rewrite the Rules of the Internet," *Atlantic*, June 18, 2018.

49. Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina*, June 29, 2018.

50. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7; Jane Li, "How China's Top Internet Regulator Became Chinese Tech Giants' Worst Enemy," *Quartz*, August 23, 2021; Paul Triolo et al., "After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come into Focus," *DigiChina*, August 18, 2021; Rogier Creemers, "China's Cyber Governance Institutions," *Leiden Asia Centre*, January 2021, 4–19; U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China*, 2020, 40; Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 25–30; John Fitzsimmons, "Enforcement of China's Multi-Level Protection Scheme: The Rapid Roll-Out of Cyber Security Compliance," *Control Risks*, 2020; Yan Luo and Eric Carlson, "China Enacts Encryption Law," *Covington*, October 31, 2019; Priscilla Moriuchi and Bill Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications," *Recorded Future*, November

16, 2017; Sebastien Heilmann and Lea Shih, "The Central Government," in Sebastien Heilmann, ed., *China's Political System*, Rowman & Littefield, 2017, 80; Rogier Creemers, "Self-Discipline Norms for Internet Search Engine Service Companies on Resisting Obscenity, Sex and Other Such Unlawful and Harmful Information," *China Copyright and Media*, December 22, 2004; Internet Society of China, "Public Pledge of Self-Regulation and Professional Ethics for China's Internet Industry," *Congressional-Executive Committee on China*, July 19 2022; *Associated Press*, "China Sites Pledge to Be Nice," July 15, 2002.

51. Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina*, June 29, 2018.

52. Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina,* June 29, 2018; Jack Wagner, "China's Cybersecurity Law: What You Need to Know," *Diplomat*, June 1, 2017.

53. Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina,* June 29, 2018; KPMG China IT Advisory, "*Overview of China's Cybersecurity Law*," February 2017, 5.

54. Lauren Maranto, "Who Benefits from China's Cybersecurity Laws?" *Center for Strategic and International Studies*, July 25, 2020; Jyh-An Lee, "Hacking into China's Cybersecurity Law," *Wake Forest Law Review* 53 (2018): 57.

55. Susan Ning and Han Wu, "Cybersecurity 2022," *Chambers and Partners*, March 17, 2022; Nikolay Bozhkov, China's Cyber Diplomacy: A Primer, *EU Cyber Direct*, March 2020, 22.

56. China's Ministry of Industry and Information Technology, State Internet Information Office, and the Ministry of Public Security, *Regulations on the Management of Security Vulnerabilities in Network Products* (工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知), July 13, 2021. Translation.

57. Devin Thorne and Samantha Hoffman, "China's Vulnerability Disclosure Regulations Put State Security First," *ASPI Strategist*, August 31, 2021; Catalin Cimpanu, "Chinese Government Lays Out New Vulnerability Disclosure Rules," *Record*, July 14, 2021; *China Law Translate*, "Provisions on the Management of Network Product Security Vulnerabilities," July 14, 2021; China's Ministry of Industry and Information Technology, State Internet Information Office, and the Ministry of Public Security, *Regulations on the Management of Security Vulnerabilities in Network Products* (工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知), July 13, 2021. Translation.

58. Devin Thorne and Samantha Hoffman, "China's Vulnerability Disclosure Regulations Put State Security First," *ASPI Strategist*, August 31, 2021.

59. Devin Thorne and Samantha Hoffman, "China's Vulnerability Disclosure Regulations Put State Security First," *ASPI Strategist*, August 31, 2021.

60. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 14.

61. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 1; Xu Wen, "Dialogue with the Director of the National Cybersecurity Talent and Innovation Base" (许雯, "对话国家网安基地办主任：网络安全人才要放到'战场'上培养), *Beijing News*, September 18, 2020.

62. Zhu Lixin, "Integrated Development Urged for Cybersecurity," *China Daily*, September 6, 2022; Cao Yin, "Nation Faces 'Talent Gap' in Cybersecurity," *China Daily*, December 13, 2017.

63. Georgetown University *Center for Security and Emerging Technology*, "Research Report on the Status of China's Information Security Professionals: 2018–2019" (中国信息安全从业人员现状调研报告:2018–2019 年度), September 6, 2019, 5, 16.

64. Xu Wen, "Dialogue with the Director of the National Cybersecurity Talent and Innovation Base" (许雯, "对话国家网安基地办主任：网络安全人才要放到'战场'上培养), *Beijing News*, September 18, 2020. Translation.

65. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 13; Dakota Cary, "What China's Vast New Cybersecurity Center Tells Us about Beijing's Ambitions," *Defense One*, July 23, 2021; Dave Liu, "Beijing's Costly Plans for Cybersecurity 'Self-Sufficiency,'" *Protocol*, July 20, 2021; Xu Wen, "Dialogue with the Director of the National Cybersecurity Talent and Innovation Base" (许雯, 对话国家网安基地办主任：网络安全人才要放到'战场'上培养), *Beijing News*, September 18, 2020. Translation; Greg Austin and Wenze Lu, "Five Years of Cyber Security Education Reform in China," in Greg Austin, ed., *Cybersecurity Education: Principles and Policies*, Routledge, 2020; *Xinhua*,

"Xi Jinping Gives Speech at Cybersecurity and Informationization Work Conference," April 19, 2016.
66. Rogier Creemers, "National Cyberspace Security Strategy," *China Copyright and Media*, December 27, 2016.
67. Rogier Creemers, "National Cyberspace Security Strategy," *China Copyright and Media*, December 27, 2016.
68. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Georgetown University Center for Security and Emerging Technology*, July 2021, 1–2.
69. Ministry of Education of the People's Republic of China, *Notice on Printing and Distributing the "Administrative Measures for the Construction of Demonstration Projects of First-Class Network Security Colleges"* (关于印发《一流网络安全学院建设示范项目管理办法》的通知), August 15, 2017. Translation.
70. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 11; Dakota Cary, *China's CyberAI Talent Pipeline*, Center for Security and Emerging Technology, July 2021, 1.
71. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Georgetown University Center for Security and Emerging Technology*, July 2021, 11, 29.
72. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Georgetown University Center for Security and Emerging Technology*, July 2021, 11, 29.
73. M. Taylor Fravel, *Active Defense: China's Military Strategy since 1949*, Princeton University Press, 2019, 187–188.
74. Japan's National Institute for Defense Studies, *NIDS China Security Report 2021: China's Military Strategy in the New Era*, 2021, 26; M. Taylor Fravel, *Active Defense: China's Military Strategy Since 1949*, Princeton University Press, 2019, 188–189.
75. Dean Cheng, "How China's Thinking about the Next War," *Breaking Defense*, May 19, 2021; Japan's National Institute for Defense Studies, *NIDS China Security Report 2021: China's Military Strategy in the New Era*, 2021, 26; Edmund J. Burke et al., "People's Liberation Army Operational Concepts," *RAND Corporation*, 2020, 4; M. Taylor Fravel, *Active Defense: China's Military Strategy since 1949*, Princeton University Press, 2019, 188–189.
76. Japan's National Institute for Defense Studies, *NIDS China Security Report 2021: China's Military Strategy in the New Era*, 2021, 26; Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 115.
77. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in Phillip Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, National Defense University Press, 2019, 463; Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 101; Timothy L. Thomas, "Chinese and American Network Warfare," *Joint Force Quarterly* 38 (2005): 77.
78. John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support Force: A 'Joint' Force for Information Operations," in Joel Wuthnow et al., eds., *The PLA beyond Borders: Chinese Military Operations in Regional and Global Context*, NDU Press, 2021, 151–152; Kevin L. Pollpeter et al., "The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations," RAND Corporation, 2017, 1.
79. Elsa Kania, "China: Active Defense in the Cyber Domain," *Diplomat*, June 12, 2015; China's State Council Information Office, *China's Military Strategy*, May 5, 2015.
80. Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informationization" (在网络安全和信息化工作座谈会上的讲话), *Xinhua*, April 19, 2016, cited in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 94–95.
81. China's State Council Information Office, *China's National Defense in the New Era*, July 2019.
82. Catherine A. Theohary, "Information Warfare: Issues for Congress," *Congressional Research Service*, March 5, 2018, 1.
83. Catherine A. Theohary, "Information Warfare: Issues for Congress," *Congressional Research Service*, March 5, 2018, 2, 4.
84. Edmund J. Burke et al., "People's Liberation Army Operational Concepts," *RAND Corporation*, 2020, 13–14; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 148. Translation; M. Tay-

lor Fravel, *Active Defense: China's Military Strategy since 1949*, Princeton University Press, 2019, 219; Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, November 27, 2012, I-1–I-8.

85. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 248; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 235. Translation; Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 95, 137; Catherine A. Theohary, "Information Warfare: Issues for Congress," *Congressional Research Service*, March 5, 2018, 3; Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, November 27, 2012, I-1.

86. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in Phillip Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, National Defense University Press, 2019, 441, 479; Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 129. Translation.

87. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3; Li Jidong and Chen Zhou, "On Strategic Cyber Warfare" (试论战略网络战), *China Military Science* 6 (2017): 47. Translation; Eric Heginbotham et al., "*The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power*, 1996–2017," *RAND Corporation*, 2015, 259; Martin C. Libicki, "*Cyberdeterrence and Cyberwar*," *RAND Corporation*, 2009, 8, 117–118, 139.

88. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3; Li Jidong and Chen Zhou, "On Strategic Cyber Warfare" (试论战略网络战), *China Military Science* 6 (2017): 47.

89. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 248; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 235. Translation.

90. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 248; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 235. Translation.

91. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 39–40.

92. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 416; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 403. Translation.

93. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 163; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 150. Translation.

94. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 163; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 150. Translation.

95. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 99.

96. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 99; Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 192–193. Translation.

97. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 420; Xiao Tianliang, ed., The Science of Military Strategy (战略学), National Defense University Press, Beijing, 2020, 407–408. Translation; Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 100.

98. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 420; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 407–408. Translation.

99. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 418; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 405. Translation; Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 100; Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 192. Translation.

100. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 418; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 405. Translation; Shou

Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 192. Translation.

101. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 100.

102. Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 192. Translation.

103. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 418; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 405. Translation.

104. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 418; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 405. Translation; Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 100; Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 192–193. Translation.

105. Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 192–193. Translation.

106. Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 193. Translation.

107. Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 193. Translation.

108. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 419–420; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 406–407. Translation; Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 101; Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 192–193. Translation.

109. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 419–420; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 406–407. Translation; Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 193. Translation.

110. Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 193. Translation.

111. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 420; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 407. Translation.

112. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 420; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 407. Translation.

113. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 420; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 407. Translation.

114. Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, 2015, 152.

115. Dean Cheng, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.

116. Dean Cheng, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 11–15; Chris Jaikaran, "Cybersecurity: Deterrence Policy," *Congressional Research Service*, January 18, 2022, 4–5; Erica Lonergan and Jacquelyn Schneider, "Cyber Challenges for the New National Defense Strategy," *War on the Rocks*, December 17, 2021; U.S. Department of Defense, *Remarks by Secretary of Defense Lloyd J. Austin III at the Reagan National Defense Forum (As Delivered)*, December 4, 2021; Jacquelyn G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare*, May 10, 2019.

117. Shou Xiaosong, ed., *The Science of Military Strategy* (战略学), Military Science Press, 2013, 193. Translation.

118. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 165; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 152–153. Translation.

119. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 165; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 152. Translation.

120. China Aerospace Studies Institute, In Their Own Words: Science of Military Strategy 2020, January 2020, 165; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 152–153. Translation.
121. Dean Cheng, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 12.
122. Dean Cheng, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 12.
123. Dean Cheng, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 30.
124. Dean Cheng, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 30.
125. Dean Cheng, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 14; Yuan Yi, "AMS Experts Reveal the Secrets of Cyberspace Deterrence" (军科院专家揭秘网络空间威慑), *China Military Online*, January 5, 2016. Translation.
126. Dean Cheng, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States,* February 17, 2022, 14–15. Yuan Yi, "AMS Experts Reveal the Secrets of Cyberspace Deterrence" (军科院专家揭秘网络空间威慑), *China Military Online*, January 5, 2016. Translation.
127. Dean Cheng, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 15.
128. Yuan Yi, "AMS Experts Reveal the Secrets of Cyberspace Deterrence" (军科院专家揭秘网络空间威慑), *China Military Online*, January 5, 2016. Translation.
129. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4.
130. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4; Herb Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 6:3 (Fall 2012): 51–52.
131. Herb Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 6:3 (Fall 2012): 51–52.
132. China Aerospace Studies Institute, *In Their Own Words: Science of Military Strategy 2020*, January 2020, 248; Xiao Tianliang, ed., *The Science of Military Strategy* (战略学), National Defense University Press, Beijing, 2020, 235. Translation.
133. Dean Cheng, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 68.
134. Ben Buchanan and Fiona S. Cunningham, "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis," *Texas National Security Review* 3:4 (Fall 2020): 58, 71.
135. Dean Cheng, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 76–77.
136. Dean Cheng, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 77; Winnona DeSombre, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 77.
137. Dean Cheng, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 77; Winnona DeSombre, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 77.
138. International Institute for Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment*, June 28, 2021, 10–12; Julia Voo et al., "National Cyber Power Index 2020," *Belfer Center*, September 2020, 8.

139. International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," June 28, 2021, 7, 174.
140. International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," June 28, 2021, 174; Helen Warrel, "China's Cyber Power at Least a Decade behind the US, New Study Finds," *Financial Times*, June 27, 2021.
141. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3; Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Georgetown University Center for Security and Emerging Technology*, July 2021, 1; International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," June 28, 2021, 89; Matthew Bey, "Great Powers in Cyberspace: The Strategic Drivers Behind U.S., Chinese and Russian Competition," *Cyber Defense Review* 3:3 (Fall 2018): 32.
142. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3–6.
143. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6.
144. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6; Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8; Shannon Vavra, "The World's Top Cyber Powers," *Axios*, April 13, 2017.
145. Emilio Iasiello, "Don't Rely on Tiered Rankings to Measure Cyber Power," *Oodaloop*, July 13, 2021.
146. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7–8; Emilio Iasiello, "Don't Rely on Tiered Rankings to Measure Cyber Power," *Oodaloop*, July 13, 2021.
147. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8.
148. International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," June 28, 2021, 3; Julia Voo et al., "National Cyber Power Index 2020," *Belfer Center*, September 2020, 38.
149. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6.
150. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, April 9, 2021, 8.
151. International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," June 28, 2021, 97–98.
152. CrowdStrike, "2022 Global Threat Report," 2022, 16–17; James Sadowski, "Zero Tolerance: More Zero-Days Exploited in 2021 than Ever Before," *Mandiant*, April 21, 2022.
153. Jacquelyn Schneider, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 9.
154. International Institute for Strategic Studies, "Chapter Ten: Military Cyber Capabilities," in *The Military Balance*+ 122:1 (2022): 508.
155. Greg Austin, "How Good Are China's Cyber Defenses?" *Diplomat*, July 11, 2018; Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informationization" (在网络安全和信息化工作座谈会上的讲话), *Xinhua*, April 19, 2016. Translation.
156. International Institute for Strategic Studies, "Chapter Ten: Military Cyber Capabilities," in *The Military Balance*+ 122:1 (2022): 509.
157. International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," June 28, 2021, 95.
158. International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," June 28, 2021, 95.
159. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 7; *Bloomberg News*, "Secretive Chinese Committee Draws Up List to Replace U.S. Tech," November 16, 2021.

160. *Bloomberg News*, "Secretive Chinese Committee Draws Up List to Replace U.S. Tech," November 16, 2021.
161. *Bloomberg News*, "China Orders Government, State Firms to Dump Foreign PCs," May 5, 2022.
162. *Bloomberg News*, "China Orders Government, State Firms to Dump Foreign PCs," May 5, 2022.
163. International Institute for Strategic Studies, "Chapter Ten: Military Cyber Capabilities," in *The Military Balance*+ 122:1 (2022): 509.
164. Dakota Cary, "Down Range: A Survey of China's Cyber Ranges," *Center for Security and Emerging Technology*, September 2022, 3–4, 6, 15.
165. Dakota Cary, "Down Range: A Survey of China's Cyber Ranges," *Center for Security and Emerging Technology*, September 2022, 15–16.
166. Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, 2015, 152.
167. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8; Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," *Recorded Future*, February 28, 2021, 1; Charlie Osborne, "Taiwan's Major Oil Refineries Struck by Malware, Causing Chaos at Gas Stations," *Daily Swig*, May 6, 2020; *Taiwan News*, "Taiwan's CPC Suffers Malware Attack, Experiences System Outage," May 4, 2020.
168. CyCraft Technology Corp, "China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware," *Medium*, June 1, 2021; Taiwan's Ministry of Justice, *Description of the Investigation into the Ransomware Attack on Important Domestic Enterprises* (國內重要企業遭勒索軟體攻擊事件調查說明), May 15, 2020. Translation; Charlie Osborne, "Taiwan's Major Oil Refineries Struck by Malware, Causing Chaos at Gas Stations," *Daily Swig*, May 6, 2020; *Taiwan News*, "Taiwan's CPC Suffers Malware Attack, Experiences System Outage," May 4, 2020.
169. Charlie Osborne, "Taiwan's Major Oil Refineries Struck by Malware, Causing Chaos at Gas Stations," *Daily Swig*, May 6, 2020; *Taiwan News*, "Taiwan's CPC Suffers Malware Attack, Experiences System Outage," May 4, 2020.
170. Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector amid Heightened Border Tensions," *Recorded Future*, February 28, 2021, 1, 7–8.
171. Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector amid Heightened Border Tensions," *Recorded Future*, February 28, 2021, 1.
172. Insikt Group, "Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group," *Recorded Future*, April 6, 2022.
173. Keoni Everington, "China Launches 272 Attempts at Spreading Disinformation in Taiwan in a Week," *Taiwan News*, August 8, 2022; Hsia Hsiao-hwa and Raymond Chung, "China Steps Up Cyberattacks, Disinformation Campaigns Targeting Taiwan," *Radio Free Asia*, August 8, 2022; Ryan Serabian and Daniel Kapellmann Zafra, "Pro-PRC 'HaiEnergy' Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites," *Mandiant*, August 4, 2022; A.A. Bastien, "China Is Stepping Up Its Information War on Taiwan," *Foreign Policy*, August 2, 2022.
174. Keoni Everington, "China Launches 272 Attempts at Spreading Disinformation in Taiwan in a Week," *Taiwan News*, August 8, 2022.
175. Taiwan FactCheck Center, "[Error] Online Photo 'PLA Navy Officers and Soldiers Watched Taiwan's Hualien Peace Power Plant from Close Range, Cruising Taiwan's Coastline'?" (【錯誤】網傳照片「解放軍海軍官兵近距離目視台灣花蓮和平電廠，巡航台灣海岸線」?), August 9, 2022. Translation; Keoni Everington, "China Launches 272 Attempts at Spreading Disinformation in Taiwan in a Week," *Taiwan News*, August 8, 2022; Taiwan FactCheck Center, "[Error] Internet Video: The Missile Launched by the People's Liberation Army Crossed the Island of Taiwan, and the Shooting Location Is Suspected to Be in Yilan'?" (【錯誤】網傳影片「解放軍發射的導彈穿越台灣島，拍攝位置疑似在宜蘭」？), August 8, 2022. Translation; Kathrin Hille, "Chinese Aircraft Simulate Attack on Taiwan's Main Island," *Financial Times*, August 7, 2022; Sophia Yang, "China's Xinhua Releases Photo of Warship Nearing Taiwan's Power Station," *Taiwan News*, August 6, 2022; Taiwan FactCheck Center, "[Error] Internet Video 'China Sent Rocket Launchers to Fujian to Attack Taiwan'?" (【錯誤】網傳影片「中國派火箭發射器至福建攻擊台灣」？), August 5, 2022. Translation; Taiwan FactCheck Center, "[Error] Online Photo: 3 Bombers Hovering over Taipei?" (【錯誤】網傳圖片「3架轟炸機在台北上方盤旋」？) August 3, 2022. Translation.

176. *Reuters*, "Taiwan Defense Ministry: Website Hit by Cyber Attacks amid China Tensions," August 3, 2022; Yimou Lee and Christopher Bing, "Attacks on Taiwan Websites Likely Work of Chinese 'Hacktivists'—Researchers," *Reuters*, August 2, 2022.

177. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in Phillip Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, National Defense University Press, 2019, 497–498.

178. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7–8; John Chen, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 80.

179. John Chen, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 72; John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8.

180. Greg Austin, presentation at virtual event "China's Weak Cyber Defenses," International Institute for Strategic Studies, Wednesday June 3, 2020; Greg Austin, *Cybersecurity in China: The Next Wave*, Springer, 2018, 1–3, 113.

181. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.

182. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3.

183. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4–5; International Institute of Strategic Studies, "Chapter Ten: Military Cyber Capabilities," in *The Military Balance+* 122:1 (2022): 509.

184. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3–6; John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6

185. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in Phillip Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, National Defense University Press, 2019, 438.

186. John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support Force: A 'Joint' Force for Information Operations," in Joel Wuthnow et al., eds., *The PLA beyond Borders: Chinese Military Operations in Regional and Global Context*, NDU Press, 2021, 164; John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in Phillip Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, National Defense University Press, 2019, 449–450.

187. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4.

188. John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support Force: A 'Joint' Force for Information Operations," in Joel Wuthnow et al., eds., *The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context*, NDU Press, 2021, 151.

189. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in Phillip Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, National Defense University Press, 2019, 449–450.

190. Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* (Spring 2018): 112.

191. John Chen, interview with Commission staff, April 26, 2022; John Chen, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 50; John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4.

192. John Chen, interview with Commission staff, April 26, 2022; John Chen, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 50.

193. Counter Threat Unit Research Team, "ShadowPad Malware Analysis," *Secureworks*, February 15, 2022; Cylance Research and Intelligence Team, "Reaver: Mapping Connections between Disparate Chinese APT Groups," *Blackberry Blog*, May 14, 2019.

194. Counter Threat Unit Research Team, "ShadowPad Malware Analysis," *Secureworks*, February 15, 2022.

195. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7; Lucian Constantin, "ShadowPad Has Become the RAT of Choice for Several State-Sponsored Chinese APTs," *CSO Online*, February 15, 2022; Counter Threat Research Unit Team, "ShadowPad Malware Analysis," *Secureworks*, February 15, 2022; Phillip C. Saunders, "Beyond Borders: PLA Command and Control of Overseas Operations," *National Defense University*, July 2020, 5; Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," *FireEye*, 2019, 10.

196. Jonathan Cheng and Josh Chin, "China Hacked South Korea over Missile Defense, U.S. Firm Says," *Washington Post*, April 21, 2017.

197. Counter Threat Research Unit Team, "ShadowPad Malware Analysis," *Secureworks*, February 15, 2022; *Secureworks*, "BRONZE GENEVA"; Phillip C. Saunders, "Beyond Borders: PLA Command and Control of Overseas Operations," *National Defense University*, July 2020, 5; Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," *FireEye*, 2019, 9; Kyaw Pyiyt Htet, "Naikon," *Mitre*, May 31, 2017; Threat Connect and Defense Group Incorporated, "CAMERASHY: Closing the Aperture on China's Unit 78020," 2015, 15.

198. Kyaw Pyiyt Htet, "Naikon," *Mitre*, May 31, 2017; Threat Connect and Defense Group Incorporated, "CAMERASHY: Closing the Aperture on China's Unit 78020," 2015, 15–16.

199. Counter Threat Unit Research Team, "ShadowPad Malware Analysis," *Secureworks*, February 15, 2022; Insikt Group, "Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries," *Recorded Future,* June 16, 2021, 1; Phillip C. Saunders, "Beyond Borders: PLA Command and Control of Overseas Operations," *National Defense University*, July 2020, 5.

200. Insikt Group, "Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries," *Recorded Future,* June 16, 2021, 3.

201. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7; Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 44.

202. U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China*, 2020, 62; John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, National Defense University, October 2018, 17.

203. Yossef Bodansky, "The Real Culprit: The PLA's Strategic Support Force," *Institute for Strategic, Political, Security and Economic Consultancy* 669 (February 2020): 4; John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, National Defense University, October 2018, 28–29.

204. John Chen, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 50.

205. Dean Cheng, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 30.

206. Dean Cheng, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 30.

207. Dean Cheng, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 30.

208. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7.

209. John Chen, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 49.
210. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7.
211. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7.
212. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7.
213. Devin Thorne, interview with Commission staff, May 2, 2022; John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.
214. Devin Thorne, interview with Commission staff, May 2, 2022; U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China*, 2021, 72.
215. John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support Force: A 'Joint' Force for Information Operations," in Joel Wuthnow et al., eds., *The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context*, NDU Press, 2021, 162.
216. Mark Pomerleau, "Military Cyber Software Developers Fix Weaknesses, Create Mission Tools Faster," *C4ISRNet*, September 8, 2021.
217. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4, 6; Chang Chengyang et al., "Polarity Analysis of Dynamic Political Sentiments from Tweets with Deep Learning Method" (基于深度学习方法对特定群体推特的动态政治情感极性分析), *Data Analysis and Data Discovery* 51:3 (March 2021): 121–131. Translation; Yuan Qingjun et al., "An Improved Template Analysis Method Based on Power Traces Preprocessing with Manifold Learning" (基于流形学习能量数据预处理的模板攻击优化方法), *Journal of Electronics and Information Technology* 42:8 (2020): 1853–1861. Translation; Hu Yongjin et al., "Method to Generate Cyber Deception Traffic Based on Adversarial Sample" (基于对抗样本的网络欺骗流量生成方法), *Journal on Communications* 41:9 (September 2020): 59–70. Translation; Zhang Zhigang, "Research on Smart Electrical Power Monitoring and Control Sensors" (电力监控网络安全态势智能感知方法研究), PhD degree dissertation, *PLA Strategic Support Force Information Engineering University*, 2019. Translation; Qu Qiang, "Research on Spam User Detection on Social Networks" (社交网络垃圾用户检测关键 技术研究), Master's degree dissertation, *PLA Strategic Support Force Information Engineering University*, 2019. Translation; Wang Shuwei et al., "Review of Malware Adversarial Sample Generation on Generative Adversarial Networks" (基于生成对抗网络的恶意软件对抗样本生成综述), *Journal of Information Engineering University* 20:5 (2019): 616–621. Translation; Li Bicheng et al., "Intelligent Agent Model for Network Public Opinion Guidance" (网络舆情引导智能代理模型), *National Defense Technology* 40:3 (June 2019): 73–77. Translation; Melanie Lee, "Top China College in Focus with Ties to Army's Cyber-Spying Unit," *Reuters*, March 23, 2013.
218. Insikt Group, "China's PLA Unit 61419 Purchasing Foreign Antivirus Products, Likely for Exploitation," *Recorded Future*, May 5, 2021.
219. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6.
220. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6; Zhang Zhigang, "Research on Smart Electrical Power Monitoring and Control Sensors" (电力监控网络安全态势智能感知方法研究), PhD degree dissertation, *PLA Strategic Support Force Information Engineering University*, 2019. Translation.
221. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6; Hu Yongjin et al., "Method to Generate Cyber Deception Traffic Based on Adversarial Sample" (基于对抗样本的网络欺骗流量生成方法), *Journal on Communications* 41:9 (September 2020): 59–70. Translation; Wang Shuwei et al., "Review of Malware Adversarial Sample Generation

on Generative Adversarial Networks" (基于生成对抗网络的恶意软件对抗样本生成综述), *Journal of Information Engineering University* 20:5 (2019): 616–621. Translation.

222. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6; Guo Xiaoyu, "Research on User Identification across Social Networks" (跨社交网络用户身份识别技术研究), Master's degree dissertation, *PLA Strategic Support Force Information Engineering University*, 2020. Translation; Li Bicheng et al., "Intelligent Agent Model for Network Public Opinion Guidance" (网络舆情引导智能代理模型), *National Defense Technology* 40:3 (June 2019): 73–77. Translation; Qu Qiang, "Research on Spam User Detection on Social Networks" (社交网络垃圾用户检测关键 技术研究), Master's degree dissertation, *PLA Strategic Support Force Information Engineering University*, 2019. Translation.

223. Li Minghai, "Reflections on the Strategy of Civil-Military Fusion in the Network Information System" (网络信息体系军民融合战略的思考), *Network Communication Magazine* (November 12, 2018). Translation.

224. Devin Thorne, interview with Commission staff, May 2, 2022; John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.

225. Devin Thorne, interview with Commission staff, May 2, 2022; Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias," in Jon R. Lindsay et al., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, 2015, 193.

226. Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias," in Jon R. Lindsay et al., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, 2015, 195.

227. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 13.

228. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 14, 16–17.

229. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 20.

230. Dakota Cary, "Down Range: A Survey of China's Cyber Ranges," *Center for Security and Emerging Technology*, September 2022, 16.

231. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 13.

232. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 13.

233. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 13; China Defense Universities Tracker, "Chinese Academy of Engineering Physics," *Australian Strategic Policy Institute*, May 5, 2021.

234. Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias," in Jon R. Lindsay et al., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, 2015, 202.

235. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5; John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support Force: A 'Joint' Force for Information Operations," in Joel Wuthnow et al., eds., *The PLA beyond Borders: Chinese Military Operations in Regional and Global Context*, NDU Press, 2021, 160.

236. John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support Force: A 'Joint' Force for Information Operations," in Joel Wuthnow et al., eds., *The PLA beyond Borders: Chinese Military Operations in Regional and Global Context*, NDU Press, 2021, 160.

237. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8.

238. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8–9.
239. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.
240. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.
241. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 8.
242. Insikt Group, "Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and 'New-Type' Militias," *Recorded Future*, March 10, 2022, 8.
243. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–3.
244. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–3.
245. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3; Alex Joske, "The China Defense Universities Tracker: Exploring the Military and Security Links of China's Universities," *Australian Strategic Policy Institute*, November 25, 2019, 6, 8.
246. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.
247. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4; Southeast University, "Huang Wei, Vice Minister of Science and Technology, Inspected the Purple Mountain Network Communication and Security Laboratory" (科技部副部长黄卫考察网络通信与安全紫金山实验室), May 10, 2019. Translation; Wu Chan, "'Purple Mountain Network Communications and Security Laboratory' Was Formally Uncurtained," *Southeast University*, September 5, 2018.
248. Dakota Cary, "Academics, AI, and APTs: How Six Advanced Persistent Threat-Connected Universities Are Advancing AI Research," *Center for Security and Emerging Technology*, March 2021, 13.
249. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4.
250. China Defense Universities Tracker, "Shanghai Jiao Tong University," *Australian Strategic Policy Institute*, November 18, 2019; China Defense Universities Tracker, "Southeast University," *Australian Strategic Policy Institute*, November 12, 2019; Bryan Krekel et al., "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," prepared for the U.S.-China Economic and Security Review Commission, March 7, 2012, 59–62, 110.
251. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.
252. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6–7; Li Guoli and Zong Zhaodun, "Strategic Support Force to Cooperate with Nine Local Organizations to Cultivate High-End Talents for New Combat Forces" (战略支援部队与地方 9 个单位合作培养新型作战力量高端人才), *Xinhua*, July 12, 2017. Translation.
253. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6–7; Li Guoli and Zong Zhaodun, "Strategic Support Force to Cooperate with Nine Local Organizations to Cultivate High-End Talents for New Combat Forces" (战略支援部队与地方 9 个单位合作培养新型作战力量高端人才), *Xinhua*, July 12, 2017. Translation.
254. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5; Dakota Cary, "Down Range:

A Survey of China's Cyber Ranges," *Center for Security and Emerging Technology*, September 2022, 14.

255. Dakota Cary, "Down Range: A Survey of China's Cyber Ranges," *Center for Security and Emerging Technology*, September 2022, 14–15.

256. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 7, 9; Jiang Jie, "China Unveils Its First Civil-Military Cybersecurity Innovation Center," *People's Daily*, December 28, 2017.

257. *Qingdao Local Treasure*, "2021 Qingdao 360 City Safety Brain Information Experience Week Appointment Entrance" (2021青岛360城市安全大脑信息体验周预约入口), September 16, 2021. Translation; Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 7.

258. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 2, 9.

259. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 26; Wang Su and Jiang Shan, "In a Race against Time to 'Build a Platform' for the Enterprise: The First Network Security Attack and Defense Laboratory of the Network Security Base Was Completed This Month" (争分夺秒为企业"搭台"，网安基地首个网络安全攻防实验室本月建成), *Yangtze River Network*, September 17, 2020. Translation.

260. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 26–27; Mark Stokes et al., "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049*, November 11, 2011, 6.

261. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 27.

262. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 27.

263. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8; Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 27.

264. Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain," *Center for Security and Emerging Technology*, July 2021, 28.

265. Jiang Jie, "China Unveils Its First Civil-Military Cybersecurity Innovation Center," *People's Daily*, December 28, 2017.

266. Jiang Jie, "China Unveils Its First Civil-Military Cybersecurity Innovation Center," *People's Daily*, December 28, 2017.

267. Li Guoli, "Jointly Build an Integrated Innovation Platform to Deal with Cyberspace Security Threats" (军地联手搭建融合创新平台　应对网络空间安全威胁), *Economic Information Daily*, December 28, 2017. Translation.

268. *Qingdao Local Treasure*, "2021 Qingdao 360 City Safety Brain Information Experience Week Appointment Entrance" (2021青岛360城市安全大脑信息体验周预约入口), September 16, 2021. Translation.

269. Zhang Zhongyu, "Network Security Urgently Requires the Development of Military-Civilian Integration" (网络安全亟须军民融合发展), *PLA Daily*, February 2, 2018. Translation.

270. Dakota Cary, oral testimony for U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 139; Dakota Cary, written testimony for U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5–6.

271. Dakota Cary, oral testimony for U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 139; Dakota Cary, written testimony for U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5–6.

272. Dakota Cary, written testimony for U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5–6.
273. Dakota Cary, oral testimony for U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 139.
274. Dakota Cary, written testimony for U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6.
275. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2; Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–3; Neil Jenkins, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8.
276. Nicole Perlroth, "How China Transformed into a Prime Cyber Threat to the U.S.," *New York Times*, July 20, 2021; James Mulvenon, written testimony for the Congressional-Executive Commission on China, *Hearing on Chinese Hacking: Impact on Human Rights and Commercial Rule of Law*, June 25, 2013, 14.
277. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 2013.
278. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2; Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–3; Paul Mozur and Chris Buckley, "Spies for Hire: China's New Breed of Hackers Blends Espionage and Entrepreneurship," *New York Times*, August 26, 2021; Nicole Perlroth, "How China Transformed into a Prime Cyber Threat to the U.S.," *New York Times*, July 20, 2021.
279. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2, 6.
280. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3.
281. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 84.
282. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 84; Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 9.
283. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6; Ben Blanchard, Benjamin Kang Lim, and Philip Wen, "Exclusive: Xi Confidant Set to Become China's New Spy Master—Sources," *Reuters*, February 28, 2018; State Council Library of Ministry and Commission Figures, *Minister of State Security Biographical Notes* (国安部部长简历). Translation.
284. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 84–85; Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5–7.
285. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6; Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina*, June 29, 2018; Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*, July 20, 2017; China Law Translate, "National Intelligence Law of the P.R.C. (2017)," June 27, 2017.

286. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6; Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*, July 20, 2017; China Law Translate, "National Intelligence Law of the P.R.C. (2017)," June 27, 2017.

287. Dakota Cary, written testimony for U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8; Devin Thorne and Samantha Hoffman, "China's Vulnerability Disclosure Regulations Put State Security First," *ASPI Strategist*, August 31, 2021; Catalin Cimpanu, "Chinese Government Lays Out New Vulnerability Disclosure Rules," *Record*, July 14, 2021; China Law Translate, "Provisions on the Management of Network Product Security Vulnerabilities," July 14, 2021; China's Ministry of Industry and Information Technology, and the Ministry of Public Security State Internet Information Office, *Regulations on the Management of Security Vulnerabilities in Network Products* (工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知), July 13, 2021. Translation.

288. Zach Dorfman, "Tech Giants Are Giving China a Vital Edge in Espionage," *Foreign Policy*, December 23, 2020.

289. Zach Dorfman, "Tech Giants Are Giving China a Vital Edge in Espionage," *Foreign Policy*, December 23, 2020.

290. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8.

291. Emily Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows that US User Data Has Been Repeatedly Accessed from China," *BuzzFeed News*, June 17, 2022.

292. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 85; Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.

293. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 84; Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.

294. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 84.

295. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 10.

296. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 10.

297. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 85; Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 13, 15.

298. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7.

299. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7–8; Insikt Group, "China's Cybersecurity Law Gives the Ministry of State Security Unprecedented New Powers over Foreign Technology," *Recorded Future*, August 31, 2017; Rogier Creemers, "China's Cyber Governance Institutions," *Leiden Asia Centre*, January 2021, 17; Jon R. Lindsay, "Introduction," in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, 2015, 11.

300. Priscilla Moriuchi and Bill Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications," *Recorded Future*, November 16, 2017.
301. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7; Priscilla Moriuchi and Bill Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications," *Recorded Future*, November 16, 2017.
302. Priscilla Moriuchi and Bill Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications," *Recorded Future*, November 16, 2017.
303. Priscilla Moriuchi and Bill Ladd, "China Altered Public Vulnerability Data to Conceal MSS Influence," *Recorded Future*, March 9, 2018.
304. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7.
305. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3; Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8.
306. Lucian Constantin, "ShadowPad Has Become the RAT of Choice for Several State-Sponsored Chinese APTs," *CSO Online*, February 15, 2022.
307. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8–9.
308. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8–9.
309. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6.
310. J.D. Work, "China Flaunts Its Offensive Cyber Power," *War on the Rocks*, October 22, 2021.
311. Waqas, "iPhone 13 Pro, Windows, Chrome, Linux and Others Pwned at Tianfu Cup," *Hackread*, October 18, 2021; *Dark Reading*, "China's Hackers Crack Devices at Tianfu Cup for $1.5M in Prizes," October 15, 2021.
312. J.D. Work, "China Flaunts Its Offensive Cyber Power," *War on the Rocks*, October 22, 2021; Patrick Howell O'Neill, "How China Turned a Prize-Winning iPhone Hack against the Uyghurs," *MIT Technology Review*, May 6, 2021; Ravie Lakshmanan, "Chinese Hackers Using New iPhone Hack to Spy on Uyghur Muslims," *Hacker News*, April 22, 2020; Andrew Case et al., "Evil Eye Threat Actor Resurfaces with iOS Exploit and Updated Implant," *Volexity*, April 21, 2020.
313. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4, 6.
314. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2, 6–7, 9.
315. John Chen, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
316. Lucian Constantin, "Report: China Supported C919 Airliner Development through Cyberespionage," *CSO Online*, October 14, 2019; Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," *FireEye*, 2019, 11; U.S. Department of Justice, *Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years*, October 30, 2018.
317. Adam Kozy, CEO and Founder of SinaCyber, interview with Commission staff, June 15, 2022; Catalin Cimpanu, "US Charges Two Chinese Intelligence Officers 'and Their Team of Hackers,'" *ZDNet*, October 30, 2018.
318. Adam Kozy, CEO and Founder of SinaCyber, interview with Commission staff, June 15, 2022; Catalin Cimpanu, "US Charges Two Chinese Intelligence Officers 'and Their Team of Hackers,'" *ZDNet*, October 30, 2018.

319. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 10.
320. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 10.
321. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 7, 10.
322. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 10.
323. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 165.
324. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 11.
325. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 11.
326. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 11.
327. U.S. Department of Justice, *Chengdu 404 Indictment*, 2019, 2, 6.; Nalani Fraser et al., "APT41: A Dual Espionage and Cyber Crime Operation," *Mandiant*, August 7, 2019.
328. U.S. Department of Justice, *Chengdu 404 Indictment*, 2019, 6.
329. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 11.
330. U.S. Department of Justice, *U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage*, November 27, 2017; Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security behind APT3," *Recorded Future*, May 17, 2017; Intrusion Truth, "APT3 Is Boyusec, a Chinese Intelligence Contractor," May 9, 2017; Bill Gertz, "Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service," *Washington Free Beacon*, November 29, 2016.
331. Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security behind APT3," *Recorded Future*, May 17, 2017; Intrusion Truth, "APT3 Is Boyusec, a Chinese Intelligence Contractor," May 9, 2017.
332. U.S. Department of Justice, *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, December 20, 2018; Philip Wen, "China Denies 'Slanderous' Economic Espionage Charges from U.S., Allies," *Reuters*, December 20, 2018; Intrusion Truth, "APT10 Was Managed by the Tianjin Bureau of the Chinese Ministry of State Security," August 15, 2018.
333. Dakota Cary, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 160; Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
334. Australian Strategic Policy Institute, China Defense Universities Tracker, "Shanghai Jiao Tong University," November 18, 2019; David Barboza, "Hacking Inquiry Puts China's Elite in New Light," *New York Times*, February 21, 2010.
335. Alex Joske, "The China Defense Universities Tracker: Exploring the Military and Security Links of China's Universities," *Australian Strategic Policy Institute*, 2019, 13.
336. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3; Dakota Cary, "Academics, AIs, and APTs: How Six Advanced Persistent Threat-Connected Chinese Universities Are Advancing AI Research," *Georgetown University Center for Security and Emerging Technology*, March 2021, 5; Intrusion Truth, "Who Is Mr. Gu?" January 10, 2020.

337. Dakota Cary, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3.
338. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
339. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
340. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
341. Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," *FireEye*, 2019, 15.
342. Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," *FireEye*, 2019, 14.
343. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.
344. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.
345. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.
346. Carly Page, "China-Backed APT41 Compromised 'At Least' Six U.S. State Governments," *TechCrunch*, March 8, 2022; Rufus Brown et al., "Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments," *Mandiant*, March 8, 2022; U.S. Department of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection with Computer Intrusion Campaigns against More than 100 Victims Globally*, September 16, 2020.
347. U.S. Department of Justice, *Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research*, Monday, July 19, 2021; Scott Henderson et al., "Chinese Espionage Group TEMP.Periscope Targets Cambodia ahead of July 2018 Elections and Reveals Broad Operations Globally," *Mandiant*, July 10, 2018.
348. Elizabeth Culliford and Raphael Satter, "Chinese Hackers Used Facebook to Target Uighurs Abroad, Company Says," *Reuters*, March 24, 2021; Jack Stubbs, "China Hacked Asian Telcos to Spy on Uighur Travelers: Sources," *Reuters*, September 5, 2019.
349. Jeff Daniels, "Chinese Theft of Sensitive US Military Technology Is Still a 'Huge Problem,' Says Defense Analyst," *CNBC News*, November 9, 2017.
350. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 12.
351. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3.
352. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4, 16–19, 24.
353. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6.
354. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 16; U.S. Department of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection with Computer Intrusion Campaigns against More than 100 Victims Globally*, September 16, 2020; U.S. Department of Justice, *Chengdu 404 Indictment*, August 11, 2020, 24.
355. U.S. Department of Justice, *Chengdu 404 Indictment*, August 11, 2020, 24.
356. U.S. Department of Justice, *Chengdu 404 Indictment*, August 11, 2020, 24–25.
357. Adam Kozy, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 16.

358. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
359. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
360. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
361. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
362. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–3; *Fortinet*, "What Is an Exploit?"
363. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3; Ang Cui, "The Overlooked Problem of 'N-Day' Vulnerabilities," *Dark Reading*, March 26, 2018.
364. Kelli Vanderlee, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 119.
365. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3.
366. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3.
367. Dan Perez et al., "Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day," *Mandiant*, April 20, 2021; Charlie Osborne, "Everything You Need to Know about the Microsoft Exchange Server Hack," *ZDNet*, April 19, 2021.
368. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3.
369. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3–4.
370. Kelli Vanderlee, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 119–120.
371. Kelli Vanderlee, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 119; Raymond Leong, Dan Perez, and Tyler Dean, "MESSAGETAP: Who's Reading Your Text Messages?" *Mandiant*, October 31, 2019; *Cyware Hacker News*, "Nine Managed Service Providers Including HPE and IBM Targeted in APT10 Attacks," December 21, 2018; Christopher Bing, Jack Stubbs, and Joseph Menn, "Exclusive: China Hacked HPE, IBM and Then Attacked Clients—Sources," *Reuters*, December 20, 2018.
372. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4.
373. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4.
374. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4.
375. Kelli Vanderlee, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 120; Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4–5.
376. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.

377. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.

378. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5; Mandiant, "APT41, A Dual Espionage and Cyber Crime Operation," 2021, 21; SecureList by Kaspersky, "Operation ShadowHammer: A High-Profile Supply Chain Attack," April 23, 2019; Kim Zetter, "Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers," *Motherboard*, March 25, 2019; *Kaspersky Daily*, "ShadowHammer: Malicious Updates for ASUS Laptops," March 25, 2019.

379. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5.

380. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.

381. Kelli Vanderlee, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.

382. Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution,* June 2, 2017, 3–4.

383. Xi Jinping, *Speech at the National Cybersecurity and Informationization Work Conference* (《在全国网络安全和信息化工作会议上的讲话》), April 20, 2018, in *Excerpts from Xi Jinping's Discussions on Strengthening the Country through the Internet* (习近平关于网络强国论述摘编), edited by Central Literature Publishing House, Beijing, 2021, 42–43. Translation; Lu Wei, "Persisting in Respect for the Principle of Cyber Sovereignty, Promoting the Construction of a Community of Common Destiny in Cyberspace," *DigiChina*, March 2, 2016.

384. Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 86; Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, June 2, 2017, 1.

385. Xinchuchu Gao, "An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model," *International Spectator*, May 27, 2022; Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution,* June 2, 2017, 14; Adam Segal, "China's Internet Conference: Xi Jinping's Message to Washington," *Council on Foreign Relations*, December 16, 2015.

386. Adam Segal, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 174.

387. Yukon Huang and Jeremy Smith, "China's Record on Intellectual Property Rights Is Getting Better and Better," *Foreign Policy*, October 16, 2019; James Andrew Lewis, "Put China's Intellectual Property Theft in a Larger Context," *Center for Strategic & International Studies*, August 15, 2017.

388. Adam Kozy, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 159; Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 4–5; Derek Scissors, "The Rising Risk of China's Intellectual-Property Theft," *National Review*, July 16, 2021; Lorand Laskai and Adam Segal, "A New Old Threat Countering the Return of Chinese Industrial Cyber Espionage," *Council on Foreign Relations*, December 6, 2018; Ben Buchanan and Robert D. Williams, "A Deepening U.S.-China Cybersecurity Dilemma," *Lawfare*, October 24, 2018; Shane Harris, "Chinese Theft Continues in Cyberspace as New Threats Emerge, U.S. Intelligence Officials Warn," *Washington Post*, July 26, 2018.

389. Adam Segal, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 175–176.

390. Kelli Vanderlee, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 158.

391. Kelli Vanderlee, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 158.

392. Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 16; Robert Morgus and Justin Sherman, "The Idealized Internet vs. Internet Realities (Version 1.0)," *New America Foundation*, July 26, 2018; Henry Farrell, "Promoting Norms for Cyberspace," *Council on Foreign Relations*, April 6, 2015; White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, May 2011, 9.
393. Robert Morgus and Justin Sherman, "The Idealized Internet vs. Internet Realities (Version 1.0)," *New America Foundation*, July 26, 2018, 14.
394. Robert Morgus and Justin Sherman, "The Idealized Internet vs. Internet Realities (Version 1.0)," *New America Foundation*, July 26, 2018.
395. Xi Jinping, "Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference," *China's Ministry of Foreign Affairs*, December 16, 2015.
396. Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 16–17.
397. Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, June 2, 2017, 3, 7.
398. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, April 9, 2021, 8.
399. Winnona DeSombre, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
400. Edward Wong, Matthew Rosenberg, and Julian E. Barnes, "Chinese Agents Helped Spread Messages that Sowed Virus Panic in U.S., Officials Say," *New York Times*, April 22, 2020, updated January 5, 2021.
401. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–3; Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 36–37.
402. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2.
403. Harold Hongju Koh, "International Law in Cyberspace," *Harvard International Law Journal* 54 (December 2012): 3–4.
404. Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 36–37.
405. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2; Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 37.
406. Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 36; Brandon S. Davis, "State Cyber Operations and International Law: Russian and Western Approaches," Thesis Presented in Partial Fulfillment of the Requirements for the Degree Master of Arts in the Graduate School of the Ohio State University, Ohio State University, 2018, 48.
407. Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 37.
408. Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 95.
409. Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 95.
410. Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 95.
411. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–3.
412. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2; UN Group of Governmental Experts, "Report of the Group of Governmental Experts on Developments in the Field

of Information and Telecommunications in the Context of International Security," A/70/174, July 22, 2015, 7–8.

413. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 2–3; UN Group of Governmental Experts, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, July 22, 2015, 7–8; UN Group of Governmental Experts, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, June 24, 2013, 8.

414. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3.

415. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3; Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 32–33.

416. Adina Ponta, "Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes," *American Society of International Law* 25:14 (July 30, 2021); Dan Efrony, "The UN Cyber Groups, GGE and OEWG—A Consensus Is Optimal, but Time Is of the Essence," *Just Security*, July 16, 2021.

417. United Nations Open-Ended Working Group, "Chair's Summary," March 10, 2021, 4; International Committee of the Red Cross, Comments on the "Substantive Report [First Draft] of the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security," March 3, 2021, 1–2.

418. Adam Segal, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 3.

419. Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 96.

420. Sarah McKune and Shazeda Ahmed, "The Contestation and Shaping of Cyber Norms through China's Internet Sovereignty Agenda," *International Journal of Communication* 12 (2018): 7; NATO Cooperative Cyber Defense Center of Excellence, "Information Security Discussed at the Dushanbe Summit of the Shanghai Cooperation Organization," 2014.

421. UN General Assembly, "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General," A/69/723, January 13, 2015; Henry Roigas, "An Updated Draft of the Code of Conduct Distributed in the United Nations—What's New?" *NATO Cooperative Cyber Defense Center of Excellence*, 2015.

422. Luca Belli, "BRIC Countries to Build Digital Sovereignty," *Open Democracy*, November 18, 2019.

423. Nikolay Bozhkov, *China's Cyber Diplomacy: A Primer*, EU Cyber Direct, March 2020, 40; *Xinhua*, "Full Text: International Strategy of Cooperation on Cyberspace," March 1, 2017.

424. Lukasz Kobierski, "Digital Cooperation between China and the Arab Leagues," *Warsaw Institute*, April 8, 2021; China's Ministry of Foreign Affairs, *China-League of Arab States Cooperation Initiative on Data Security*, March 29, 2021.

425. Liu Xuan, "Data Security Pact with Arab States Provides Model," *China Daily*, April 13, 2021; Wendy Wu, "China Hails Arab Data Security Pact amid Battle for Cyber Influence," *South China Morning Post*, March 31, 2021.

426. Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 94–95.

427. Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 94–95.

428. Jiaxing Li, "China's World Internet Conference Goes 'International' as Beijing Seeks to Promote its Own Vision of Global Cyberspace," *South China Morning Post*, July 13, 2022; Adam Segal, "China's Vision for Cyber Sovereignty and the Global Gov-

ernance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 91, 97.

429. Jiaxing Li, "China's World Internet Conference Goes 'International' as Beijing Seeks to Promote its Own Vision of Global Cyberspace," *South China Morning Post*, July 13, 2022; Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 91, 97; World Internet Conference, "2014 WIC Overview," November 12, 2015.

430. Elliott Zaagman, "Cyber Sovereignty Cuts Both Ways," *Lowy Institute*, August 7, 2020; Justin Sherman, "How Much Cyber Sovereignty Is Too Much Cyber Sovereignty?" *Council on Foreign Relations*, October 30, 2019; Franz-Stefan Gady, "The Wuzhen Summit and the Battle over Internet Governance," *Diplomat*, January 14, 2016.

431. Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 97.

432. Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace," in Nadège Rolland, ed., *An Emerging China-Centric Order: China's Vision for a New World Order in Practice*, National Bureau of Asian Research 87 (August 2020): 97; Josh Horwitz, "Starting This Weekend, China Celebrates Its "Open" Internet after a Year of Unprecedented Censorship," *Quartz*, December 1, 2017.

433. Josh Horwitz, "Starting This Weekend, China Celebrates Its 'Open' Internet after a Year of Unprecedented Censorship," *Quartz*, December 1, 2017; *Xinhua*, "Xi to Attend 2nd World Internet Conference," December 10, 2015.

434. Council of Europe, "The Budapest Convention on Cybercrime: Benefits and Impact in Practice," July 13, 2020, 2; Council of Europe, "The Budapest Convention and Its Protocols."

435. Jennifer Daskal and Debrae Kennedy-Mayo, "Budapest Convention: What Is It and How Is It Being Updated?" *Cross-Border Data Forum*, July 2, 2020; Council of Europe, "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY."

436. Alex Grigsby, "Coming Soon: Another Country to Ratify the Budapest Convention," *Council on Foreign Relations*, December 11, 2014.

437. Summer Walker, "The Quixotic Quest to Tackle Global Cybercrime," *Foreign Policy*, February 11, 2022; David Ignatius, "How Russia and China Are Attempting to Rewrite Cyberworld Order," *Washington Post*, March 30, 2021.

438. Summer Walker, "The Quixotic Quest to Tackle Global Cybercrime," *Foreign Policy*, February 11, 2022; David Ignatius, "How Russia and China Are Attempting to Rewrite Cyberworld Order," *Washington Post*, March 30, 2021.

439. Katitza Rodriguez and Karen Gullo, "Negotiations over UN Cybercrime Treaty Under Way in New York, with EFF and Partners Urging Focus on Human Rights," *Electronic Frontier Foundation*, March 3, 2022; Deborah Brown, "Cybercrime Is Dangerous, but a New UN Treaty Could Be Worse for Rights," *Human Rights Watch*, August 13, 2021; *Associated Press*, "UN Approves Timetable for New Treaty to Combat Cybercrime," May 27, 2021.

440. Deborah Brown, "Cybercrime Is Dangerous, but a New UN Treaty Could Be Worse for Rights," *Human Rights Watch*, August 13, 2021.

441. Jacquelyn Schneider, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 9.

442. Stavros Atlamazoglou, "Chinese Espionage against America Steals up to $600 Billion a Year," *SandBoxx*, February 12, 2022.

443. Jennifer R. Franks, testimony for the U.S. House of Representatives Committee on Oversight and Reform, U.S. Government Accountability Office, January 11, 2022, i, 6–7.

444. Jacquelyn Schneider, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 8.

445. Jacquelyn Schneider, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 225.

446. C. Todd Lopez, "Cyber Mission Force Set to Add More Teams," *DOD News*, April 6, 2022; Mark Pomerleau, "Here's How DoD Organizes Its Cyber Warriors," *C4ISRNet*, July 25, 2017.

447. Jacquelyn Schneider, oral testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 225–226.
448. Microsoft, "Microsoft Digital Defense Report," October 2021, 54.
449. Neil Jenkins, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 10; Paul Rosenzweig, "Is It Really 85 Percent?" *Lawfare*, May 11, 2021.
450. Neil Jenkins, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 10.
451. Neil Jenkins, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 10.
452. Neil Jenkins, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 10.
453. Neil Jenkins, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 5–7.
454. Neil Jenkins, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6–7.
455. Neil Jenkins, written testimony for the U.S.-China Economic and Security Review Commission, *Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, February 17, 2022, 6.
456. International Institute for Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment*, June 28, 2021, 7.
457. International Institute for Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment*, June 28, 2021, 7.
458. *Covington*, "China Enacts New National Security Law," July 2, 2015, 3; National Security Law of the People's Republic of China (中华人民共和国国家安全法), July 1, 2015. Translation.
459. National Security Law of the People's Republic of China (中华人民共和国国家安全法), July 2015. Translation.
460. Ninth Amendment to the Criminal Law of the People's Republic of China (中华人民共和国刑法修正案(九)), 2015. Translation.
461. Ninth Amendment to the Criminal Law of the People's Republic of China (中华人民共和国刑法修正案(九)), 2015. Translation.
462. U.S.-China Business Council, "Unofficial Translation of the Counter-Terrorism Law of the People's Republic of China," December 27, 2015.
463. U.S.-China Business Council, "Unofficial Translation of the Counter-Terrorism Law of the People's Republic of China," December 27, 2015.
464. Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina*, June 29, 2018.
465. Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina*, June 29, 2018.
466. Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina*, June 29, 2018.
467. Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina*, June 29, 2018.
468. Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *DigiChina*, June 29, 2018.
469. Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*, July 20, 2017; China Law Translate, "National Intelligence Law of the P.R.C. (2017), June 27, 2017.
470. Yingzhi Yang, "China Discourages Its Hackers from Foreign Competitions So They Don't Help Others," *South China Morning Post*, March 21, 2018; Chris Bing, "China's Government Is Keeping Its Security Researchers from Attending Conferences," *Cyber Scoop*, March 8, 2018.
471. Yan Luo and Eric Carlson, "China Enacts Encryption Law," *Covington*, October 31, 2019; Cryptography Law of the People's Republic of China, 2019.
472. Yan Luo and Eric Carlson, "China Enacts Encryption Law," *Covington*, October 31, 2019; Cryptography Law of the People's Republic of China, 2019.
473. Law of the People's Republic of China on National Defense, 2020.
474. DigiChina, "Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)," June 29, 2021.

475. Rogier Creemers et al., "Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021)," *DigiChina*, August 18, 2021; Paul Triolo et al., "After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come into Focus," *DigiChina*, August 18, 2021.
476. Rogier Creemers et al., "Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021)," *DigiChina*, August 18, 2021; Paul Triolo et al., "After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come into Focus," *DigiChina*, August 18, 2021.
477. Rogier Creemers et al., "Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021)," *DigiChina*, August 18, 2021; Paul Triolo et al., "After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come into Focus," *DigiChina*, August 18, 2021.
478. Devin Thorne and Samantha Hoffman, "China's Vulnerability Disclosure Regulations Put State Security First," *ASPI Strategist*, August 31, 2021; Catalin Cimpanu, "Chinese Government Lays Out New Vulnerability Disclosure Rules," *Record*, July 14, 2021; China's Ministry of Industry and Information Technology, State Internet Information Office, and the Ministry of Public Security, *Regulations on the Management of Security Vulnerabilities in Network Products* (工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知), July 13, 2021. Translation.
479. Devin Thorne and Samantha Hoffman, "China's Vulnerability Disclosure Regulations Put State Security First," *ASPI Strategist*, August 31, 2021; Catalin Cimpanu, "Chinese Government Lays Out New Vulnerability Disclosure Rules," *Record*, July 14, 2021; China's Ministry of Industry and Information Technology, State Internet Information Office, and the Ministry of Public Security, *Regulations on the Management of Security Vulnerabilities in Network Products* (工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知), July 13, 2021. Translation.
480. Devin Thorne and Samantha Hoffman, "China's Vulnerability Disclosure Regulations Put State Security First," *ASPI Strategist*, August 31, 2021; Catalin Cimpanu, "Chinese Government Lays Out New Vulnerability Disclosure Rules," *Record*, July 14, 2021; China's Ministry of Industry and Information Technology, State Internet Information Office, and the Ministry of Public Security, *Regulations on the Management of Security Vulnerabilities in Network Products* (工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知), July 13, 2021. Translation.
481. Devin Thorne and Samantha Hoffman, "China's Vulnerability Disclosure Regulations Put State Security First," *ASPI Strategist*, August 31, 2021; Catalin Cimpanu, "Chinese Government Lays Out New Vulnerability Disclosure Rules," *Record*, July 14, 2021; China's Ministry of Industry and Information Technology, State Internet Information Office, and the Ministry of Public Security, *Regulations on the Management of Security Vulnerabilities in Network Products* (工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知), July 13, 2021. Translation.
482. Rogier Creemers and Graham Webster, "Translation: Cybersecurity Review Measures (Revised)—Effective Feb. 15, 2022," *DigiChina*, January 10, 2022.
483. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 79.
484. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 79.
485. M. Taylor Fravel, *Active Defense: China's Military Strategy Since 1949*, Princeton University Press, 2019, 219.
486. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 99.
487. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 99.
488. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in Phillip Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, National Defense University Press, 2019, 465.
489. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 81–82.
490. Edmund J. Burke et al., "People's Liberation Army Operational Concepts," *RAND Corporation*, 2020, 8.
491. Edmund J. Burke et al., "People's Liberation Army Operational Concepts," *RAND Corporation*, 2020, 8.
492. Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 101–102; Eric Heginbotham et al., "The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017," *RAND Corporation*, 2015, 274.
493. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in Phillip Saunders et al., eds., *Chairman Xi Remakes the PLA: As-*

sessing Chinese Military Reforms, National Defense University Press, 2019, 446–447; Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks*, January 30, 2018.

494. @BushidoToken, "Threat Group Naming Schemes in Cyber Threat Intelligence," *Curated Intelligence*, May 20, 2022.

495. Kevin Townsend, "What's in a Threat Group Name? An Inside Look at the Intricacies of Nation-State Attribution," *SecurityWeek*, October 6, 2021.

496. Kevin Townsend, "What's in a Threat Group Name? An Inside Look at the Intricacies of Nation-State Attribution," *SecurityWeek*, October 6, 2021; Florian Roth, "The Newcomer's Guide to Cyber Threat Actor Naming," *Medium*, March 25, 2018.

497. Kevin Townsend, "What's in a Threat Group Name? An Inside Look at the Intricacies of Nation-State Attribution," *SecurityWeek*, October 6, 2021.

498. Florian Roth, "The Newcomer's Guide to Cyber Threat Actor Naming," *Medium*, March 25, 2018; Florian Roth, "APT Groups and Operations."

499. Florian Roth, "The Newcomer's Guide to Cyber Threat Actor Naming," *Medium*, March 25, 2018.

500. CrowdStrike, "Wicked Panda"; Federal Bureau of Investigation, *APT 41 GROUP*; Mandiant, "Advanced Persistent Threats (APTs)"; U.S. Department of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection with Computer Intrusion Campaigns against More than 100 Victims Globally*, September 16, 2020.

501. Intrusion Truth, "APT41: A Case Study," July 20, 2022; Mandiant, "Advanced Persistent Threats (APTs)"; Nalani Fraser et al., "APT41: A Dual Espionage and Cyber Crime Operation," *Mandiant*, August 7, 2019.

502. Mandiant, "Advanced Persistent Threats (APTs)".

503. U.S. Department of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection with Computer Intrusion Campaigns against More than 100 Victims Globally*, September 16, 2020.

504. Carly Page, "China-Backed APT41 Compromised 'at Least' Six US State Governments," *TechCrunch*, March 8, 2022; Rufus Brown et al., "Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments," *Mandiant*, March 8, 2022.

505. Mandiant, "Advanced Persistent Threats (APTs)"; Hara Hiroaki and Ted Lee, "APT41 Resurfaces as Earth Baku with New Cyberespionage Campaign," *Trend Micro*, August 24, 2021.

506. Mandiant, "Advanced Persistent Threats (APTs)"; Hara Hiroaki and Ted Lee, "APT41 Resurfaces as Earth Baku with New Cyberespionage Campaign," *Trend Micro*, August 24, 2021.

507. U.S. Department of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection with Computer Intrusion Campaigns against More than 100 Victims Globally*, September 16, 2020.

508. Mandiant, "Advanced Persistent Threats (APTs)"; Cybersecurity & Infrastructure Security Agency, *Alert (AA21-200A): Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department*, July 19, 2021.

509. Mandiant, "Advanced Persistent Threats (APTs)"; MITRE ATT&CK, "Leviathan," April 15, 2022; U.S. Cybersecurity and Infrastructure Security Agency, *Alert (AA21-200A): Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department*, July 19, 2021; Fred Plan et al., "APT40: Examining a China-Nexus Espionage Actor," *Mandiant*, March 4, 2019.

510. U.S. Cybersecurity and Infrastructure Security Agency, *Alert (AA21-200A): Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department*, July 19, 2021.

511. Kurt Mackie, "White House Says China's APT40 Responsible for Exchange Hacks, Ransomware Attacks," *Redmond*, July 19, 2021.

512. Mandiant, "Advanced Persistent Threats (APTs)."

513. Mandiant, "Advanced Persistent Threats (APTs)."

514. U.S. Department of Justice, *Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research*, Monday, July 19, 2021.

515. Suleyman Ozarslan, "Tactics, Techniques, and Procedures (TTPs) Used by HAFNIUM to Target Microsoft Exchange Servers," *Picus Security*, March 10, 2021.

516. National Counterintelligence and Security Center, "HAFNIUM Compromises MS Exchange Servers," *Office of the U.S. Director of National Intelligence*, August 19, 2021.

517. White House, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*, July 19, 2021.
518. Suleyman Ozarslan, "Tactics, Techniques, and Procedures (TTPs) Used by HAFNIUM to Target Microsoft Exchange Servers," *Picus Security*, March 10, 2021.
519. Malwarebytes Labs, "Backdoor.Hafnium."
520. Sergiu Gatlan, "Google: Chinese Hackers Target Gmail Users Affiliated with US Govt," *Bleeping Computer*, March 8, 2022.
521. Mandiant, "Advanced Persistent Threats (APTs)"; United Kingdom's National Cyber Security Centre, *UK and Allies Hold Chinese State Responsible for Pervasive Pattern of Hacking*, July 19, 2021; Tom Burt, "New Cyberattacks Targeting U.S. Elections," *Microsoft*, September 10, 2020.
522. Sergiu Gatlan, "Google: Chinese Hackers Target Gmail Users Affiliated with US Govt," *Bleeping Computer*, March 8, 2022.
523. Mandiant, "Advanced Persistent Threats (APTs)"; Sekoia, "Walking on APT31 Infrastructure Footprints," November 10, 2021.
524. Mandiant, "Advanced Persistent Threats (APTs)"; Sekoia, "Walking on APT31 Infrastructure Footprints," November 10, 2021.
525. Secureworks, "BRONZE GENEVA."
526. Mandiant, "Advanced Persistent Threats (APTs)"; FireEye, "APT30 and the Mechanics of a Long-Running Cyber Espionage Operation," April 2015, 3.
527. FireEye, "APT30 and the Mechanics of a Long-Running Cyber Espionage Operation," April 2015, 4.
528. MITRE ATT&CK, "Naikon."
529. Mandiant, "Advanced Persistent Threats (APTs)."
530. Mandiant, "Advanced Persistent Threats (APTs)."
531. MITRE ATT&CK, "Naikon."
532. MITRE ATT&CK, "Naikon"; Kurt Baumgartner and Maxim Golovkin, "The Naikon APT," *SecureList by Kaspersky*, May 14, 2015.
533. Kyaw Pyiyt Htet, "Naikon," *Mitre*, May 31, 2017; Threat Connect and Defense Group Incorporated, "CAMERASHY: Closing the Aperture on China's Unit 78020," 2015, 1, 15–16.
534. Ionut Ilascu, "New 'Aria-Body' Backdoor Gets Advanced Hackers Back in the Spy Game," *Bleeping Computer*, May 7, 2020; Threat Connect and Defense Group International, "Project Camerashy: Closing the Aperture on China's Unit 78020," 2019, 15; Kurt Baumgartner and Maxim Golovkin, "The MsnMM Campaigns: The Earliest Naikon APT Campaigns," May 2015, 3–4.
535. Florian Roth, "APT Groups and Operations."
536. Secureworks, "BRONZE HUNTLEY"; MITRE ATT&CK, "Tonto Team."
537. Counter Threat Research Unit Team, "ShadowPad Malware Analysis," *Secureworks*, February 15, 2022; Phillip C. Saunders, "Beyond Borders: PLA Command and Control of Overseas Operations," *National Defense University*, July 2020, 5; Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," *FireEye*, 2019, 10.
538. Jonathan Cheng and Josh Chin, "China Hacked South Korea over Missile Defense, U.S. Firm Says," *Washington Post*, April 21, 2017.
539. Daniel Lunghi and Jaromir Horejsi, "Tonto Team: Exploring the TTPs of an Advanced Threat Actor Operating a Large Infrastructure," *TrendMicro*, October 2, 2020, 7.
540. Secureworks, "BRONZE HUNTLEY."
541. Counter Threat Research Unit Team, "ShadowPad Malware Analysis," *Secureworks*, February 15, 2022; Insikt Group, "Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries," *Recorded Future,* June 16, 2021, 1; Phillip C. Saunders, "Beyond Borders: PLA Command and Control of Overseas Operations," *National Defense University*, July 2020, 5.
542. Insikt Group, "Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries," *Recorded Future,* June 16, 2021, 3.
543. Morgan Dembroski et al., "China Cyber Attacks: The Current Threat Landscape," *Iron Net*, October 26, 2021; Insikt Group, "Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries," *Recorded Future,* June 16, 2021, 3.
544. Insikt Group, "Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries," *Recorded Future,* June 16, 2021, 2.
545. Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector amid Heightened Border Tensions," *Recorded Future*, February 28, 2021, 1.
546. Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector amid Heightened Border Tensions," *Recorded Future*, February 28, 2021, 1.

547. Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector amid Heightened Border Tensions," *Recorded Future*, February 28, 2021, 1.
548. Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector amid Heightened Border Tensions," *Recorded Future*, February 28, 2021, 1.
549. Insikt Group, "RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations," *Recorded Future*, August 16, 2022, 1.
550. Insikt Group, "RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations," *Recorded Future*, August 16, 2022; Insikt Group, "RedAlpha: New Campaigns Discovered Targeting the Tibetan Community," *Recorded Future*, June 26, 2018, 1.
551. Insikt Group, "RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations," *Recorded Future*, August 16, 2022, 4–5.
552. Insikt Group, "RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations," *Recorded Future*, August 16, 2022, 4.
553. Insikt Group, "RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations," *Recorded Future*, August 16, 2022, 2.
554. *Cyware*, "APT27: An In-Depth Analysis of a Decade-Old Active Chinese Threat Group," March 29, 2022.
555. Mandiant, "Advanced Persistent Threats (APTs)"; MITRE ATT&CK, "Threat Group-3390"; Secureworks, "Threat Profiles: BRONZE UNION."
556. Lisa Brownlee, "China-Based Cyber Attacks on US Military Are 'Advanced, Persistent and Ongoing': Report," *Forbes*, September 17, 2015.
557. *Cyware*, "APT27: An In-Depth Analysis of a Decade-Old Active Chinese Threat Group," March 29, 2022; Steve Zurier, "Chinese Espionage Group APT27 Moves into Ransomware," January 5, 2021.
558. Sergiu Gatlan, "German Govt Warns of APT27 Hackers Backdooring Business Networks," *Bleeping Computer*, January 26, 2022.
559. *Cyware*, "APT27: An In-Depth Analysis of a Decade-Old Active Chinese Threat Group," March 29, 2022.
560. Mandiant, "Advanced Persistent Threats (APTs)."
561. Mandiant, "Advanced Persistent Threats (APTs)"; Catalin Cimpanu, "Building China's Comac C919 Airplane Involved a Lot of Hacking, Report Says," *ZDNet*, October 14, 2019.
562. Mandiant, "Advanced Persistent Threats (APTs)"; Nalani Fraser and Kelli Vanderlee, "Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions," *FireEye*, 2019, 11.
563. Pierluigi Paganini, "China-Linked Cyberspies Turbine PANDA Targeted Aerospace Firms for Years," *Security Affairs*, October 18, 2019; Catalin Cimpanu, "Building China's Comac C919 Airplane Involved a Lot of Hacking, Report Says," *ZDNet*, October 14, 2019.
564. Catalin Cimpanu, "Building China's Comac C919 Airplane Involved a Lot of Hacking, Report Says," *ZDNet*, October 14, 2019.
565. Mandiant, "Advanced Persistent Threats (APTs)."
566. Mandiant, "Advanced Persistent Threats (APTs)"; CrowdStrike, "2015 Global Threat Report," 2015, 19.
567. U.S. Department of Justice, *Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years*, October 30, 2018.
568. Mandiant, "Advanced Persistent Threats (APTs)."
569. Mandiant, "Advanced Persistent Threats (APTs)."
570. Mandiant, "Advanced Persistent Threats (APTs)."
571. Mandiant, "Advanced Persistent Threats (APTs)."
572. Mandiant, "Advanced Persistent Threats (APTs)."
573. Mandiant, "Advanced Persistent Threats (APTs)."
574. Mandiant, "Advanced Persistent Threats (APTs)."
575. Eduard Kovacs, "'Pitty Tiger' Threat Actors Possibly Active since 2008: FireEye," *SecurityWeek*, August 1, 2014.
576. Mandiant, "Advanced Persistent Threats (APTs)."
577. Mandiant, "Advanced Persistent Threats (APTs)."
578. Malpedia, "Pirate Panda."
579. Mandiant, "Advanced Persistent Threats (APTs)"; Robert Lemos, "China-Linked Group Attacked Taiwanese Financial Firms for 18 Months," *Dark Reading*,

February 4, 2022; Anomali, "Anomali Suspects that China-Backed APT Pirate Panda May Be Seeking Access to Vietnam Government Data Center," April 30, 2020.
580. Mandiant, "Advanced Persistent Threats (APTs)"; Robert Lemos, "China-Linked Group Attacked Taiwanese Financial Firms for 18 Months," *Dark Reading*, February 4, 2022; Anomali, "Anomali Suspects that China-Backed APT Pirate Panda May Be Seeking Access to Vietnam Government Data Center," April 30, 2020.
581. Anomali, "Anomali Suspects that China-Backed APT Pirate Panda May Be Seeking Access to Vietnam Government Data Center," April 30, 2020.
582. Mandiant, "Advanced Persistent Threats (APTs)."
583. Mandiant, "Advanced Persistent Threats (APTs)."
584. Secureworks "BRONZE OLIVE."
585. Mandiant, "Advanced Persistent Threats (APTs)."
586. Secureworks "BRONZE OLIVE."
587. Mandiant, "Advanced Persistent Threats (APTs)."
588. Mandiant, "Advanced Persistent Threats (APTs)"; Secureworks "BRONZE OLIVE."
589. Mandiant, "Advanced Persistent Threats (APTs)"; CyberMasterV, "Dissecting APT21 Samples Using a Step-By-Step Approach," *Cyber Geeks*, November 27, 2020.
590. Mandiant, "Advanced Persistent Threats (APTs)."
591. Mandiant, "Advanced Persistent Threats (APTs)."
592. CrowdStrike, "Hammer Panda"; CrowdStrike (@CrowdStrike), "HAMMER PANDA: Chinese threat actor last seen in 12/2017 using ZeroT malware. Targets: finance, telecom. May soon reappear under China's Strategic Support force. Visit the Adversary Universe website to learn more about this adversary: *https://bit.ly/2ZjwgTQ* #CSAdversaryUniverse," Twitter, May 14, 2021, 12:44p.m.
593. Mandiant, "Advanced Persistent Threats (APTs)."
594. Mandiant, "Advanced Persistent Threats (APTs)."
595. Mandiant, "Advanced Persistent Threats (APTs)."
596. Mandiant, "Advanced Persistent Threats (APTs)."
597. Mandiant, "Advanced Persistent Threats (APTs)."
598. Akshaya Asokan, "Researchers: Chinese APT Espionage Campaign Bypasses 2FA," *Bank Info Security*, December 26, 2019.
599. Mandiant, "Advanced Persistent Threats (APTs)."
600. Mandiant, "Advanced Persistent Threats (APTs)."
601. Secureworks, "BRONZE FIRESTONE."
602. Mandiant, "Advanced Persistent Threats (APTs)"; MITRE ATT&CK, "APT19," May 26, 2021.
603. Ian Ahl, "Privileges and Credentials: Phished at the Request of Counsel," *Mandiant*, June 6, 2017.
604. MITRE ATT&CK, "APT19," May 26, 2021; Council on Foreign Relations, "Deep Panda"; Secureworks, "BRONZE FIRESTONE."
605. Mandiant, "Advanced Persistent Threats (APTs)."
606. Mandiant, "Advanced Persistent Threats (APTs)."
607. MITRE ATT&CK, "APT18," March 30, 2020; Eduard Kovacs, "Chinese APT Group Uses Hacking Team's Flash Player Exploit," *SecurityWeek*, July 10, 2015; Aaron Shelmire, "Evasive Maneuvers by the Wekby Group with Custom ROP-Packing and DNS Covert Channels," *Anomali*, July 6, 2015.
608. Mandiant, "Advanced Persistent Threats (APTs)"; MITRE ATT&CK, "APT18," March 30, 2020.
609. Malpedia, "APT 18"; Bran Defense, "Dynamite Panda APT Group," August 8, 2022.
610. Mandiant, "Advanced Persistent Threats (APTs)"; Eduard Kovacs, "Chinese APT Group Uses Hacking Team's Flash Player Exploit," *SecurityWeek*, July 10, 2015.
611. Mandiant, "Advanced Persistent Threats (APTs)"; Bran Defense, "Dynamite Panda APT Group," August 8, 2022.
612. Mandiant, "Advanced Persistent Threats (APTs)."
613. Mandiant, "Advanced Persistent Threats (APTs)"; MITRE ATT&CK, "APT17," October 13, 2020; Intrusion Truth, "APT17 Is Run by the Jinan Bureau of the Chinese Ministry of State Security," July 24, 2019; FireEye, "Hiding in Plain Sight: FireEye and Microsoft Expose Obfuscation Tactic," May 14, 2015.
614. Darien Huss and Matthew Mesa, "Operation RAT Cook: Chinese APT Actors Use Fake Game of Thrones Leaks as Lures," *Proofpoint*, August 25, 2017.
615. Mandiant, "Advanced Persistent Threats (APTs)"; Darien Huss and Matthew Mesa, "Operation RAT Cook: Chinese APT Actors Use Fake Game of Thrones Leaks as Lures," *Proofpoint*, August 25, 2017.
616. Mandiant, "Advanced Persistent Threats (APTs)."
617. Mandiant, "Advanced Persistent Threats (APTs)."

618. SecureList by Kaspersky, "CVE-2015-2545: Overview of Current Threats," May 25, 2016; Ryann Winters, "The EPS Awakens—Part 2," *FireEye*, December 20, 2015.
619. SecureList by Kaspersky, "CVE-2015-2545: Overview of Current Threats," May 25, 2016; Ryann Winters, "The EPS Awakens—Part 2," *FireEye*, December 20, 2015.
620. Mandiant, "Advanced Persistent Threats (APTs)"; Florian Roth, "APT Groups and Operations."
621. Mandiant, "Advanced Persistent Threats (APTs)."
622. Mandiant, "Advanced Persistent Threats (APTs)"; Proficio, "Actor—APT 15 / Vixen Panda"; Microsoft, "Microsoft Digital Defense Report," October 2021, 60; Jurgita Lapienyte, "Microsoft Disrupts Activities of a China-Based Hacking Group in 29 Countries," *Cyber News*, December 8, 2021.
623. Mandiant, "Advanced Persistent Threats (APTs)"; Catalin Cimpanu, "Connection Discovered between Chinese Hacker Group APT15 and Defense Contractor," *ZDNet*, July 1, 2020.
624. Lookout, "Mobile APT Surveillance Campaigns Targeting Uyghurs: A Collection of Long-Running Android Tooling Connected to a Chinese mAPT Actor," June 2020.
625. Sergiu Gatlan, "Microsoft Seizes Sites Used by APT15 Chinese State Hackers," *Bleeping Computer*, December 6, 2021.
626. Catalin Cimpanu, "Connection Discovered between Chinese Hacker Group APT15 and Defense Contractor," *ZDNet*, July 1, 2020.
627. Mandiant, "Advanced Persistent Threats (APTs)."
628. Mandiant, "Advanced Persistent Threats (APTs)"; General Services Administration, "Advanced Persistent Threat (APT) Buyer's Guide," January 2021, 4.
629. Mandiant, "Advanced Persistent Threats (APTs)"; General Services Administration, *Advanced Persistent Threat (APT) Buyer's Guide*, January 2021, 4.
630. Adam Meyers, "Who Is Anchor Panda?" *CrowdStrike*, March 22, 2013.
631. Mandiant, "Advanced Persistent Threats (APTs)."
632. Mandiant, "Advanced Persistent Threats (APTs)"; General Services Administration, *Advanced Persistent Threat (APT) Buyer's Guide*, January 2021, 4.
633. Mandiant, "Advanced Persistent Threats (APTs)."
634. Mandiant, "Advanced Persistent Threats (APTs)"; Secureworks, "BRONZE GLOBE"; MITRE ATT&CK, "APT12c," March 30, 2020; Adam Meyers, "Who Is Numbered Panda?" *CrowdStrike*, March 29, 2013.
635. Mandiant, "Advanced Persistent Threats (APTs)."
636. Lucian Constantin, "The Chinese Hacker Group That Hit the N.Y. Times Is Back with Updated Tools," *Computer World*, August 12, 2013.
637. Ned Moran and Mike Oppenheim, "Darwin's Favorite APT Group," September 3, 2014.
638. Mandiant, "Advanced Persistent Threats (APTs)."
639. Mandiant, "Advanced Persistent Threats (APTs)."
640. Trend Micro, "Operation Cloud Hopper: What You Need to Know," April 10, 2017; Adrian Nish and Tom Rowles, "APT10 - OPERATION CLOUD HOPPER," *BAE Systems*, April 3, 2017.
641. Mandiant, "Advanced Persistent Threats (APTs)"; U.S. Department of Justice, *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, December 20, 2018.
642. Mandiant, "Advanced Persistent Threats (APTs)."
643. Trend Micro, "Operation Cloud Hopper: What You Need to Know," April 10, 2017.
644. Symantec, "Cicada: Chinese APT Group Widens Targeting in Recent Espionage Activity," April 5, 2022; Symantec, "Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign," November 17, 2020; Ayako Matsuda and Irshad Muhammad, "APT10 Targeting Japanese Corporations Using Updated TTPs," *Mandiant*, September 13, 2018.
645. Mandiant, "Advanced Persistent Threats (APTs)."
646. Mandiant, "Advanced Persistent Threats (APTs)."
647. U.S. Department of Justice, *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, December 20, 2018.
648. U.S. Department of Justice, *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, December 20, 2018.
649. Florian Roth, "APT Groups and Operations."
650. Mandiant, "Advanced Persistent Threats (APTs)."

651. James Scott and Drew Spaniel, "China's Espionage Dynasty: Economic Death by a Thousand Cuts," *Institute for Critical Infrastructure Technology*, 2016, 18.
652. Mandiant, "Advanced Persistent Threats (APTs)."
653. Mandiant, "Advanced Persistent Threats (APTs)"; James Scott and Drew Spaniel, "China's Espionage Dynasty: Economic Death by a Thousand Cuts," *Institute for Critical Infrastructure Technology*, 2016, 18.
654. Mandiant, "Advanced Persistent Threats (APTs)."
655. Mandiant, "Advanced Persistent Threats (APTs)."
656. Mandiant, "Advanced Persistent Threats (APTs)."
657. Mandiant, "Advanced Persistent Threats (APTs)."
658. Mandiant, "Advanced Persistent Threats (APTs)."
659. Mandiant, "Advanced Persistent Threats (APTs)."
660. Mandiant, "Advanced Persistent Threats (APTs)."
661. Mandiant, "Advanced Persistent Threats (APTs)."
662. Mandiant, "Advanced Persistent Threats (APTs)."
663. Aaron Boyd, "FBI Issues Alert on Hacking Campaign Targeting Federal Networks," *Federal Times*, April 5, 2016; Lorenzo Franceschi-Bicchierai, "FBI Says a Mysterious Hacking Group Has Had Access to US Govt Files for Years," *Motherboard by Vice*, April 4, 2016.
664. Mandiant, "Advanced Persistent Threats (APTs)."
665. Mandiant, "Advanced Persistent Threats (APTs)."
666. Secureworks, "BRONZE FLEETWOOD"; Microsoft, "Microsoft Digital Defense Report," October 2021, 60.
667. Microsoft, "Microsoft Digital Defense Report," October 2021, 60–62; Dan Perez et al., "Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day," *Mandiant*, April 20, 2021; Mandiant, "Advanced Persistent Threats (APTs)"; Council on Foreign Relations, "APT5"; FireEye, "Southeast Asia: An Evolving Cyber Threat Landscape," March 2015, 9.
668. Mandiant, "Advanced Persistent Threats (APTs)."
669. *Cyware Hacker News*, "Chinese Hacker Group APT5 Targets Fortinet and Pulse Secure VPN Servers," September 6, 2019.
670. Mandiant, "Advanced Persistent Threats (APTs)."
671. Mandiant, "Advanced Persistent Threats (APTs)."
672. Mandiant, "Advanced Persistent Threats (APTs)"; Secureworks, "BRONZE EDISON."
673. Mandiant, "Advanced Persistent Threats (APTs)."
674. Mandiant, "Advanced Persistent Threats (APTs)."
675. Secureworks, "BRONZE EDISON."
676. Secureworks, "BRONZE EDISON."
677. Mandiant, "Advanced Persistent Threats (APTs)."
678. Mandiant, "Advanced Persistent Threats (APTs)."
679. Mitre ATT&CK, "APT3," October 1, 2021; Intrusion Truth, "APT3 Is Boyusec, a Chinese Intelligence Contractor," May 9, 2017.
680. Intrusion Truth, "APT3 Is Boyusec, a Chinese Intelligence Contractor," May 9, 2017.
681. Mandiant, "Advanced Persistent Threats (APTs)."
682. Mitre ATT&CK, "APT3," October 1, 2021; Erica Eng and Dan Caselden, "Operation Clandestine Wolf—Adobe Flash Zero-Day in APT3 Phishing Campaign," *Mandiant*, June 23, 2015; Ned Moran et al., "Operation Double Tap," *Mandiant*, November 21, 2014.
683. A. L. Johnson, "Buckeye Cyberespionage Group Shifts Gaze from US to Hong Kong," *Symantec*, September 6, 2016.
684. Mandiant, "Advanced Persistent Threats (APTs)."
685. Mandiant, "Advanced Persistent Threats (APTs)."
686. U.S. Department of Justice, *U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage*, November 27, 2017.
687. Mitre ATT&CK, "Putter Panda," March 30, 2020.
688. Mandiant, "Advanced Persistent Threats (APTs)"; Mitre ATT&CK, "Putter Panda," March 30, 2020; CrowdStrike, "CrowdStrike Intelligence Report: Putter Panda," June 9, 2014, 5.
689. Mandiant, "Advanced Persistent Threats (APTs)."
690. Mandiant, "Advanced Persistent Threats (APTs)."
691. Mitre ATT&CK, "APT1," May 26, 2021.
692. Mandiant, "APT 1: Exposing One of China's Cyber Espionage Units," 2013.
693. Mandiant, "APT 1: Exposing One of China's Cyber Espionage Units," 2013.

694. 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; Kevin Johnson and Donna Leinwand Leger, "U.S. Accuses China of Hacking Westinghouse, U.S. Steel," *USA Today*, May 19, 2014; Council on Foreign Relations, "Indictment of PLA Officers," May 2014.

695. Ellen Nakashima and William Wan, "U.S. Announces First Charges against Foreign Country in Connection with Cyberspying," *Washington Post*, May 19, 2014.

696. Mandiant, "Advanced Persistent Threats (APTs)."

697. Mandiant, "Advanced Persistent Threats (APTs)."

698. 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.