SEPTEMBER 2025

A Playbook for Winning the Cyber War

Part 3: Evaluating China's Cyber Strategy

Aosheng Pusztaszeri Emily Harding Julia Dickson

A Report of the CSIS Intelligence, National Security, and Technology Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

SEPTEMBER 2025

A Playbook for Winning the Cyber War

Part 3: Evaluating China's Cyber Strategy

AUTHORS
Aosheng Pusztaszeri
Emily Harding
Julia Dickson

A Report of the CSIS Intelligence, National Security, and Technology Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2025 by the Center for Strategic and International Studies. All rights reserved.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

The authors would like to extend their gratitude to those who graciously agreed to be interviewed. They would also like to thank Krista Auchenbach and James Andrew Lewis for providing valuable feedback, Susan Hines for helping with the project contract, and the CSIS iDeas Lab for offering their design expertise.

This report is made possible by project support from the Smith Richardson Foundation.

Contents

Authors' Note About the Series

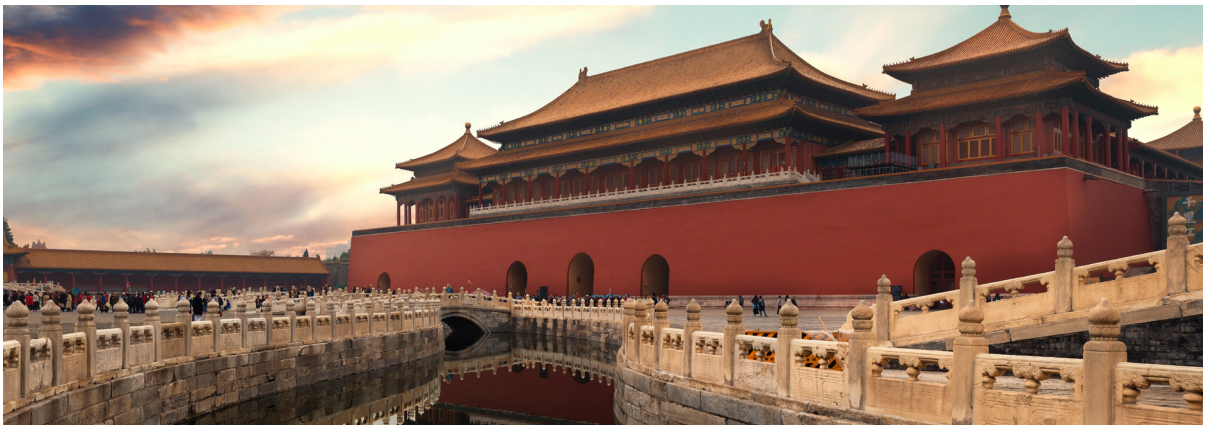


Photo Source: ake1150/Adobe Stock

This report is part of a series on the future of cyber warfare. This part of the series examines how China fights in the cyber domain, including the core elements of Beijing's strategy for conducting cyber operations, how that strategy fits in a larger foreign policy context, and who the frontline fighters are in this new mode of conflict.

Part 1 of this series offers a broad introduction to the report, covers key takeaways from the comparative studies and wargames, and summarizes the authors' recommendations. Parts 2, 3, and 4 examine how Russia, China, and Iran, respectively, fight in the cyber domain, and Part 5 examines U.S. cyber practices. Part 6 tests how U.S. policymakers view cyber operations as part of the spectrum of war, peace, and irregular warfare, illuminated by a set of wargames. Finally, Part 7 fully explains the new playbook that will close the gap between how the United States and its adversaries fight and succeed in the cyber domain.

Overview of China's Cyber Playbook

"Efforts should be made to build our country into a network powerhouse."

– Chinese President Xi Jinping, 2014 Central Network Security and Informatization Leading Small Group meeting[1]

Chinese President Xi Jinping's remarks at the 2014 Central Network Security and Informatization Leading Small Group meeting marked a new phase in the Chinese government's approach to cyberspace.[2] Beijing is making a determined effort to fully integrate cyber operations with its other military capabilities, with an end goal of excelling at a comprehensive, agile form of modern conflict. China views conditions of peace and war not as a dichotomy, with different rules governing each, but as a spectrum. What the United States and its allies refer to as strategic competition, China sees as akin to low-level warfare. That low-level war explicitly includes information operations, including computer network operations. China's cyber tool kit is an extensive part of the arsenal, providing opportunities for a range of actions. Further, China's view of what qualifies as appropriate targets means it is willing to use cyber tools against a variety of targets, including some which Western countries would see as out-of-bounds.

China's offensive cyber operations are part of a larger, integrated concept of information warfare. That concept is embedded in its military, diplomatic, and economic strategy. In 1995, Major General Wang Pufeng, who is considered to be the father of Chinese information warfare, wrote, "Information war is a crucial stage of high-tech war. . . . At its heart are information technologies, fusing intelligence war, strategic war, electronic war, guided missile war, a war of 'motorization' (*jidong zhan*), a war of firepower (*huoli*)—a total war. It is a new type of warfare."[3] Chinese military

scholars wrote in the 2017 *Guofang Keji*, a Chinese defense journal, about the integration of these efforts:

> The physical level requires the realization of the vertical and horizontal connection and integration of various combat units and combat elements, unified command, unified control and unified coordination. The information level requires the controllability, sharing, and robustness of command information. The above-mentioned command and control capabilities play a decisive role in the control of cyberspace and the success or failure of operations, so they have become one of the core capabilities of cyberspace combat power construction.[4]

People's Liberation Army (PLA) planners envision cyber as a key part of a comprehensive, integrated strategy for the entire spectrum of modern warfare, from espionage to competition to conflict.[5] Beijing seeks to collect intelligence; prepare the environment for cyberattacks; imperil a potential adversary's command, control, and communications systems; disrupt commerce and critical infrastructure; and influence populations.[6]

Like Moscow, Beijing views offensive cyber capability and information warfare as inextricably linked. Beijing's 2015 Military Strategy extensively discusses the "informatisation of warfare" and says China will build an "informationised military" to win "future informationised wars."[7] China's understanding of information operations combines military capabilities with cyber warfare, electromagnetic warfare, counterspace, propaganda, and denial and deception, which reflects a bent toward gaining an "information advantage" over its adversaries.[8] Beijing views achieving this "information superiority" as an essential prerequisite for kinetic warfare, which is rooted in the belief of the Chinese Communist Party (CCP) that losing a major military operation could jeopardize the regime's domestic legitimacy. Consequently, the CCP prioritizes securing "information superiority" before deploying military force to ensure conditions are fully prepared and success is "virtually guaranteed."[9] Beijing also sees data as a strategic asset and sees no boundary between industry intellectual property (IP) and state secrets: Both are fair game for espionage. Using tactics honed for internal surveillance, it has mined the rest of the world for useful data.[10]

Beijing notably does not employ the term "cybersecurity" but rather uses "network security" (*wangluo anquan*), which includes the "use of information . . . to influence or control . . . an opponent's decision-making activities" and can serve both "offensive and defensive" purposes.[11] As a result, China's concept of network security extends beyond the West's narrower focus on protecting cyberspace from cyberattacks and encompasses broader national security concerns across economic, political, and social dimensions.[12] This perspective continues to shape and inform much of China's cyber strategy and playbook.

Chinese activity in the cyber domain is also characterized by exceedingly broad collection, typically for espionage and information gathering.[13] According to CrowdStrike Intelligence, China-affiliated actors were the most active intrusion groups in 2022, targeting "nearly all 39 global industry sectors and 20 geographic regions."[14] While the primary focus was on organizations in the government and technology sectors across Asia (66 percent), organizations in Europe and North America were

also heavily targeted, accounting for approximately 25 percent of Chinese intrusion activity. Africa, South America, and Oceania made up the remaining 9 percent.[15] China-affiliated intrusion groups also rank among the most capable in exfiltrating massive amounts of personal data. According to an August 2021 U.S. Senate Select Committee on Intelligence hearing, China has hacked and stolen the personal data of about 80 percent of Americans since 2014.[16] Further, over the past five years, U.S. government officials have identified Chinese hacking groups covertly embedding themselves into U.S. critical infrastructure. These actions, which "have no legitimate espionage value," according to the Cybersecurity and Infrastructure Security Agency (CISA), strongly indicate that the groups' ultimate objective is sabotage (see Volt Typhoon, also known as Vanguard Panda, on page 25).[17]

Beijing has used information warfare to deter what it views as the United States and its allies' interference in its affairs. This approach manifests itself as both denial and compellence. To deny, Beijing enacts policies like the Great Firewall, locking down incoming information, by way to prevent the United States from gaining a foothold. Meanwhile, it has sought to compel actors to align with China's view or remain on the sidelines, largely through a combination of economic power and its vast army of cyber "trolls."[18] For instance, in October 2019, after Houston Rockets Manager Daryl Morey tweeted in support of the Hong Kong protests, China's "troll mob" retaliated by posting 170,000 tweets criticizing Morey, while China's state media temporarily suspended all National Basketball Association (NBA) broadcasts in the country. This resulted in hundreds of millions of dollars in lost NBA revenue and a rapid apology from Morey.[19] Similarly, in 2021, Lithuania experienced a 91 percent drop in its exports to China after allowing Taiwan to open a representative office in Vilnius.[20]

Despite rapidly developing its cyber capabilities over the past decade, China's cyber ecosystem may still have underlying flaws. According to the International Institute for Strategic Studies (IISS), China's intelligence analysis and dissemination capabilities remain "less mature" than those of the West.[21] Furthermore, China's intelligence analysis tends to be driven by ideology, often "enmeshed with questions of prestige around the political goals of the CCP leaders," making it more vulnerable to political influence, intrigue, scandals, and corruption purges.[22] For instance, the PLA's Strategic Support Force (SSF), which housed China's Cyber Department, was completely restructured after eight short years, likely due to corruption concerns among SSF leadership.[23] Certain secretive PLA cyber groups have been detected—and exposed—by private U.S. companies, leading to fierce denials from Beijing.[24] For instance, on February 19, 2013, cybersecurity firm Mandiant uncovered and exposed the highly secretive PLA cyber espionage group Comment Panda (also known as PLA Unit 61398) by reportedly exploiting significant vulnerabilities in the group's network.[25]

Core Elements of China's Strategy

"Without cybersecurity, there is no national security; without informatization, there is no modernization. Cybersecurity and informatization are two wings of one body and two wheels of one drive."

– China's 2016 National Cyber Strategy[26]

While Beijing has released little in the way of an official explanation of its cyber playbook, a combination of scholarly writings by individuals associated with the military and a careful analysis of China's uncovered cyber operations provide a rough map of Chinese theory and practice in this domain. Still, any observer of Chinese activity must keep in mind that theory can look good on paper while implementation falls short. Although this is true everywhere, it is particularly pronounced in authoritarian societies, where good news is reported and bad news is silenced. This section of the report describes what China has officially said about its approach to cyber, and the next section examines how China applies these concepts in practice.

"World-Class" Cyber as a Core Mission

Beijing first acknowledged the critical role of the cyber domain in conflict in a 2013 Academy of Military Science's publication, *The Science of Military Strategy*.[27] In the ensuing 12 years, the PLA has built out its offensive and defensive cyber capabilities, including as part of a massive reorganization of its military forces. Its original goal was to create a strategically valuable cyber capability by 2020, but as of 2019, China described its cyber capabilities as "commensurate with its status as a major cyber country developing into a cyber power."[28]

Similarly, China's 2015 Military Strategy called computer network operations a "new pillar of economic and social development" and a "new domain of national security."[29] It further laid out a clear goal to "expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, [and] support for the country's endeavors in cyberspace."[30] China also aims to become a world-leading cyber power by 2035.[31] To achieve this goal, it intends to heavily focus on the "informatization" of warfare, and strengthen its cyber situational awareness and defense capabilities in order to "stem major cyber crises, ensure national network and information security, and maintain national security and social stability," according to its 2015 Military Strategy.[32]

Further, according to a 2020 U.S. Department of Defense (DOD) report, China is also increasingly prioritizing an "intelligentized" approach to warfare, which focuses on developing emerging technologies such as artificial intelligence (AI), cloud and quantum computing, and unmanned systems to target and degrade adversaries' systems.[33] In short, China believes its cyber goals are intertwined with "social stability" and that only by building an "informatized" and "intelligentized" military will it be able to meet its cyber objectives and "win future 'informatized' wars."[34]

Highly Motivated for Success

Part of the motivation for China's efforts in the cyber domain is a desire to maintain stability and control over its domestic population. The 2017 National Cyber Strategy says that:

> Political stability is the basic prerequisite for national development and people's happiness. The use of the network to interfere in [China's] internal affairs, attack [its] political system, incite social unrest, and [conduct] large-scale network monitoring, network theft and other activities seriously endanger the national political security and user information security.[35]

According to the IISS, China's primary strategic objective in cyberspace has been to control domestic thought, specifically by preventing the online spread of Western ideas.[36] Drawing from the 2003 UN concept of "cyber sovereignty," which calls on states to exert control over their own portion of the internet, China developed its "Golden Shield Project"—an internal surveillance and censorship system that evolved into what is now known as the "Great Firewall of China."[37] Further, witnessing the growing role of social media in sparking social unrest—notably the 2009 Iran protests, 2010 Arab Spring, and 2011 England riots—caused the CCP to intensify its monitoring of domestic internet activity.[38] Today, Chinese surveillance efforts remain focused on domestic control, with its Ministry of Public Security (MPS) operating what is considered to be the largest surveillance system in the world.[39]

This view of domestic technological innovation as a national security priority may help explain certain state-sponsored cyberattacks on foreign technology companies aimed at stealing IP.[40] For example, in 2016, the China-affiliated threat group Stone Panda stole "hundreds of gigabytes" of sensitive data from companies in aviation, space, communications, advanced manufacturing, maritime technology, and oil and gas—all core sectors outlined in the CCP's Made in China 2025 plan to boost the country's technology industry and reduce its reliance on U.S. companies.[41] On

paper, China has set the ambitious goal of ensuring that 70 percent of its core internet technology is domestically produced by 2025.[42]

Further, China's cyber legislation and regulations are intentionally designed to enhance and refine the country's cyber capabilities. For example, the 2021 Regulations on the Management of Network Product Security Vulnerabilities, drafted by the Cyberspace Administration of China (CAC), the MPS, and the Ministry of Industry and Information Technology (MIIT), "require companies doing business in China to report software vulnerabilities in their products or products they use to the MIIT within forty-eight hours of discovery," according to an Atlantic Council report.[43] This regulation, coupled with state-sponsored student hacking competitions (such as the TOPSEC Cup), provides China's security services with a "steady stream of vulnerabilities to exploit for state-sponsored operations," according to a 2022 report by the U.S.-China Economic and Security Review Commission (USCC).[44]

China's concept of network security encompasses political dimensions, which may explain why the CCP views commercial communication networks and information technology (IT) standards as tools to strengthen its influence and project power abroad.[45] Consequently, China sees competition with the West over IT architectures as a zero-sum game.[46]

How Cyber Strategy Fits into Foreign Policy

China, like Russia and the United States, portrays its efforts as entirely defensive. The 2013 Defense White Paper and 2015 Military Strategy note that China would not attack unless attacked first, but "we will surely counterattack if attacked."[47] This strategy, known as "Active Defense," aims "to enhance defense capabilities in order to survive and counter after suffering an offensive cyber strike."[48] As a retired PLA colonel, citing an active-duty PLA colonel, put it in 2019: "After the first round of a cyberattack, the targeted side can respond with a precise counterattack as long as it has a strong defense. The attacker will then suffer unfavorable outcomes if its defense is not good enough. From this perspective, it is wiser to make efforts in building up a strong defense."[49] Furthermore, China's National Cyber Strategy asserts that China is prepared to "take all measures, including economic, administrative, scientific and technological, legal, diplomatic, [and] military" to "protect . . . [its] information facilities" and "safeguard [its] cyberspace sovereignty."[50]

China sees cyber as a lawless space with weak international norms.[51] Sovereignty is a particularly fluid concept: While Beijing insists on absolute authority within its own borders, it also aggressively operates within the physical and cyber borders of other nations. A government official from a U.S. ally summed up this approach as "there is an area of me you can't attack and areas of you that I can."[52] Put differently, Beijing views China's internal internet as its own sovereign territory and other countries' internet as its hunting grounds. Just as China sees heavy censorship as completely acceptable, it also sees civilian suffering at a low level as justified to accomplish larger goals.[53] Media manipulation, power disruption, point-of-sale manipulation, and disruption of communications are all legitimate actions to accomplish the state's goal.[54] Further, attacks on civilian infrastructure, like power grids, are also a part of the plan to deter or coerce the United States and its allies.

Ke Hongfa, Zhu Jilu, and Zhao Rong in *Guofang Keji* describe two types of attacks: "information utilization" also known as "soft kill" attacks like influence campaigns; and "high-precision physical destruction of hardware," such as IT infrastructure. These two forms of attack have the benefit of "remote control, flexible maneuverability, strong destructive power, and small collateral damage."[55] This simple taxonomy of attacks sheds light on what China values in cyber warfare—the ability to destroy hardware or manipulate information from afar, with little risk.

At the time of writing, Beijing has largely focused its cyber efforts on the first type of attack: espionage and information utilization. These efforts can also be split into two main lines: (1) theft of data, and (2) research on the setup of a network for potential exploitation later. In the first instance, stealing research and development (R&D), state secrets, or personal data can advance Chinese political or economic interests. In the second, operational preparation of the environment (OPE), or establishing the knowledge of networks and footholds, is necessary to execute later operations, including destructive ones. Writing in *Guofang Keji*, Ke, Zhu, and Zhao describe these reconnaissance operations:

> Cyberspace reconnaissance operations are mission behaviors to obtain information about opponents or potential opponents' cyberspace operations and network resources. The network information of reconnaissance is the prerequisite basis for all cyber combat operations and can also be used to verify current intelligence or predictions.[56]

"Information Utilization" or "Soft Kill" Attacks

While China views information operations—such as propaganda and cyber operations—as existing along a spectrum of information warfare, this project draws a clear, bright line between the two and focuses nearly exclusively on the latter: computer network operations designed to move or change data, not minds. While modern information operations use computers as a delivery mechanism for their substantive payload, the 1s and 0s are incidental to the operation; in contrast, in cyber operations the 1s and 0s themselves are the payload. Changing minds can be among the most powerful of weapons, but the methods and future in that space are different from those of cyber warfare. This report is scoped solely to examine operations intended to produce an outcome in the physical world.

Still, these arenas occasionally overlap. Australian officials have highlighted Chinese efforts to undermine computer security training with Pacific Island nations by engaging in a smear campaign against U.S. and Australian capabilities. For example, Beijing's diplomats will say that the United States has no proof that China engages in offensive cyber activity, then make the counteraccusation that Google, Microsoft, and others are really tools of the U.S. government and that those companies are the ones planting dangerous back doors. Hacks and leaks can also be a combination of the two tool sets—computer network operations to obtain the data, then a leak strategy designed to maximize the effect on minds.

According to the Office of the Director of National Intelligence (ODNI), China is also increasingly using information operations to undermine U.S. global leadership and democracy and expand Beijing's influence.[57] These efforts primarily focus on promoting pro-China narratives and countering foreign policies that threaten "China's international image, access to markets, and technological expertise." This is especially evident when China views the issues as matters of internal sovereignty, such as those involving Hong Kong, Taiwan, Tibet, and Xinjiang.[58] China is continually refining its influence operations, even experimenting with generative AI to run fake TikTok accounts.[59] These accounts, made by the CCP-affiliated threat actor "Spamouflage," spread divisive content on social media to sow division among U.S. voters.[60] According to ODNI, China's recent efforts to exploit perceived societal divisions in the United States increasingly resemble Moscow's approach to influence operations.[61]

SOFT KILL: DATA THEFT

Unlike Moscow, China stands out in its approach to collecting vast quantities of data. One reason for Beijing's focus on data theft is almost certainly in part to train its artificial intelligence/machine learning (AI/ML) systems. A 2021 DOD report highlighted this approach, stating that the PLA explicitly called out big data as "useful for monitoring and early warning." Further, AI is "a tool for more realistic exercises and the ability to respond quickly in the case of a conflict in cyberspace."[62]

China also engages in extensive industrial cyber espionage, exfiltrating vast amounts of private sector information, trade secrets, R&D data, and products. According to the U.S. Department of Justice (DOJ), "more than 90 percent of [its] cases alleging economic espionage . . . involv[ed] China."[63] In an October 2014 interview, then-Federal Bureau of Investigation (FBI) Director James Comey estimated that Chinese cybercrime costs the U.S. economy "billions" of dollars every year.[64] The USCC estimates the figure to be closer to "tens of billions of dollars" every year.[65]

China's intelligence collection against the United States has been comprehensive:[66]

- In early 2014, Chinese actors hacked the health insurance company Anthem, exfiltrating an estimated 78 million member names, birth dates, and phone and Social Security numbers.[67]
- Beijing hacked the Office of Personnel Management (OPM) in 2014 and stole 21.5 million records, including background check data and employee fingerprints.
- In 2017, Beijing hacked credit reporting agency Equifax and stole the credit data of 147.9 million Americans.
- Between 2014 and 2018, Beijing hacked Starwood Hotels' reservation system and stole credit card and passport information from approximately 500 million people.[68]

With this combination of data, China could identify U.S. government employees with security clearances who had financial or health problems, trace where they are about to travel, and create opportunities for Chinese intelligence agents to make an approach (a "bump"). In addition to this

kind of tactical use, data at scale is a strategic asset—whether to train AI/ML models or to develop knowledge that could inform an influence campaign.

HARD KILL: "HIGH-PRECISION PHYSICAL DESTRUCTION OF HARDWARE"

The second type of attack Ke, Zhu, and Zhao describe in *Guofang Keji* is "hard kill," or high-precision destruction. Russia and Iran have both executed this type of cyberattack in recent years—for example, Russia took Ukraine's power grid offline in 2015 and again in 2022, while Iran destroyed thousands of computers belonging to Aramco, the Saudi state-owned oil company, in 2012.[69] China has not yet executed such an attack, but it has pre-positioned assets to do so when deemed necessary.[70]

The theory behind this kind of attack is to create disruption, confusion, and disarray during a crisis. The aggressor simply needs to identify pain points in the target's logistical operations and make everything just a little bit harder, slowing or temporarily halting effective functioning. If the target country cannot move people, fuel, and materiel, it cannot effectively fight. For example, if China were able to disrupt transport around military bases—such as train signals, port equipment, or electricity—it could likely slow deployment of U.S. forces for hours, if not days. In the case of a Taiwan contingency, a 24-hour deployment delay might be enough to allow the PLA to gain a foothold on the island before the United States could effectively assist. One member of an allied military noted that it might be as simple as changing the barcodes on shipping containers in a military warehouse or shuffling the data in an Excel spreadsheet managing deployments.[71] If mufflers, rather than munitions, are loaded onto the ship, that vessel's effectiveness is greatly diminished. Another allied official said a military must be able to "move, feed, and power" soldiers—illustrating the targets of Chinese operations.[72]

Beijing could also cause disruption by targeting critical infrastructure, which governments define as items necessary for the functioning of daily life. Critical infrastructure, however, is generally considered off-limits to military activity. Targeting civilian critical infrastructure is illegal under the Law of Armed Conflict because of the potential for mass casualties and the high likelihood of civilian suffering if, for example, a water treatment plant were taken offline for days.[73] However, what constitutes critical infrastructure is often in the eye of the victim, and China has demonstrated a willingness to penetrate water, power, and fuel systems within the United States.[74] Australia, too, saw an uptick in attacks on critical infrastructure systems from 2022 to 2023.[75] New requirements in Australia make reporting breaches of critical infrastructure systems mandatory, which will lead to better data on the trend lines of the problem and more comprehensive awareness of the problem's scope.

Beijing's efforts against critical infrastructure are not new. In July 2021, the U.S. Department of Homeland Security issued a threat alert on Chinese penetrations of natural gas pipelines, citing efforts dating back to 2011.[76] The alert disclosed that suspected Chinese hackers had gained access to the controls of several U.S. natural gas pipeline companies.[77] Ominously, it also stated that these penetration strategies "remain relevant" today.[78] At the time, a Mandiant researcher asserted that the goal of the attack was likely economic espionage: "We have seen little evidence over the past 10 years of [Chinese] cyber operations targeting critical infrastructure with the end goal of disruption

or destruction, but we do not discount the possibility that they may do so in future conflict scenarios, such as in the event of war."[79]

The Mandiant researcher was wrong, but the latter half of the comment was prescient: Since 2011, China-affiliated actors—most notably Volt Typhoon—have embedded themselves in the networks of "aviation, rail, mass transit, highway, maritime, pipeline, water, and sewage organizations" in the mainland United States.[80] Indeed, the researcher went on to say that Mandiant had recorded "multiple threat actors linked to China" targeting industrial control system (ICS) operators and natural gas pipeline companies, an energy company, and an ICS equipment manufacturer and security firm.[81] While this activity may have yielded some economic benefit, it now appears far more likely that the Chinese attackers were conducting reconnaissance for future operations, such as OPE.

In Australia, cyberattacks may be redundant. Canberra has discovered that China may have established a more direct route: A large percentage of critical infrastructure is already Chinese-owned. For instance, Hong Kong-based CKI controls 51 percent of the South Australia Power Network and a majority share of gas transmission and distribution pipelines—68 percent in Victoria, 86 percent in South Australia, and 72 percent in Queensland.[82] A New South Wales group recently intervened to prevent a Chinese company from buying additional power generation and distribution capacity.[83] Australia is hardly alone; China has also sought contracts to build critical infrastructure—including power and transportation systems—around newly constructed national capitals in Egypt and Indonesia.[84]

The 2024 Annual Threat Assessment from the U.S. Intelligence Community (IC) and the Australian Signals Directorate (ASD) both note an increase in Chinese operations targeting critical infrastructure. The IC reports that U.S. private sector entities have found that Chinese cyber operations probably intend to "pre-position cyber attacks against infrastructure in Guam and to enable disrupting communications between the United States and Asia," as well as "deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces" in the event of a conflict.[85] Similarly, ASD reports that cyber incidents at the second-highest level (Category 2) "rose from 2 in Fiscal Year (FY) 2021–22 to 5 in FY 2022–23."[86] (Canberra's report does not name either the perpetrator or the target specifically, but government officials in interviews indicated China's responsibility for at least some attacks.)

How China Approaches Deniability

China's activities in cyberspace include opportunistic campaigns conducted by patriotic hackers and hacktivists, which create highly visible effects while offering Beijing plausible deniability, as well as operations affiliated with the PLA and Ministry of State Security (MSS), which are intended to remain clandestine while enabling long-dwell espionage or pre-positioning for future attacks. Some actors cross these categories, with certain proxies maintaining loose or close affiliations with the Chinese government.

The first category comprises high-profile hacktivist campaigns aimed primarily at responding to perceived slights against China. For example, in 1999, "patriotic hackers" defaced U.S. government

websites in retaliation for the accidental U.S. bombing of the Chinese embassy in Belgrade, Serbia.[87] This category also includes high-profile cyberattacks on Taiwan, often in response to a specific event. For instance, just before then-U.S. Speaker of the House Nancy Pelosi's visit to Taiwan in August 2022, Chinese hacktivists launched multiple distributed denial-of-service (DDoS) attacks against Taiwanese government websites.[88]

China also leverages its vast and opaque network of PLA- and MSS-affiliated threat groups to carry out more sophisticated cyberattacks while maintaining a level of plausible deniability. These operations are often carried out by "a collection of Chinese state-sponsored intelligence officers, contract hackers, and support staff" that operate out of PLA- or MSS-affiliated front companies and receive varying levels of government support.[89] Furthermore, the central MSS body in Beijing delegates considerable authority to its provincial branches and exercises varying degrees of control over these groups, making it difficult for policymakers to determine the central government's true degree of involvement and calculate an appropriate response.[90] According to Alex Joske, a consultant at McGrathNicol, this partially explains why "no cyber-attacks have been publicly attributed to the central MSS" in Beijing, whereas many have been linked to advanced persistent threats (APTs) affiliated with MSS regional bodies at the provincial or municipal level (see MSS on page 22).[91]

Beijing has also engaged in sophisticated, long-term clandestine campaigns. These operations typically focus on espionage—either establishing a sustained, covert presence to gather intelligence or creating an infiltration that could be weaponized later. For example, the threat actor Volt Typhoon operated undetected for at least five years within the systems of U.S. aviation, rail, and water organizations, according to the FBI, National Security Agency, and CISA.[92]

Implementation: Campaigns or Opportunism

China's path from opportunism to campaigns to thoroughly integrating cyber domain operations into its warfighting strategy has been reasonably linear. Its early cyber operations were attributed to a loose collection of private "patriotic hackers."[93] Over the next 15 years, the number of actors and the spread of activity expanded dramatically until the 2015 reorganization and consolidation of cyber operations, which coincided with the broader PLA restructuring. This unified approach has resulted in more targeted cyber activity, with campaign targets aligning largely with China's five-year plans.

Cyber campaigns are inherently challenging due to the difficulties of timing and coordination. As a result, cyberattack operations often combine deliberate targeting with opportunism (which involves identifying exploitable vulnerabilities). For example, the China-affiliated threat group Wicked Panda identified and quickly exploited zero-day vulnerabilities in the USAHerds application (CVE-2021-44207) and Log4j (CVE-2021-44228) framework. This quiet but effective operation ran from May 2021 to February 2022, successfully compromising at least six unidentified U.S. state government networks.[94]

China's Vulnerabilities

Creating pre-positioned tools to deploy at a moment's notice in case of a contingency looks good on paper, but translating a script into reality on the battlefield is far harder. As the adage goes, no battle plan survives first contact with the enemy. China has not fought a shooting war since 1979, and many of its cyber operations remain more theoretical than practical. While they can still be highly disruptive, orchestrating the right sequence of dominoes to fall at the precise moments to fit perfectly with a larger battle plan remains difficult. As an allied interviewee put it, "China thinks it can leverage a large number of effects simultaneously around the globe. They like to follow a script, and they don't think about the flexibility in planning that is so critical for cyberattacks."[95]

One way to manage a highly scripted operation is through extensive testing. A cyber range can be useful, but like any controlled environment, it is inherently artificial. Testing on a live target is the most effective way to gauge the impact of a cyberattack, but this approach is brazen and generally only used by Russia and North Korea. Moreover, it risks alerting the target, prompting patching and improved defenses that render the tool obsolete.[96] For example, Beijing might consider testing tools on the Philippines before deploying them against the United States, but Philippine systems are likely to be quite different, to the point of not being a useful comparison. On the other hand, testing tools in environments where detection is less likely could be advantageous.[97]

China heavily relies on foreign vendors for core network technologies, including essential U.S. software and hardware.[98] For instance, it often refers to the "eight King Kongs" *(bada jingang)* when discussing the largest internet companies in its domestic supply chain: Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle, and Qualcomm. China has long regarded its reliance on this small number of companies to be a national security risk.[99] This concern is amplified by China's state-run media, which often portrays these U.S. companies as proxies for the U.S. government. Many Chinese experts also hold the mistaken belief that, as in China, the U.S. government wields significant influence over U.S. companies, and that "the United States [government] can disrupt or corrupt the functioning of any device with U.S.-made software."[100]

Cyber War on Taiwan?

Pairing cyber operations with a potential amphibious assault on Taiwan would be extremely high risk but also high reward. According to the Australian Cyber Security Centre (ACSC), in a Taiwan contingency, China would need to cross Taiwanese airspace uncontested.[101] One way to achieve this would be to use cyber tools to disable operations at Taiwan's airfields and air defenses, allowing China to land on intact airfields. This could help China establish air superiority, funnel supplies, and deploy small contingents of ground troops in preparation for a larger amphibious assault. However, if these cyber operations fail to sufficiently degrade Taiwan's air defenses, China risks significant losses in aircraft, personnel, and equipment—along with a serious blow to morale and prestige.

In parallel, China could launch cyberattacks on U.S. systems as part of its invasion strategy. It is already embedding itself in U.S. critical infrastructure, and if Beijing manages to compromise and sabotage key systems supporting U.S. military bases—such as power grids or water treatment facilities in the Philippines, Guam, or Hawaii—it could time these disruptions with its blockade of Taiwan. Even a 24-hour delay in the U.S. response could tip the balance in China's favor and secure its control over the island. However, if these cyber operations fail or prove insufficient, and the United States is able to send enough aid to Taiwan in time, the situation could quickly escalate into a direct military conflict between the world's two most powerful countries.

Organizational Capabilities

Who Are the Fighters?

China's efforts in the cyber realm began much like those of other nations, with volunteer or patriotic hackers experimenting in a private capacity. As the Chinese government recognized the potential of this domain, it gradually developed an in-house cadre of hackers. In recent years, China has pursued a strategy of military-civil fusion, including in the cyber domain, which a 2021 DOD study found attempts to "increase the proportion of private companies that contribute to military projects and procurements." These enterprises include "technology companies that specialize in unmanned systems, robotics, artificial intelligence, cybersecurity, and big data."[102] The resulting Chinese ecosystem of cyber actors is diverse and capitalizes on the strengths of military, civilian, and ostensibly nongovernmental organizations.

Inside the government, Beijing has gone through multiple iterations of organizing itself for cyber activity, much like every other sophisticated actor. However, Beijing has made large, sweeping changes several times, likely with the aim of creating smoother integration between cyber activity and other military and intelligence operations. China completely revamped its cyber structure between 2015 and 2018. Prior to 2015, the PLA, Technical Reconnaissance Bureaus, and MSS all conducted cyber operations.[103] A military reorganization in 2015 was intended to bring peripheral activity under far tighter state control, while a 2018 civilian reorganization did the same. Another reorganization in 2024, meanwhile, was likely part of an anti-corruption push by President Xi. This section of the report reviews the current organization of China's cyber forces, including the 2024 reorganization, as well as previous iterations.

Military

THE PLA'S STRATEGIC SUPPORT FORCE (SSF): MADE AND UNMADE

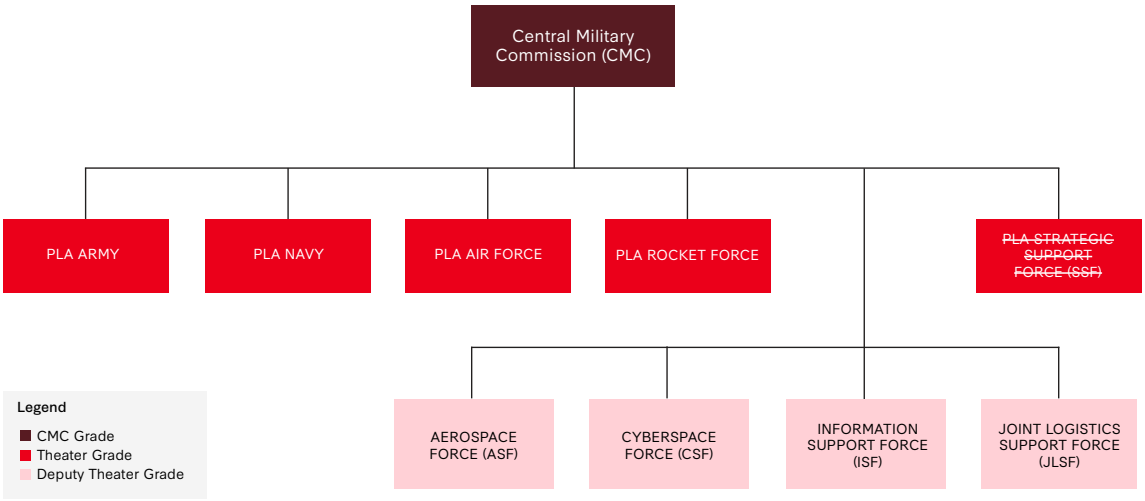
In 2015, apparently seeking to bring more discipline and order to Chinese efforts, Xi ordered a restructuring of China's cyber and information warfare capabilities. With the new structure, the SSF centralized military elements of warfare in the cyber domain, including electronic, information, and psychological warfare. The new group became a full service alongside the PLA Army, Navy, Air Force, Rocket Force, and Joint Logistics Support Force.[104] Several departments were placed under the new SSF, including the Aerospace Systems Department, the Electronic and Electromagnetic Systems Department, and, central to this discussion, the Network Systems Department.[105] At the time, the SSF appeared to be firmly in charge of coordinated Chinese efforts in the cyber domain. But less than a decade later, the PLA effectively disbanded the SSF. The reasons for this shift are unclear from the outside, but theories include an anti-corruption push, a recognition that the leaders of this new organization had too much power, or a reorganization aimed at further streamlining support functions.

The 2024 disbanding had several impactful features. First, the large SSF that was intended to streamline military functions is now a collection of independent "arms." Second, the heads of each arm were downgraded in rank and are no longer equivalent to the heads of the other theater-grade services. Despite this demotion, they still report to the Central Military Commission (CMC), whereas previously only the head of the SSF answered directly to the CMC.[106] Third, the information support role of the former SSF may have gained prominence. Finally, the disaggregation could be designed to more closely mirror the U.S. system, which might be seen as either a compliment or an attempt to more effectively measure Beijing's capability versus U.S. Cyber Command (USCYBERCOM). The actual roles and responsibilities of the forces appear largely unchanged.

For those who enjoy the lines and boxes of bureaucracy, the detailed breakdown of the SSF restructuring follows: On April 19, 2024, the PLA officially disbanded the SSF and created three new arms. The heads of these arms were declared "deputy theater-level branches," led by generals of slightly lower rank than the previous heads and lower ranks than the heads of the full services, like the PLA Army and Navy.[107]

The three new arms are the PLA Military Aerospace Force (ASF) (created from the SSF's Aerospace Systems Department), the PLA Information Support Force (ISF) (created from the SSF's Electronic and Electromagnetic Systems Department), and the PLA Cyberspace Force (CSF) (created from the SSF's Network Systems Department).[108] A fourth is the PLA Joint Logistic Support Force (JLSF), which was a preexisting body reclassified an arm and primarily oversees logistical operations.[109] Engaging in a bit of Kremlinology-type speculation, researcher Meia Nouwens suggested in an analysis for the IISS that the order in which the arms were announced in the Ministry of National Defense's press release might be significant. Specifically, the ASF and CSF might rank as more senior than the ISF.[110] This alignment completes the "three services and four arms" model. While the distinction between a service and an arm is unclear, arms appear to be largely independent of the four services.[111]

Figure 1: PLA Structure Post-2024 Reorganization



Source: J. Michael Dahm, "A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force," Jamestown Foundation, China Brief, vol. 24, no. 9, April 26, 2024, https://jamestown.org/program/a-disturbance-in-the-force-the-reorganization-of-peoples-liberation-army-command-and-elimination-of-chinas-strategic-support-force/.

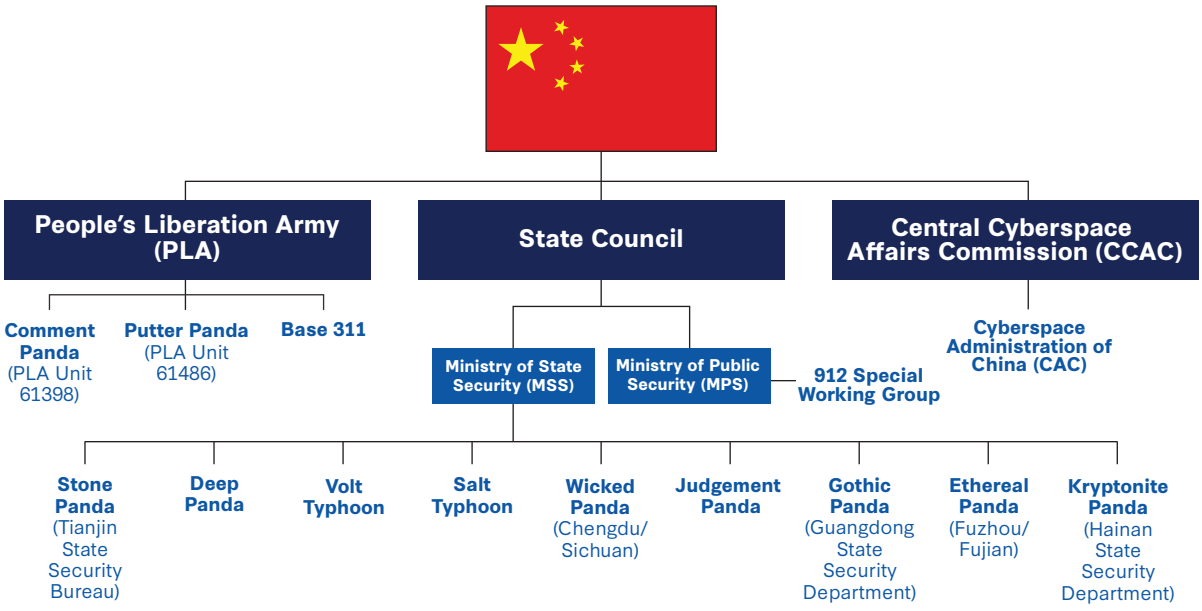
Initial analyses indicate that the roles and responsibilities of the arms will remain the same. The CSF will likely continue to conduct "defensive and offensive information operations," including "reinforcing national cyber border defense, . . . detecting and countering network intrusions and maintaining national cyber sovereignty and information security."[112] Further, according to a Usanas Foundation paper by Tenzin Younten, the CSF will also conduct "electronic warfare, psychological warfare, and technical reconnaissance" operations. The ISF will likely be responsible for "build[ing] a network information system that fulfils the [PLA's] requirements of modern warfare" and will oversee "informational warfare."[113] The reasons for this rapid reorganization are far more interesting and tell a potential story of corruption and weakness. They broadly fall into the categories of operational efficiency, a rise in prominence of these functions, or corruption crackdowns. The last of the three is the most likely explanation, but the following paragraphs will address each theory in turn.

Operational efficiency could conceivably be the main reason for the reorganization, but the evidence is thin.[114] In an article for *The Diplomat*, Ying Yu Lin and Tzu-Hao Liao write that the SSF's mandate encompassed a wide range of fields, including information and communications technology, aerospace, cyber operations, and electronic warfare. This range, combined with the SSF's decentralization, caused the service to "spread [itself] thin, with individual units vying for resources." Further, the model of incorporating everything into the SSF also led to redundancies and "overlapping organizational structures [that] impeded operational efficiency." For instance, the SSF's Aerospace Department "managed backend systems for space-related [systems and] equipment development." However, these were also overseen by the SSF's Equipment Development Department and certain bodies within the PLA Rocket Force and Air Force.[115] This may all be true, but it is hard to see how demotions and reorganization solve any of these problems. Subordinate operational efficiency may have been a notable side effect of the re-reorganization.

Another option is that this restructuring occurred to further separate and prioritize the cyber, space, and information domains within the PLA.[116] For instance, while the ASF and CSF likely retained much of their structures from their SSF predecessors, the entirely new ISF was created primarily to support general PLA activities. Therefore, Nouwens argues that in creating the ISF, Xi "likely thinks that the 'information support' function requires greater prominence," particularly at the "inter-service and inter-theatre levels."[117] In his Usanas Foundation paper, Younten partially supports this assessment by noting that the restructuring transformed the SSF "from a subordinate organization to a fully-fledged independent armed forces with enhanced capabilities, operational status, and resources." This shift may indicate a growing prioritization of these domains within the armed forces.[118] Lin and Liao partially concur: The 2024 "restructuring aims to enhance the PLA's capabilities in an era increasingly defined by information warfare and cyber operations."[119] At best, however, there is a mixed message regarding prominence. Demoted leadership suggests less priority is placed on these missions, but direct reporting to the CMC might suggest a higher priority, at least for centralizing these functions.

The third explanation is far more likely: a corruption purge. Two commanders disappeared after the reorganization and have not resurfaced. The former SSF commander, General Ju Qiansheng, and the former SSF deputy commander, Lieutenant General Shang Hong, have not been reshuffled into the PLA structure and have "largely disappeared from public view," according to Nouwens.[120] This could also explain why Xi sought to ensure the new leaders of these arms were of lower rank than the full theater-grade generals of the services, while still maintaining direct oversight over them through the CMC, which he chairs. However, this remains impossible to confirm and is entirely speculative.[121]

Figure 2: Chinese Cyber Actors



Source: CSIS research.

The true impact of this reorganization may not be revealed for years, or perhaps ever, if none of these units ever find themselves in conflict. The CCP does experiment with organization, which is made easier by a centralized, authoritarian system. However, reorganizations are disruptive, whether in a democracy or an autocracy, and this one could present opportunities to China's rivals.

PLA Cyber Units

The PLA has known military cyber units, primarily Comment Panda and Putter Panda, though much of the information surrounding both groups remains heavily guarded as state secrets.[122] There is also the PLA's "Three Warfares Base," also known as Base 311 (311 *jidi*), which is headquartered in Fujian Province.[123] According to the *Taiwan Link*, this base primarily focuses on "strategic psychological operations and propaganda directed against Taiwan."[124]

Cybersecurity firm Mandiant and Thailand's Electronic Transactions Development Agency (ETDA) believe Comment Panda and Putter Panda were engaged in cyber espionage as early as 2006 and 2007, respectively, making them some of the earliest known Chinese cyber units.[125] Comment Panda, in particular, is considered by Mandiant to be "one of the most prolific [Chinese] cyber espionage groups in terms of the sheer quantity of information stolen," although the full extent of its theft remains unknown.[126] Furthermore, because these PLA units are believed to "receive direct government support," they are thought to be among the largest and best-funded Chinese cyber units.[127] Both APTs appear to be headquartered in Shanghai.[128]

Both Comment Panda and Putter Panda likely fall under the newly formed CSF. This is because, prior to the establishment of the SSF in 2014, both groups were part of the PLA's 3rd General Staff Department (3PLA).[129] Following the PLA's 2015 reorganization, which created the SSF, 3PLA—along with other General Staff Departments (mainly 2PLA and 4PLA)—was merged into the Network Systems Department of the SSF, the precursor to the current Cyberspace Force.[130] According to the IISS and the Usanas Foundation, many components of the SSF's Network Systems Department were subsumed into the newly formed Cyberspace Force in 2024, which could mean that both Comment Panda and Putter Panda now fall under the Cyberspace Force.[131] However, this remains nearly impossible to publicly verify.

A 2024 report by cybersecurity firm Sekoia.io found a notable decline in reported PLA hacking operations since 2017.[132] This trend is attributed to the growing role of the MSS as China's main body for IP theft and the PLA being "retasked to directly support military operations," according to a piece in Lawfare.[133] Sekoia.io's 2024 report also notes that PLA operations increasingly target military and government organizations, prioritizing long-term persistence and stealth—factors that may explain why recent PLA hacking activities remain undiscovered. Additionally, Sekoia.io observes that many of the PLA's targets—such as military and government organizations—are reluctant to disclose incidents in which they have been successfully hacked, further contributing to the lack of public reports on PLA-related hacking.[134] Despite this, the report concludes it is unlikely that PLA hacking activities have diminished; rather, they have likely evolved and become more covert.[135]

COMMENT PANDA

Table 1: Aliases of Comment Panda

CrowdStrike	Mandiant	Secureworks	Chinese Government
Comment Panda	APT1	TG-8223	Unit 61398

Comment Panda was first active in 2006 and is believed to be among the largest and best-funded of China's cyber units.[136] Mandiant estimates that Comment Panda "is staffed by hundreds, and perhaps thousands of people."[137] According to Tom Uren of the Australian Strategic Policy Institute (ASPI), this estimate is based on several factors: the size of Comment Panda's compound in Shanghai's Pudong New Area (estimated by Mandiant at 130,663 square feet and 12 stories), the number of "concurrent operations" the group has carried out, and the overall volume of its cyber activities since 2007.[138] If this estimate is accurate, this could put the group on par with USCYBERCOM in terms of personnel size (USCYBERCOM is estimated to have approximately 6,200 civilian and military staff).[139] Furthermore, Comment Panda has its own dedicated fiber-optic communications infrastructure built by China Telecom.[140] Mandiant formally attributed the group to PLA Unit 61398, a secretive military hacking unit which was formerly part of the Second Bureau of the 3PLA.[141]

Comment Panda primarily targets U.S. companies and organizations and has stolen "hundreds of terabytes of data" from 141 U.S. organizations worldwide since 2006, according to the USCC. During this time, the group stole "technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, [company] emails, contact lists," primarily targeting the "nuclear power, metals, and solar" industries, likely to benefit Chinese state-owned enterprises.[142] To support its operations, Mandiant estimates that Comment Panda has "hundreds, and perhaps thousands of people . . . [including] linguists, open-source researchers, malware authors, [and] industry experts," in addition to facility and logistical staff. Mandiant also conservatively estimates that the group operates an attack infrastructure of "over 1,000 servers."[143]

The group primarily targets the IT, aerospace, telecommunications, and energy industries, along with other sectors China has identified as "strategic to [its] growth."[144] These include four of the seven "strategic emerging industries" highlighted in China's 12th Five-Year Plan.[145] Comment Panda is known for using spear-phishing e-mails containing malicious attachments to create custom back doors into its victims' systems as well as for deploying malware such as TROJAN.ECLTYS, BACKDOOR.BARKIOFORK, and BACKDOOR.WAKEMINAP.[146]

Comment Panda is responsible for the following notable cyberattacks:

- In May 2014, DOJ charged five "military hackers" affiliated with Comment Panda with conducting cyber espionage campaigns against Westinghouse Electric Company; the U.S. subsidiaries of SolarWorld; the United States Steel Corporation; Allegheny Technologies; the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union; and the Alcoa Corporation. This operation is believed

to have taken place between 2006 and 2014, and the subsequent 2014 DOJ indictment marked the first time the United States filed criminal charges against a foreign country for cyber espionage.[147]

- Comment Panda has been accused of stealing "hundreds of terabytes of data" from 141 organizations across 20 industries as part of a broader espionage campaign that spanned from 2006 to 2013.[148]

PUTTER PANDA

Table 2: Aliases of Putter Panda

CrowdStrike	Mandiant	Microsoft (old)	Secureworks	Chinese Government
Putter Panda	APT2	SULPHUR	TG-6952	Unit 61486

Cyber activity linked to Putter Panda was identified as early as 2007.[149] According to the USCC, the group is affiliated with PLA Unit 61486, formerly part of the 12th Bureau of the 3PLA.[150] Headquartered in Shanghai, Putter Panda primarily targets non-U.S. Western countries (though it has occasionally targeted U.S. companies) and has been known to conduct cyber espionage targeting the "satellite, aerospace, and communications industries to support China's space surveillance network."[151] Putter Panda's previous supervising body, 3PLA, was sometimes referred to as China's "National Security Agency" and was believed to be responsible for electronic intelligence, cyber reconnaissance, and signals intelligence collection for the PLA.[152] This background likely explains Putter Panda's focus on targeting foreign satellite, aerospace, and communications industries.

CrowdStrike noted that Putter Panda has a close working relationship with students from the School of Information Security Engineering at Shanghai Jiao Tong University (SJTU) and actively recruits them to "conduct network offense and defense campaigns." Putter Panda is also reportedly "staffed in part by current or former [SJTU] students."[153] The group typically uses spear-phishing emails and has been known to exploit the CVE-2012-0158 vulnerability in Microsoft Office and deploy MOOSE and WARP690 malware, according to MITRE and the USCC.[154]

Putter Panda was responsible for the following notable cyberattack:

- In June 2014, CrowdStrike investigators discovered that Putter Panda was conducting spear-phishing attacks to target attendees of space technology conferences. In one attack, the group sent fake emails inviting attendees to a yoga studio in Toulouse, France, along with malware-infused attachments disguised as conference-related information. Putter Panda also reportedly sent infected documents posing as job opportunities to lure additional victims.[155]

Intelligence and Civilian Bodies

Civilian agencies also play a key role in China's cyber operations. Beijing leverages a combination of government security services and ostensibly private front companies to advance its foreign policy objectives. Key among these agencies is the MSS, which serves as China's primary foreign intelligence agency; the MPS, which focuses mostly on domestic surveillance; and the CAC, which serves as China's central cyber regulator and oversees internet control and censorship.[156] While not much is known about the MPS's cyber units, the MSS operates a vast array of affiliated cyber units, each with varying specializations and expertise.

MINISTRY OF STATE SECURITY (MSS)

The MSS is China's main civilian intelligence service and is often likened to a combination of the United States' FBI and Central Intelligence Agency (CIA). Responsible for counterintelligence, political security for the CCP, and foreign, industrial, and cyber espionage, the MSS is responsible for some of China's most high-profile some of China's most high-profile cyberattacks, including operations targeting the United States.[157] According to Peter Mattis, a long-time China expert and former analyst in the CIA's counterintelligence center, the MSS's hacking activities are less well-known than the PLA's because they are "more skilled and much better at hiding their tracks."[158]

The MSS conducts cyber operations to gather various types of intelligence, including foreign, military, and commercial information.[159] CISA highlights that MSS-affiliated cyber actors often "us[e] publicly available information sources and common, well-known tactics, techniques, and procedures (TTPs) to target U.S. government agencies."[160] For example, Chinese MSS-affiliated cyber threat actors often "use open-source information to plan and conduct cyber operations . . . [and] use readily available exploits and exploit toolkits to quickly engage target networks."[161]

The MSS frequently hires contract hackers, often working through front companies, to conduct offensive cyber activities, infiltrate critical infrastructure, and steal IP.[162] According to a March 2024 U.S. Treasury Department indictment, Judgment Panda—a group believed to be linked to the Hubei State Security Department (HSSD)—is "a collection of Chinese state-sponsored intelligence officers, contract hackers, and support staff that conduct malicious cyber operations on behalf of the [HSSD]." This suggests that other MSS-affiliated APTs may also consist of a similar mix of contract hires, intelligence officers, and support staff connected to the MSS.[163] Intrusion Truth, a mysterious group known for exposing suspected Chinese cyber espionage operations, supports this assessment, noting that its "original blueprint for an APT in China requires: contract hackers and specialists, front companies, and an intelligence officer."[164]

Further, the MSS also operates through numerous subordinate branches at the provincial, city, municipality, and township levels, each wielding significant degrees of authority. However, the MSS "exercises coordination and leadership" over these lower levels of bureaucracy and oversees the country's "network of regional agencies."[165] Notably, provinces in China have their own MSS department (SSD) or bureau (SSB), each functioning as a regional government agency and integrated into the national state security system. This sharply contrasts with the intelligence community in the West, where international intelligence operations are often under the sole authority of the central government.

According to Joske, "the vast majority of China's state security personnel are working in these provincial agencies [and] by extension, probably carry out the majority of foreign intelligence operations."[166] This might also explain why "no cyber-attacks have been publicly attributed to the central MSS" in Beijing, while many attacks have been linked to APTs affiliated with MSS regional bodies at the provincial or municipality level (most notably the Sichuan, Guangdong, Hainan, Shandong, and Tianjin Security Departments and Bureaus).[167] The PLA's military intelligence is structured similarly, though its operations are organized by "regional theater command rather than province."[168]

Many of these regional bodies have specialized areas of focus. For example, the Zhejiang State Security Department focuses on "operations targeting Europe," while the Fuzhou branch of the MSS is dedicated to gathering intelligence on Taiwan.[169] Other provinces have technical expertise, such as Jiangsu, which is home to the Nanjing Institute of Information Technology, a large MSS research unit.[170] Additionally, provincial state security agencies under the MSS often recruit locally, which likely creates a correlation between the strength of a province's cyber capabilities and its proximity to highly ranked Chinese universities.[171] According to Joske, "the exact . . . reasons for different specialisations [at the provincial level] generally remains unclear, and it is not known how the MSS coordinates and controls provincial agencies."[172]

Notable MSS-affiliated groups involved in these operations include Stone Panda, Deep Panda, Vanguard Panda (Volt Typhoon), Salt Typhoon, Judgment Panda, Kryptonite Panda, Wicked Panda, Gothic Panda, and Ethereal Panda.

STONE PANDA

Table 3: Aliases of Stone Panda

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Stone Panda	APT10	POTASSIUM	Purple Typhoon	Bronze Riverside	menuPass

Stone Panda is an APT that has been active since at least 2006. The group typically targets construction, engineering, aerospace, and telecommunications firms, as well as foreign governments, with the goal of "acquiring valuable military and intelligence information" and stealing trade secrets to support Chinese businesses, according to Mandiant.[173] Symantec also reported that Stone Panda has historically targeted Japanese corporations and media organizations, likely for similar reasons.[174] The group is best known for using spear phishing and gaining access to victims' networks through managed service providers (MSPs). The group has been known to use the HAYMAKER, SNUGRIDE, and BUGJUICE malware retools.[175] Stone Panda has also been known to customize versions of the open-source QUASARRAT malware, using it as second-stage back doors in its attacks.[176]

In an indictment of two Stone Panda hackers, DOJ linked the group to the Tianjin State Security Bureau, a municipal division of the MSS. Stone Panda is also believed to operate through the Huaying Haitai Science and Technology Development Company, a front company affiliated with the MSS.[177]

Stone Panda is responsible for the following notable cyberattacks:

- Stone Panda's most notorious attack is the 2016 Cloud Hopper Operation, a hacking campaign that used spear phishing to infiltrate multiple MSPs. Once in their systems, the group would "hop" into the MSPs' client networks, stealing vast amounts of corporate IP and government secrets. High-profile targets included IBM, Hewlett Packard, NASA, Ericsson, Sabre, Huntington Ingalls Industries (HII), and several unnamed U.S. government agencies.[178]
- Stone Panda is also believed to have played a key role in the "Technology Theft Campaign," a long-running operation that began in 2006. During this campaign, the group gained access to the computers "of more than 45 technology companies," stealing "hundreds of gigabytes of sensitive data." The campaign primarily targeted companies in aviation, space, communications, advanced manufacturing, maritime technology, and oil and gas—all sectors highlighted in the CCP's Made in China 2025 plan to boost China's domestic tech industry and reduce its reliance on foreign companies.[179]
- According to cybersecurity company ESET, Stone Panda carried out Operation LiberalFace, a spear-phishing campaign in 2022 that targeted Japanese political entities and an unnamed Japanese political party. This operation occurred in the weeks leading up to Japan's House of Councilors election in July 2022.[180]

DEEP PANDA

Table 4: Aliases of Deep Panda

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Deep Panda	APT19	CHLORINE	Checkered Typhoon	Bronze Firestone	C0d0so0

Deep Panda is responsible for some of China's most invasive and large-scale cyber espionage campaigns. Deep Panda has been active since 2013 and primarily targets technology companies, U.S. defense contractors, nongovernmental organizations, and federal departments and agencies, likely for espionage purposes.[181] Deep Panda is known for breaching companies' defenses through customized spear-phishing emails, utilizing various malware tools such as C0d0so0, Cobalt Strike, Derusbi, EmpireProject, and Fire Chili, as well as exploiting a zero-day vulnerability in Adobe Flash.[182] Reports also suggest that Deep Panda has used malware created during student hacking competitions in China.[183] While Deep Panda is believed to be affiliated with the MSS, the specific SSB or SSD to which the group is connected is unknown.[184]

The group is responsible for the following notable cyberattacks:

- In February 2014, Deep Panda launched a phishing attack on employees at Anthem Blue Cross, successfully exfiltrating approximately 78.8 million members' medical records, including names, birth dates, Social Security numbers, phone numbers, email and home addresses, and patient financial data.[185] According to *The Record* and the *Washington Post*, the malware used in this attack was likely developed during the 2014 TOPSEC Cup, a student hacking competition sponsored by Southeast University's Information Security Research Center in Nanjing and the Beijing Topsec Network Security Technology Company, a defense contractor partially funded by the PLA.[186] According to ThreatConnect analysts quoted by Healthcare Finance News, the MSS may have hacked Anthem "for the purposes of gathering sensitive information for follow-on (human intelligence) targeting via blackmail [and] asset recruitment."[187]
- In June 2015, Deep Panda breached OPM, stealing 21.5 million Social Security numbers, including 19.7 million from Americans who had applied for a U.S. security clearance.[188] Later that year, the group also hacked United Airlines, compromising an undisclosed amount of personal travel records.[189]
- In February 2015, Deep Panda exploited a zero-day vulnerability in Adobe Flash to compromise the web servers of *Forbes* magazine. However, there was no evidence of successful data exfiltration in this breach.[190]

VANGUARD PANDA (VOLT TYPHOON)

Table 5: Aliases of Vanguard Panda

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Vanguard Panda	UNC3236	DEV-0391	Volt Typhoon	Bronze Silhouette	VOLTZITE

Vanguard Panda, more commonly known as Volt Typhoon, is a relatively new APT, first active in 2021, although some have suggested that activity in 2019 should also be attributed to the group.[191] It is known for secretly embedding itself in critical infrastructure sectors such as "communications, manufacturing, utilities, transportation, construction, maritime, government, and information" systems—often remaining undetected for months, or even years.[192] Volt Typhoon has targeted networks in Australia, India, and the United Kingdom but is perhaps best known for its attacks on U.S. critical infrastructure.[193] To date, the group has successfully breached infrastructure in Guam, as well as "water treatment plants, water wells, electrical substations, OT Systems, and network security systems" across the United States.[194]

According to Microsoft, the group is developing "capabilities that could disrupt critical communications infrastructure between the United States and Asia."[195] Additionally, Eric Goldstein, a former senior CISA official, told Reuters that most of Volt Typhoon's identified targets, such as mass transit systems or water treatment facilities, "have no legitimate espionage

value," suggesting that the group's true objective may be sabotage.[196] Volt Typhoon almost certainly has been "pre-positioning" itself to attack U.S. systems in the event of a "hot" conflict between China and the United States.[197]

In response, U.S. government officials have issued advisory warnings, including a joint statement on February 7, 2024, by then-FBI Director Christopher Wray and then-National Cyber Director Harry Coker. Coker warned that Volt Typhoon's efforts are designed to "disrupt [the U.S.] military's ability to mobilize," while Wray stated that the group is preparing to "wreak havoc and cause real-world harm to American citizens and communities if and when China decides the time has come to strike."[198]

According to CrowdStrike and *The Guardian*, Volt Typhoon uses living-off-the-land (LOTL) techniques to remain hidden.[199] This method involves using legitimate, often native tools already present within the victim's operating system to carry out the attack, which significantly complicates detection, especially when used with stolen valid credentials obtained through phishing.[200] Volt Typhoon tries to "blend into normal network activity by routing traffic through compromised small office and home office (SOHO) equipment, including routers, firewalls, and VPN hardware."[201] The group is known to use customized versions of open-source malware tools and Fast Reverse Proxy tunneling tools to breach firewalls and covertly sign into systems.[202] While it is widely believed that Volt Typhoon is affiliated with the MSS, there is no definitive information on which specific provincial subunit of the MSS oversees the group.[203]

The group is responsible for the following notable cyberattack:

- In December 2023, Lumen Technologies uncovered the "KV-botnet," a botnet likely developed by Volt Typhoon.[204] According to the January 2024 DOJ indictment, most of the compromised devices were outdated Cisco and NetGear routers that had reached "end of life" status, meaning they no longer received security patches or updates.[205] This vulnerability allowed Volt Typhoon hackers to infiltrate SOHO routers, firewalls, and VPNs across the United States and embed themselves into the networks of multiple critical infrastructure sectors, including "aviation, rail, mass transit, highway, maritime, pipeline, water and sewage organizations."[206] Although it is unclear how long Volt Typhoon has been embedded in U.S. networks, some U.S. intelligence officials believe the group has maintained quiet access and footholds within U.S. IT systems for "at least five years."[207] This suggests the group may have actually been active as early as 2019.

KRYPTONITE PANDA

Table 6: Aliases of Kryptonite Panda

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Kryptonite Panda	APT40	GADOLINIUM	Gingham Typhoon	Bronze Mohawk	Leviathan

Kryptonite Panda has been active since 2013 and is affiliated with the Hainan State Security Department, a provincial branch of the MSS.[208] The group is primarily known for targeting naval defense contractors to support China's naval modernization efforts.[209] Kryptonite Panda has also targeted research institutions, private companies, and government entities across the aviation, government, defense, healthcare, and biopharmaceutical sectors, mostly in the United States, Canada, the Middle East, and Western Europe.[210] The main objective of these attacks is believed to be the theft of IP and proprietary research to reduce R&D costs for Chinese businesses.[211]

According to CISA and the USCC, Kryptonite Panda primarily uses spear phishing to target internet-facing routers and VPNs.[212] The group has also been known to use over 51 different malware families, including BADSIGN, FIELD GOAL, and FINDLOCK, and it employs LOTL techniques similar to those used by Volt Typhoon.[213] Kryptonite Panda is believed to operate through the Hainan MSS-affiliated front company Hainan Xiandun Technology Development Company, which it has used to conduct cyber espionage campaigns targeting universities and to steal proprietary research related to infectious diseases.[214]

Furthermore, in 2021, *The Record* and the USCC linked Kryptonite Panda to the HAFNIUM group (also known as Silk Typhoon).[215] This connection seems plausible, as both groups operate out of Hainan and are heavily involved in industrial espionage.[216]

The group is responsible for the following notable cyberattacks:

- In September 2017, Proofpoint detected spear-phishing emails, allegedly sent by Kryptonite Panda, targeting U.S. shipbuilding companies and universities. The emails posed as fake internship applications containing malicious files and attachments.[217] While the targeted shipbuilding companies were not named, the *Wall Street Journal* reported that over 27 universities in the United States, Canada, and Southeast Asia were targeted, including the University of Hawaii, the University of Washington, the Massachusetts Institute of Technology, Pennsylvania State University, and Duke University. These attacks are widely believed to have targeted university research laboratories receiving funding from DOD.[218]
- In July 2021, DOJ charged four members of Kryptonite Panda with hacking and stealing IP from the "aviation, defense, education, government, health care, biopharmaceutical and maritime" industries between 2011 and 2018.[219] The stolen trade secrets included technologies related to submersibles, autonomous vehicles, chemical formulas,

aircraft, and "proprietary genetic-sequencing technology and data."[220] The group also notably targeted research universities, exfiltrating infectious disease research on Ebola, MERS, HIV/AIDS, Marburg, and tularemia. According to the indictment, the aim was to help Chinese companies bypass "lengthy and resource-intensive research and development processes."[221]

- If Kryptonite Panda is indeed the same group as HAFNIUM, it would also be responsible for the infamous 2021 Microsoft Exchange Server hack, which compromised more than 30,000 servers in the United States and hundreds of thousands other servers worldwide.[222] For further details on the 2021 Microsoft Exchange Server hack, please refer to Case Study 2 on page 39.

WICKED PANDA

Table 7: Aliases of Wicked Panda

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Wicked Panda	APT41	BARIUM	Brass Typhoon	Bronze Atlas	Double Dragon

Wicked Panda has been active since 2012 and is affiliated with the Sichuan branch of the MSS.[223] A prolific APT, the group has targeted over 100 organizations across 14 countries.[224] According to a DOJ indictment, the group has been accused of stealing "source code, software code signing certificates, [and] customer account data" from IT, telecommunications, social media, and video game companies, as well as from "non-profit organizations, universities, think tanks, and foreign governments, . . . [and] pro-democracy politicians and activists in Hong Kong."[225]

Wicked Panda primarily employs "spear-phishing, . . . credential stealers, keyloggers, and rootkits" in its attacks. The group has also been involved in ransomware and cryptojacking schemes, which hijack victims' devices to mine cryptocurrency.[226] According to Demian Ahn, a former assistant U.S. attorney, Wicked Panda has significant resources at its disposal, including "tens of thousands of machines [running] at one time."[227] FireEye Threat Intelligence has also linked Wicked Panda to another group, Vixen Panda (APT15), due to their use of similar tools and digital certificates, although this remains difficult to confirm.[228]

The group is responsible for the following notable cyberattacks:

- In May 2021, Wicked Panda launched a months-long campaign exploiting zero-day vulnerabilities in the USAHerds application (CVE-2021-44207) and the Log4j framework (CVE-2021-44228). This quiet but effective cyber espionage operation, which ran from May 2021 to February 2022, successfully compromised at least six U.S. state government networks and harvested an undisclosed quantity of user credentials.[229]
- In December 2022, Wicked Panda hackers were accused of stealing over $20 million in U.S. Covid-19 relief benefits, including Small Business Administration loans and unemployment

insurance funds across 12 U.S. states, according to the U.S. Secret Service. The Secret Service also suggested that the operation may have targeted all 50 states. This marked the first time the United States publicly acknowledged a case of foreign, state-sponsored pandemic fraud.[230]

JUDGMENT PANDA

Table 8: Aliases of Judgment Panda

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Judgment Panda	APT31	ZIRCONIUM	Violet Typhoon	Bronze Vinewood	RedBravo

Judgment Panda has been active since 2016 and is affiliated with the Hubei State Security Department.[231] According to a Treasury Department indictment, the group consists of "a collection of Chinese state-sponsored intelligence officers, contract hackers, and support staff."[232] The group is believed to operate through Wuhan Xiaoruizhi Science and Technology Company Limited (Wuhan XRZ), a front company sanctioned by the U.S. Department of the Treasury.[233]

Judgment Panda primarily engages in cyber espionage, targeting U.S. government officials, including high-ranking advisers, White House national security staff, and U.S. government personnel from the Departments of Justice, Commerce, Treasury, and State. The group has also targeted both Democratic and Republican members of Congress, political campaign staffers, and individuals involved in the 2020 Trump and Biden campaigns.[234] Similar to Kryptonite Panda, Judgment Panda has conducted cyberattacks against universities with ties to DOD and organizations in the financial sector.[235]

Judgment Panda has also carried out cyber espionage campaigns against dissidents living abroad and other individuals and organizations the CCP perceives as threats. According to CyberScoop, the group monitored "thousands of U.S. and Western politicians, foreign policy experts, academics, journalists and democracy activists . . . 'perceived as being critical of PRC government policies.'"[236] Judgment Panda has also targeted the family members of dissidents through malicious emails and tracking links to gather information on their locations, IP addresses, and online activities.[237] The group has primarily exploited vulnerabilities in applications like Java and Adobe Flash and is known to use a variety of malware, including SOGU, LUCKYBIRD, SLOWGYRO, and DUCKFAT. Judgment Panda frequently employs remote access trojans (RAT) such as 9002, Gh0st RAT, Sakula RAT, and Trochilus to gain access to its victims' systems.[238]

The group is responsible for the following notable cyberattacks:

- In March 2022, Judgment Panda targeted an undisclosed number of Gmail accounts associated with U.S. government personnel. The group used sophisticated credential-phishing emails and emails containing tracking links to target the personal

accounts of campaign staffers. The likely purpose of the attack was espionage and information gathering.[239]

- In March 2024, Judgment Panda launched a sweeping cyber espionage campaign targeting "millions of people" worldwide. Although the primary targets were individuals critical of Beijing, Reuters also uncovered evidence of trade secret theft, suggesting a potential element of opportunism.[240] The targets included "White House staffers, U.S. senators, British parliamentarians, and government officials." The breach is also believed to have compromised the work accounts, personal emails, and phone records of "millions of Americans."[241] According to then-Deputy U.S. Attorney General Lisa Monaco, the hack aimed to "repress critics of the Chinese regime, compromise government institutions, and steal trade secrets."[242]

GOTHIC PANDA

Table 9: Aliases of Gothic Panda

CrowdStrike	Mandiant	Microsoft (old)	Microsoft (new)	Secureworks	Other
Gothic Panda	APT3	BORON	Brocade Typhoon	Bronze Mayfair	Boyusec

Gothic Panda has been active since 2007 and is believed to be affiliated with the Guangdong State Security Department (GSSD).[243] Gothic Panda is believed to operate out of Guangzhou Boyu Information Technology Company, Ltd. ("Boyusec"), a front company posing as a cybersecurity firm but affiliated with the GSSD and the Guangdong Provincial Information Security Assessment Center, a government bureau that "conducts security assessments of software."[244]

According to the USCC, the group targets organizations in the "aerospace, defense, construction, engineering, high-technology, telecommunications, and transportation sectors."[245] Winnona DeSombre of Harvard University's Belfer Center noted that Gothic Panda has also been known to observe and reverse engineer U.S. hacking tools allegedly used against Chinese systems.[246] This may explain why the group was found using NSA-developed hacking tools and artifacts a full year before these capabilities were made public in the 2016 Shadow Brokers leak.[247] Gothic Panda previously used phishing emails and zero-day exploits in browsers such as Internet Explorer and Firefox and in the now discontinued Adobe Flash Player.[248] The group is also known to deploy malware like SHOTPUT, COOKIECUTTER, and SOGU.[249]

The group is responsible for the following notable cyberattack:

- In November 2017, DOJ charged three hackers, allegedly belonging to Gothic Panda, for sending spear-phishing emails containing malicious attachments and links to employees at Trimble, Siemens, and Moody's Analytics. These attacks were carried out between 2011 and 2017 and stole trade secrets.[250]

ETHEREAL PANDA

Table 10: Aliases of Ethereal Panda

CrowdStrike	Microsoft (old)	Microsoft (new)	Other
Ethereal Panda	Storm-0919	Flax Typhoon	RedJuliett

Ethereal Panda has been active since 2021 and is known for targeting "government agencies and education, critical manufacturing, and information technology organizations," mostly in Taiwan.[251] The group has also hacked organizations in Southeast Asia, North America, and Africa.[252] According to Recorded Future, Ethereal Panda operates out of Fuzhou, a city whose MSS branch focuses on gathering intelligence on Taiwan.[253] However, since Fuzhou is within the PLA's Eastern Theater Command, which also focuses on Taiwan, some speculate that Ethereal Panda may instead be affiliated with the PLA rather than the MSS, though this remains difficult to confirm.[254]

According to Microsoft, Ethereal Panda uses LOTL techniques to "quietly remain in [organizations'] networks" for extended periods, similar to Volt Typhoon.[255] However, unlike Volt Typhoon, which mostly targets internet routers, Ethereal Panda exploits vulnerabilities in public-facing servers and Internet of Things devices such as "cameras, video recorders and storage devices."[256] The group then uses LOTL methods to maintain persistence and exfiltrate credentials from victims' networks.[257] Ethereal Panda's focus on Taiwan is noteworthy, as it shares many attributes with Volt Typhoon, such as its extensive use of LOTL techniques to remain covertly embedded in systems for extended periods of time. Consequently, like Volt Typhoon, Ethereal Panda could be positioning itself within Taiwan's systems to potentially disrupt critical infrastructure in the event of a full-scale Chinese invasion of the island. If true, this would make Ethereal Panda the Taiwan equivalent of Volt Typhoon, which targets U.S. critical infrastructure. In addition to targeting Taiwan, the group has also hacked organizations in countries such as Djibouti, Kenya, Rwanda, Hong Kong, Malaysia, the Philippines, and South Korea.[258]

The group is responsible for the following notable cyberattack:

- In June 2024, Insikt Group, Recorded Future's threat research division, identified Ethereal Panda as responsible for hacking government organizations in Taiwan, Laos, Kenya, and Rwanda. The attacks, which took place between November 2023 and April 2024, targeted "70 Taiwanese organizations in the academic, government, think tank, and technology sectors," as well as three Taiwanese universities and de facto embassies.[259] The group is also believed to have stolen 1.7 terabytes of sensitive data from Taiwanese telecom giant Chunghwa Telecom, including government contacts and files from the Taiwanese armed forces, foreign ministry, and coast guard.[260] Insikt Group suggests that Ethereal Panda exploited vulnerabilities in Linux operating systems to carry out these attacks.[261]

SALT TYPHOON

Table 11: Aliases of Salt Typhoon

Mandiant	Microsoft (new)	Other	Other
UNC2286	Salt Typhoon	FamousSparrow	GhostEmperor

Salt Typhoon has been active since at least 2019 and is known for targeting numerous telecommunications companies as well as high-profile individuals in the 2024 U.S. presidential election. Initially focused on organizations in Southeast Asia, the group has since expanded its operations globally, targeting industries such as hospitality, engineering, and law in Brazil, Burkina Faso, Canada, France, Guatemala, Israel, Lithuania, Saudi Arabia, South Africa, Taiwan, Thailand, and the United Kingdom.[262] Salt Typhoon is likely an arm of the MSS, and its operations are believed to focus on intelligence gathering.[263]

The group is known for exploiting ProxyLogon vulnerabilities in Microsoft Exchange Server (including CVE-2021-26855) and for using the Demodex rootkit.[264] In its most recent breaches of U.S. telecommunications companies in September 2024 (described below), the group is suspected of exploiting vulnerabilities in Cisco internet routers, though this has yet to be confirmed.[265]

The group is responsible for the following notable cyberattack:

- On September 26, 2024, hackers believed to be part of Salt Typhoon successfully gained access to the networks of cable and broadband providers, enabling them to retrieve data stored by U.S. telecommunications companies.[266] The affected companies include AT&T, Lumen Technologies, T-Mobile, and Verizon.[267] While some speculate that the group exploited vulnerabilities in Cisco internet routers to achieve this access, this has not been confirmed.[268] The campaign also allowed the group access to the communications of U.S. officials and candidates, including then-presidential candidate Donald Trump, then-vice presidential candidate JD Vance, and the campaign staff of then-Vice President Kamala Harris.[269] According to the *Washington Post*, Salt Typhoon was able to "listen in on audio calls in real time"—data that is highly valuable to Chinese intelligence agencies.[270] The group reportedly had access to this system for "months" and appeared to be collecting intelligence, according to the *Wall Street Journal*.[271]

MINISTRY OF PUBLIC SECURITY (MPS)

The MPS is responsible for overseeing China's public security, including domestic surveillance and cybersecurity.[272] Similar to the MSS, the MPS has a provincial-level Public Security Bureau in "each province, autonomous region, and municipality directly under the central government."[273] The MPS plays a key role in China's cybersecurity infrastructure, and its powers were significantly expanded under the 2017 National Cybersecurity Law (CSL).[274] Under the CSL, the MPS is designated as one of the agencies responsible for "cybersecurity protection, supervision, and management" and has since incorporated cyber into its already broad mandate of "investigating matters in public and internal security."[275] Additionally, the MPS is tasked with "punishing actors that violate the [2017] CSL," giving it significant autonomy and authority to monitor and inspect domestic cyber

and network systems, as well as foreign companies operating in China. For example, as of 2018, the MPS has the power to "conduct on-site and remote inspections of any company with five or more computers connected to the internet"—a broad definition that effectively includes almost every foreign company operating in China.[276] During these inspections, the MPS can "copy user information, log security response plans during on-site inspections, and check for vulnerabilities."[277] According to *The Record*, this information can also be used by state surveillance or security agencies "to monitor a company's inner workings as well as its customers."[278]

The MPS is further permitted to involve third-party "cybersecurity service agencies" in remote inspections, allowing it to enforce China's censorship laws under the guise of network security.[279] Additionally, according to the USCC, the PLA "may call up personnel within . . . the MSS and MPS to participate in cyberwarfare missions on an ad hoc basis."[280] However, little information is available about these arrangements, though it is likely that both the MPS and MSS would "have operational roles during a conflict."[281]

According to Sekoia.io, a primary purpose of the MPS is to combat the "five poisons" to maintain internal security. These include democracy advocates, Taiwan, Tibetans, Uyghurs, and Falun Gong—a domestic religious and spiritual movement that the CCP perceives as a threat.[282] The MPS's classification of these groups as threats to internal security could explain its activities beyond China's borders, including harassment campaigns targeting dissidents living abroad, often linked to the MPS's United Front Work, as well as cyber influence operations conducted by its 912 Special Working Group.[283]

While there are very few publicly known cyber-related units within the MPS, notable examples include the aforementioned 912 Special Working Group and the MPS's First Research Institute. The 912 group is responsible for influence operations and uses thousands of fake social media accounts to target Chinese dissidents and pro-democracy activists living abroad.[284] For example, in its April 2023 indictment, DOJ charged 40 MPS officers—many suspected of belonging to the 912 Special Working Group—and two CAC officials for perpetrating "transnational repression schemes targeting U.S. residents."[285]

The First Research Institute "supports the operational elements of the MPS" and has been known to post programming job vacancies on EvilOctal.com and XFOcus.net—two large online hacker communities—likely to recruit talent and "build consulting relationships." [286] For example, Peng Yinan, the founder of Chinese hacker group Javaphile (who breached the White House website in 2001) maintains a "formal consulting relationship" with the Shanghai Public Security Bureau, the city's municipal branch of the MPS.[287] However, aside from these examples, researchers were unable to identify other publicly known MPS-affiliated cyber units, institutes, or hacker groups for this report, though they likely exist.

CYBERSPACE ADMINISTRATION OF CHINA (CAC)

The CAC is China's central internet regulator and its primary agency for control, oversight, and censorship. The CAC originates from the CCP's propaganda system and operates under the Central Cyberspace Affairs Commission (which itself falls under the CCP Central Committee). Since 2018, the CAC has operated under the Office of the Central Cyberspace Affairs Commission (CCAC).[288] However, some sources suggest that the CCAC and CAC may refer to the same entity, with the CAC serving as its public regulatory-body name.[289] In 2017, the CAC released a policy document directing "the

deepened development of military-civilian integration for cybersecurity and informatisation," further strengthening ties between the PLA and Huawei, China's telecommunications giant.[290]

The CAC oversees administrative licensing and regulation and "represents China in international cyber-related activities."[291] According to Thomson Reuters, the CAC is also "in charge of cyberspace security and internet content regulation" and is responsible for "directing, coordinating and supervising online content management and handling administrative approval of businesses related to online news reporting."[292] Stanford University's DigiChina Project notes that the CAC "lacks many formal attributes of an administrative agency," notably "institutional transparency and accountability," making it an especially powerful regulatory body.[293] Similarly, the CAC's original mandate to "manage and enforce requirements for online content" has expanded significantly in recent years and now encompasses "policy and regulation on cybersecurity, data security, and privacy", according to the DigiChina Project.[294] Consequently, the CAC functions much like a "supra-ministerial regulator," with authority over "all state and private sectors touched by . . . online activity."[295]

This broad jurisdiction was notably demonstrated in its surprise 2021 crackdown on DiDi Global, a Chinese ride-sharing company that went public in June 2021 through an initial public offering (IPO) on the New York Stock Exchange. Immediately after the IPO, the CAC launched a comprehensive cybersecurity review of the company, ordered that DiDi's apps be removed from Chinese online stores for "illegally collecting personal information," and fined the company $1.2 billion for violating "cybersecurity, data security, and personal information protection laws."[296] The exact reasons for the CAC's intense scrutiny of DiDi remain unclear. Some speculate that DiDi may have angered the CAC by proceeding with its U.S. IPO despite the agency's request for a delay. Others suggest the move was politically motivated rather than security-driven or that DiDi's frequent rule-bending became a problem, though the specific political objectives remain unclear.[297]

Public/Private

NONGOVERNMENTAL ACTORS

National Cybersecurity Center

One step removed from the government are organizations like the National Cybersecurity Center, which houses multiple research and talent centers, laboratories, and an operational national cybersecurity school. Two of its labs, the Combined Cybersecurity Research Institute and the Offense-Defense Lab, conduct cybersecurity research for the Chinese government.[298] Furthermore, in 2017, China established the Central Commission for Integrated Military and Civilian Development within the 360 Enterprise Security Group—one of China's most prominent cybersecurity companies—with the aim of "enhancing private sector cooperation" with the PLA and furthering its cyber warfare capabilities.[299] China has also called on private entities for certain tasks, though this area is thinly studied. This project will attempt to identify trends in China's use of ostensibly private entities for developing accesses and conducting offensive operations in the cyber domain.

Patriotic Hackers and Hacktivists

China is home to a large array of patriotic hackers, primarily from the private sector.[300] These hackers first gained notoriety for defacing U.S. government websites in response to the accidental 1999 bombing of the Chinese embassy in Belgrade, marking the first documented cyber operation by actors based in China against the United States.[301] However, since 2015, the central government has gradually tightened its control over these groups, which now largely operate under the loose supervision of intelligence officers and primarily focus on surveillance and espionage rather than incendiary offensive cyber operations.[302]

China also employs more independent, less supervised cyber volunteers known as hacktivists. This group consists primarily of malware developers and security researchers who engage in large-scale, politically motivated cyber operations such as DDoS attacks, foreign network defacement, and data destruction.[303] Hacktivist activity often includes high-profile cyberattacks on Taiwan in response to specific events. For instance, immediately before then- U.S. Speaker of the House Nancy Pelosi's visit to Taiwan in August 2022, Chinese hacktivists hit the websites of then-Taiwanese President Tsai Ing-wen, the National Defense Ministry, the Foreign Affairs Ministry, and the Taiwan Taoyuan International Airport, the island's largest airport, with DDoS attacks.[304] Some 7-Eleven convenience store television screens were also hacked, displaying the message: "Warmonger Pelosi, get out of Taiwan!"[305] Since these attacks were ostensibly carried out by independent hackers, Beijing could deny involvement, but it is likely that Beijing played some role in enabling these activities or, at the very least, turned a blind eye to them.

Screen of a device hacked by the Javaphile hacktivist group.

Source: "Extant Hacker Typology," Hacker Innovation, https://hackerinnovation.mikepinder.co.uk/index.php?title=Extant_Hacker_Typology.

To strengthen its hacker network, China frequently also hires individuals as contractors for offensive cyber tasks or recruits them into information security roles and programming positions affiliated with the MSS or MPS. As with MSS-affiliated front companies, the blurred line between Chinese government actors and state-sponsored actors makes it especially challenging for outside countries to attribute responsibility for the actions of these patriotic hackers and hacktivists. According to Amy Chang of the Center

for a New American Security (CNAS), the Chinese government uses non-state actors to "credibly signal coercive threats" on its behalf, targeting countries with which the CCP has conflicts or disagreements.[306] This assessment is supported by researcher Jeffrey Kwong, who found a recurring pattern in which official threats issued by the Chinese government against a country are often followed by cyberattacks carried out by Chinese hacktivist groups.[307]

However, Kwong also notes that many of these hacktivist groups are relatively "uncontrolled and more nationalistic than the state," posing a "risk of domestic unrest" if the Chinese government retreats from its threats.[308] Ultranationalist hacktivist groups have even launched cyberattacks against the Chinese state to "express displeasure" about perceived CCP restraint, which also often "coincide with periods of discontent with the CCP."[309] For example, in 2014, a hacktivist group hijacked the state television network in Wenzhou to broadcast "nationalistic and anti-CCP messages," likely in protest against the detention of Wang Bingzhang, a nationalist activist.[310]

Case Studies

Case Study 1: The Great Sucking Sound: Data Leaves in Droves

China has been highly effective at stealing massive amounts of data. Since 2014, China has hacked and stolen the data of about 80 percent of Americans.[311] In the attack that year on the health insurance company Anthem, China exfiltrated an estimated 79 million member names, birth dates, Social Security numbers, and highly sensitive personally identifiable information.[312] The same year, China's hack of OPM compromised 21.5 million personnel records. Millions more records followed in the 2016 hack of Starwood Hotels and in the 2017 hack of Equifax. Data at this scale is helpful for a range of uses, including training AI models, identifying vulnerabilities among people with security clearances, and informing potential influence campaigns.

Some of these hacks have involved hoovering up data seemingly indiscriminately, but four instances in particular suggest a campaign to create a constellation of highly useful data. The first occurred on February 18, 2014, when the Chinese state-backed group Deep Panda used a phishing scam to trick an Anthem employee into opening an e-mail containing malware. Once opened, the email deployed malware on the employee's computer, allowing the attackers to infect the device and move laterally within Anthem's networks, ultimately gaining access to "over 50 employee accounts and 90 different systems." Among these systems was Anthem's data warehouse, which stored records for "millions" of Anthem members.[313] From February to December 2014, the group successfully exfiltrated approximately 78.8 million member records, including names, birthdates, Social Security numbers, email addresses, home addresses, and patient financial data.[314] It was not until January 27, 2015, that Anthem discovered the breach and notified law enforcement. By then, however, the

damage was done. The 2014 Anthem hack remains the largest known cyber incident in the U.S. healthcare industry.[315]

What makes the Anthem hack even more notable is that the malware used in the initial breach was likely developed by Chinese university students only a few months prior.[316] ThreatConnect was able to trace the IP address embedded in the Anthem malware back to the 2014 TOPSEC Cup, a student hacking competition sponsored by Southeast University's Information Security Research Center in Nanjing and the Beijing Topsec Network Security Technology Company, a defense contractor partially funded by the PLA. The competition, which reportedly awarded an internship at Beijing Topsec as the final prize, is believed to have awarded points to students for hacking real targets inside the United States. Deep Panda hackers are believed to have modified malware developed in this competition for their breach of Anthem.[317] Southeast University is also known for connecting promising students to jobs in government security services and "research positions," drawing from a consistent pipeline of young talent for the MSS.[318]

The second incident occurred concurrently with the 2014 Anthem hack, when the same APT, Deep Panda, is also believed to have breached OPM.[319] According to CSO Online, this breach began when the group successfully compromised the systems of USIS and KeyPoint, two U.S. government contractors that were conducting background checks on government employees with "access to OPM servers." These initial breaches trace back to December 2013; however, OPM officials did not detect the breach until March 2014. Notably, because OPM officials determined that the hackers were "confined to a part of the network that didn't have any personnel data," they chose not to immediately expel the hackers, opting instead to monitor their activity to gather counterintelligence.[320] According to a report by the House Committee on Oversight and Government Reform, OPM planned a "Big Bang" system reset to expel the hackers on May 27, 2014.[321] However, by this time, Deep Panda had already used stolen credentials from its earlier KeyPoint hack to establish a secondary, hidden foothold within OPM's network and create a backdoor. After the May 27 reset, Deep Panda retained access to OPM's networks, quietly exfiltrating data from July to October 2014.[322] By October, the group had used OPM's compromised network to breach the Department of the Interior's servers, which contained millions of U.S. government personnel records.[323] This continued through December 2014, resulting in the exfiltration of an additional 4.2 million personnel records. By March 2015, federal personnel fingerprint data had also been compromised.[324]

Overall, the OPM breach resulted in the theft of 21.5 million records, including some of the most sensitive data, such as "millions" of SF-86 forms, which contain personal background check information for individuals seeking U.S. government security clearances, including details on "past drug use, financial history, mental health history and personal relationships," as well as information about their friends, family members, known associates, and contacts abroad.[325] The breach also compromised the fingerprints of 5.6 million federal employees and the information of 3.6 million current and former government employees.[326] According to a July 2015 OPM statement, "If an individual underwent a background investigation through OPM in 2000 or afterwards . . . it is highly likely that the individual is impacted by this cyber breach."[327]

Since these two major attacks, China has also been implicated in other high-profile breaches, though it remains unclear if the same APT, Deep Panda, was responsible. In 2016, hackers successfully compromised Starwood Hotels' reservation system and stole the credit card and passport information of approximately 500 million people.[328] In 2017, Beijing's hackers broke into Equifax, a credit reporting agency, and stole the financial information of approximately 148 million Americans, including hundreds of thousands of credit card numbers and credit dispute documents.[329] This combination of data is highly valuable to Beijing, as it can help identify U.S. government employees with security clearances who have financial or health issues, track their past and upcoming travel, and create opportunities for recruitment.[330]

Case Study 2: Exchange Hack

From January to March 2021, hackers associated with the HAFNIUM group (possibly Kryptonite Panda) conducted a rapid and audacious campaign of data exfiltration.[331] As early as January 3, 2021, the hackers began conducting cyber espionage operations against on-premises Microsoft Exchange servers.[332] In February, attacks spread globally.

In early March, Microsoft finally detected multiple zero-day exploits targeting its on-premises Microsoft Exchange Server.[333] CISA followed rapidly with an emergency directive, instructing all Federal Civilian Executive Branch agencies to "immediately disconnect Microsoft Exchange on-premises servers" and conduct incident response procedures.[334] As Microsoft prepared to issue a patch on its normal release schedule (March 9 or "patch Tuesday"), attacks increased between Friday, March 5, and Monday, March 8, and Chinese operators began to exfiltrate huge amounts of information, particularly emails.[335] According to Tom Burt, Microsoft's then-corporate vice president for security and trust, Microsoft saw attacks grow from "hundreds a day . . . [to] north of several thousand a day." Security researchers eventually assessed that China breached more than 30,000 servers in the United States and hundreds of thousands worldwide.[336]

This attack showed the power of a hybrid approach, where skilled government hackers quietly capitalized on the vulnerability. However, as soon as Beijing saw Microsoft ready to patch, a huge number of attackers apparently joined the operation. To what end is unclear: that much data may or may not ever be fully exploited and useful, but one potential use might be to train AI large language models.

Case Study 3: Volt Typhoon

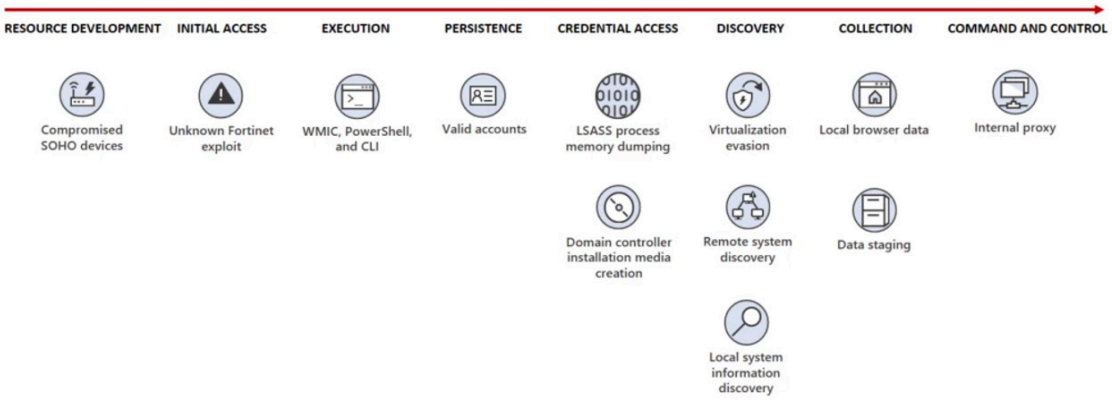
In late 2023 and throughout 2024, U.S. entities revealed a Chinese effort to compromise critical infrastructure in the mainland United States and Guam. The attacks produced little to no intelligence value; instead, they seemed designed to hold U.S. infrastructure at risk of outage at a time of China's choosing.

In December 2023, Lumen Technologies uncovered the KV-botnet, a botnet likely developed by Volt Typhoon.[337] According to a January 2024 DOJ indictment, most of the compromised devices were outdated Cisco and NetGear routers that had reached "end of life" status, meaning they

no longer received security patches or updates.[338] Volt Typhoon exploited these vulnerabilities using LOTL techniques to covertly infiltrate SOHO routers, firewalls, and VPNs across the United States.

Volt Typhoon embedded itself into the networks of "aviation, rail, mass transit, highway, maritime, pipeline, water and sewage organizations."[339] Earlier attacks successfully breached the internet servers of the Port of Houston, the largest U.S. port by total annual tonnage, in September 2021, as well as the two largest telecommunications providers in Guam.[340] Chinese cyberattacks on U.S. critical infrastructure likely predate 2021, as breaches were detected as early as December 2011 and 2013 within the systems of U.S. oil and natural gas pipelines. However, CISA has not formally attributed these breaches to a specific APT, and there is no indication that they were the work of Volt Typhoon.[341]

Figure 3: Volt Typhoon Attack Diagram



Source: Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques," Microsoft Security (blog), Microsoft, May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

China's true agenda is almost certainly sabotage. According to Microsoft, Volt Typhoon is developing capabilities that could "disrupt critical communications infrastructure between the United States and Asia during future crises."[342] CISA has noted that most of Volt Typhoon's identified targets, such as mass transit systems or water treatment facilities, "have no legitimate espionage value."[343] Coker, at the time serving as national cyber director, warned that Volt Typhoon's efforts are designed to "disrupt [the U.S.] military's ability to mobilize," while then-FBI Director Wray stated that the group is preparing to "wreak havoc and cause real-world harm to American citizens and communities if and when China decides the time has come to strike."[344]

Similarly, the 2024 Annual Threat Assessment of the U.S. Intelligence Community indicates that if China perceives an "imminent" conflict with the United States, it might consider launching "aggressive cyber operations against critical U.S. critical infrastructure and military assets . . . [to] deter U.S. military action, . . . impede U.S. decisionmaking, induce societal panic, and interfer[e] with the deployment of U.S. forces."[345] U.S. authorities have also found "software tools left behind

that could be used to destroy infrastructure components," warning that if the United States "go[es] to war with [China], they will try to turn them on."[346] A compromise of critical infrastructure around U.S. military bases—such as power grids or water treatment facilities—could slow U.S. mobilization and buy China enough time to successfully blockade Taiwan. Even a 24-hour delay in the U.S. response could shift the balance in China's favor and secure its control over the island.

The length of time Volt Typhoon has managed to remain covertly embedded within U.S. critical infrastructure is also a serious concern. According to *The Guardian,* intelligence officials estimate that Volt Typhoon has "maintain[ed] access and footholds" in U.S. systems for as long as five years.[347] As early as 2009, U.S. intelligence officials observed China attempting to "map [U.S.] infrastructure," including electrical grids.[348]

About the Authors

Aosheng Pusztaszeri is a research assistant with the Intelligence, National Security, and Technology (INT) Program at CSIS, where he focuses on emerging technologies and their implications for national security. Prior to joining CSIS, Aosheng interned in the U.S. Senate and the U.S. House of Representatives and worked as an undergraduate research assistant in Cornell University's Department of Government. He holds a BA in government and history from Cornell University.

Emily Harding is director of the Intelligence, National Security, and Technology (INT) Program and vice president of the Defense and Security Department at CSIS. As the head of the INT Program, she provides thought leadership on the most critical issues facing intelligence professionals and on the future of intelligence work. She also serves as vice president of the Defense and Security Department, where she is responsible for leading a team of world-renowned scholars providing policy solutions that shape national security. Drawing on her decades of experience in national security, Emily has established herself as an expert on how technology is revolutionizing national security work. Harding has served in a series of high-profile national security positions at critical moments. While serving as deputy staff director on the Senate Select Committee on Intelligence, she led the committee's investigation into Russian interference in the 2016 elections, which was lauded for its bipartisanship. At CIA, she led analysts and analytic programs through moments of crisis, including shepherding the Iraq Group during the attempted Islamic State takeover. During a tour at the National Security Council, she served as director for Iran. After leaving the White House, her team ran the first Office of the Director of National Intelligence-led presidential transition, where she was responsible for briefing the incoming administration. Harding is an adjunct lecturer

at the Johns Hopkins School of Advanced International Studies. Her analysis has appeared in the Wall Street Journal, BBC, NPR, Bloomberg, and other outlets. Harding holds a master's degree from Harvard University's Kennedy School of Government and a bachelor's degree from the University of Virginia.

Julia Dickson is a research associate with the Intelligence, National Security, and Technology (INT) Program at CSIS. Her research interests include cybersecurity and cybercrime and the role of technology in conflict. Prior to joining CSIS, she was awarded a Fulbright grant and spent a year teaching English in Osh, Kyrgyzstan. She was also previously a research assistant at the Wilson Center, an intern for the Conventional Defense Program at the Stimson Center, and a communications and outreach intern at the International Crisis Group. She holds a BA in international studies with a minor in French from the Johns Hopkins University.

Endnotes

1 Amy Chang, Warring State: *China's Cybersecurity Strategy* (Washington, DC: Center for a New American Security, December 2014), https://cryptome.org/2014/12/chinas-cybersecurity-strategy-china-file-14-1205.pdf; and "习近平:把我国从网络大国建设成为网络强国" [Xi Jinping: Build Our Country Into a Cyber Power], Xinhuanet, February 27, 2014, http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm.

2 Chang, *Warring State*; Shannon Tiezzi, "Xi Jinping Leads China's New Internet Security Group," *The Diplomat*, February 28, 2014, https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/; and "Xi Jinping: Build my country," Xinhuanet.

3 Alex Richards, "Evolution of China's Cyber Threat," *Small Wars Journal*, September 23, 2021, https://smallwarsjournal.com/2021/09/23/evolution-chinas-cyber-threat/; and "Chinese Definitions of Information Warfare," Innovative Sicherheits- und Geopolitik [Swiss Institute for Global Affairs], July 5, 2022, https://www.globalaffairs.ch/2022/06/08/chinese-definitions-of-information-warfare/.

4 Ke Hongfa, Zhu Jilu, and Zhao Rong, "Promote the Construction of Core Support Capabilities in Cyberspace," *Guofang Keji* 38, no. 2 (2017): 50–4.

5 Office of the Secretary of Defense (OSD), *Military and Security Developments Involving the People's Republic of China: 2021* (Washington, DC: U.S. Department of Defense, 2021), https://media.defense.gov/2021/nov/03/2002885874/-1/-1/0/2021-cmpr-final.pdf.

6 Ibid.; and 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, https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.

7 Mikk Raud, China and Cyber: *Attitudes, Strategies, Organisation* (Tallinn, Estonia: CCDCOE, 2016), https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf.

8 OSD, *Military and Security Developments*, 2021.

9 Jacqueline Newmyer, "The Revolution in Military Affairs with Chinese Characteristics," *Journal of Strategic Studies* 33, no. 4 (August 2010): 483–504, https://www.tandfonline.com/doi/epdf/10.1080/01402390.2010.489706?needAccess=true.

10 Cate Cadell, "Beyond security crackdown, Beijing charts state-controlled data market," Reuters, July 20, 2021, https://www.reuters.com/technology/beyond-security-crackdown-beijing-charts-state-controlled-data-market-2021-07-20/; Shannon Tiezzi, "China's 'Sovereign Internet'," *The Diplomat*, June 24, 2014, https://thediplomat.com/2014/06/chinas-sovereign-internet/; Daryna Olyniychuk, "New Cyber-Espionage Campaign Detection: Suspected China-Backed Actors Target High-Profile Organizations in Southeast Asia," SOC Prime, December 11, 2024, https://socprime.com/blog/chinese-apt-cyberespionage-southeast-asia-detection/.

11 Chang, *Warring State*.

12 Amy Chang, "China's Maodun: A Free Internet Caged by the Chinese Communist Party," Jamestown Foundation, *China Brief*, vol. 15, no. 8, April 16, 2015, https://jamestown.org/program/chinas-maodun-a-free-internet-caged-by-the-chinese-communist-party/.

13 Dan Harris, "How to Fight Back Against China Corporate Espionage," Harris Sliwoski, October 16, 2024, https://harris-sliwoski.com/chinalawblog/how-to-fight-back-against-china-corporate-espionage/; "Survey of Chinese Espionage in the United States Since 2000," CSIS, March 2023, https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000; and Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques," Microsoft, May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

14 CrowdStrike, *2023 Global Threat Report* (Austin, TX: CrowdStrike, March 3, 2023), https://iitd.com.ua/wp-content/uploads/2023/03/crowdstrike2023globalthreatreport.pdf.

15 Ibid.

16 William R. Evanina, *Hearing Concerning the Comprehensive Threat to America Posed by the Communist Party of China* (CCP), testimony before the Senate Select Committee on Intelligence, 117th Cong., 1st sess. (August 4, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf.

17 "Chinese Hackers Infiltrated Plane, Train and Water Systems for Five Years, US Says," *The Guardian*, February 8, 2024, https://www.theguardian.com/technology/2024/feb/08/chinese-hack-us-transportation-infrastructure.

18 Interview with Australia's Office of National Intelligence (ONI), January 24, 2024; Seth G. Jones et al., *Competing without Fighting: China's Strategy of Political Warfare* (Washington, DC: CSIS, August 2023), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-08/230802_Jones_Competingwithout-Fighting.pdf?VersionId=Zb5B2Le0lf0kk7.QH7E0meA9phGqQEZf; OSD, Military and Security, 2021; and Tarun Chhabra et al., "Global China: Regional Influence and Strategy," Brookings Institution, July 2020, https://www.brookings.edu/articles/global-china-regional-influence-and-strategy/.

19 Jones et al., *Competing without Fighting*; Ben Golliver, "Coronavirus Could Cost NBA $1 Billion, Bring About Record Salary Cap Drop," *Washington Post*, March 21, 2020, https://www.washingtonpost.com/sports/2020/03/21/coronavirus-could-cost-nba-1-billion-bring-about-record-salary-cap-drop/; and Jenna West, "Report: Rockets Lost $20 Million from Sponsorship Deals After Daryl Morey's Tweet," *Sports Illustrated*, November 12, 2019, https://www.si.com/nba/2019/11/12/rockets-lost-revenue-sponsorships-daryl-morey-tweet.

20 Victor Cha, *Examining China's Coercive Economic Tactics*, testimony before the House of Representatives Committee on Rules, 118th Congress, 1st sess. (May 10, 2023), https://www.csis.org/analysis/examining-chinas-coercive-economic-tactics.

21 International Institute for Strategic Studies (IISS), "China" in *Cyber Capabilities and National Power: A Net Assessment* (London: IISS, June 2021), https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---china.pdf.

22 Ibid.

23 Meia Nouwens, "China's New Information Support Force," IISS, May 3, 2024, https://www.iiss.org/online-analysis/online-analysis/2024/05/chinas-new-information-support-force/.

24 Zoe Li, "What We Know About the Chinese Army's Alleged Cyber Spying Unit," CNN World, May 20, 2014, https://www.cnn.com/2014/05/20/world/asia/china-unit-61398/index.html.

25 IISS, "China."

26 "China's national cyberspace security strategy," Digwatch, December 2016, https://dig.watch/resource/chinas-national-cyberspace-security-strategy.

27 Academy of Military Science, *The Science of Military Strategy* (Beijing: Academy of Military Science, 2013), https://nuke.fas.org/guide/china/sms-2013.pdf.

28 OSD, *Military and Security Developments*, 2021.

29 "China's Military Strategy," Ministry of National Defense, People's Republic of China, May 2015, http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html; Lyu Jinghua, "What Are China's Cyber Capabilities and Intentions?," Carnegie Endowment for International Peace, April 1, 2019, https://carnegieendowment.org/posts/2019/04/what-are-chinas-cyber-capabilities-and-intentions?lang=en; and Jones et al., *Competing without Fighting*.

30 "China's Military Strategy," Ministry of National Defense.

31 Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China* (Washington, DC: U.S. Department of Defense, 2020), https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

32 "China's Military Strategy," Ministry of National Defense.

33 OSD, *Military and Security Developments*, 2020; and Mark Pomerleau, "China Moves Toward New 'Intelligentized' Approach to Warfare, Says Pentagon," C4ISRNET, September 1, 2020, https://www.c4isrnet.com/battlefield-tech/2020/09/01/china-moves-toward-new-intelligentized-approach-to-warfare-says-pentagon/.

34 Annette Lee and James Bellacqua, "The Chinese Military's New Information Support Force," CNA, August 2, 2024, https://www.cna.org/our-media/indepth/2024/08/chinese-information-support-force; John Costello, "The Strategic Support Force: Update and Overview," Jamestown Foundation, *China Brief*, vol. 16, no. 19, December 21, 2016, https://jamestown.org/program/strategic-support-force-update-overview/; Adam Kozy, *China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, testimony before the U.S.-China Economic and Security Review Commission, 117th Cong., 2nd sess. (February 17, 2022), https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf; "China's Military Strategy," Ministry of National Defense; and Raud, China and Cyber.

35 "Full Text of China's National Cyberspace Security Strategy // 國家網絡空間安全戰略全文," Red Dragon 1949, December 27, 2017, https://reddragon1949.com/china-cyber-dilemma-in-the-21st-century/full-text-of-chinas-national-cyberspace-security-strategy-%E5%9C%8B%E5%AE%B6%E7%B6%B2%E7%B5%A1%E7%A9%BA%E9%96%93%E5%AE%89%E5%85%A8%E6%88%B0%E7%95%A5%E5%85%A8%E6%96%87/.

36 IISS, "China"; and Grady McGregor, "The World's Largest Surveillance System Is Growing—and So Is the Backlash," *Fortune*, November 3, 2020, https://fortune.com/2020/11/03/china-surveillance-system-backlash-worlds-largest/.

37 IISS, "China."

38 Lyu Jinghua, "What Are China's Cyber Capabilities and Intentions?," *IPI Global Observatory* (blog), March 22, 2019, https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/.

39 McGregor, "The World's Largest Surveillance."

40 CrowdStrike, *2023 Global Threat Report*.

41 Sebastian Moss, "US Charges Chinese Hackers Over 12-Year Campaign to Steal Data from HPE, IBM, NASA and More," Datacenter Dynamics, December 21, 2018, https://www.datacenterdynamics.com/en/news/us-charges-chinese-hackers-over-12-year-campaign-steal-data-hpe-ibm-nasa-and-more/; and Eric Rosenbach, *China: Challenges for U.S. Commerce*, testimony before the Senate Committee on Commerce, Science, and Transportation, 116th Cong., 1st sess. (March 7, 2019), https://www.govinfo.gov/content/pkg/CHRG-116shrg52567/pdf/CHRG-116shrg52567.pdf.

42 IISS, "China."

43 Dakota Cary and Kristin Del Rosso, *Sleight of Hand: How China Weaponizes Software Vulnerabilities* (Washington, DC: Atlantic Council, September 2023), https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/; and "Section 2: China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States," in *2022 Annual Report to Congress*, United States-China Economic and Security Review Commission (USCC), November 15, 2022, https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf.

44 "Section 2: China's Cyber Capabilities," USCC; Ellen Nakashima, "Security Firm Finds Link Between China and Anthem Hack," *Washington Post*, February 27, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/; Catalin Cimpanu, "Chinese Universities Connected to Known APTs Are Conducting AI/ML Cybersecurity Research," *The Record*, March 10, 2021, https://therecord.media/chinese-universities-connected-to-known-apts-are-conducting-ai-ml-cybersecurity-research; and "The Anthem Hack: All Roads Lead to China," ThreatConnect, February 27, 2015, https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/.

45 Rush Doshi et al., *China as a "Cyber Great Power": Beijing's Two Voices in Telecommunications* (Washington, DC: Brookings Institution, April 2021), https://www.brookings.edu/articles/china-as-a-cyber-great-power-beijings-two-voices-in-telecommunications/; and Chang, "China's Maodun."

46 Doshi et al., *China as a "Cyber Great Power."*

47 "China's Military Strategy (2015)," Ministry of National Defense, 27; and Raud, *China and Cyber*.

48 Jinghua, "What Are China's Cyber Capabilities?"

49 Ibid.

50 Hui Li and Xin Yang, "Interpretation of Network Sovereignty," in *Co-governed Sovereignty Network: Legal Basis and Its Prototype & Applications with MIN Architecture* (Singapore: Springer, July 27, 2021), 29–60, https://doi.org/10.1007/978-981-16-2670-8_2; and "Chinese Military Information Warfare Attacks on Mind and Spirit // 中國軍隊信息戰隊思想和精神的攻擊," Red Dragon 1949, September 2018, https://reddragon1949.com/2018/09/.

51 Interview with Australia's Office of National Intelligence (ONI), January 24, 2024.

52 Ibid.

53 Interview with the Australian Cyber Security Centre (ACSC), January 25, 2024.

54 Ibid.

55 Ke, Zhu, and Zhao, "Promote the Construction."

56 Ibid.

57 "An Introduction to Foreign Malign Influence," Office of the Director of National Intelligence (ODNI), *FMI Primer*, vol. 1, April 2024, https://www.dni.gov/files/FMIC/documents/products/04-25-24_Report_FMI-Primer-Public-Release.pdf.

58 Ibid.

59 Ibid.

60 Graphika, *The #Americans: Chinese State-Linked Influence Operation Spamouflage Masquerades as U.S. Voters to Push Divisive Online Narratives Ahead of 2024 Election* (New York: Graphika, September 2024), https://22006778.fs1.hubspotusercontent-na1.net/hubfs/22006778/graphika-report-the-americans.pdf?utm_campaign=Report%20Demand%20Gen&utm_medium=email&_hsenc=p2ANqtz-9AEt-l519sr-toVzNUm53nGIghGgUCkalkdju1Z6814M4GgK_H0RVfzGz7CRkvwhEgG6SFQi3X1bNw0AAbhJsAUNV-b08A&_hsmi=323992254&utm_content=323992254&utm_source=hs_automation.

61 "An Introduction to Foreign Malign Influence," ODNI.

62 OSD, *Military and Security Developments*, 2021.

63 John C. Demers, *China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses*, testimony before the Senate Committee on the Judiciary, 115th Cong., 2nd sess. (December 12, 2018), https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2018/12/18/12-05-2018_john_c._demers_testimony_re_china_non-traditional_espionage_against_the_united_states_the_threat_and_potential_policy_responses.pdf.

64 Chang, *Warring State*; and Scott Pelley, "FBI Director on Threat of ISIS, Cybercrime," CBS News, October 5, 2014, https://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/.

65 U.S.-China Economic and Security Review Commission (USCC), "Section 4: Commercial Cyber Espionage and Barriers to Digital Trade in China," in *2015 Annual Report to Congress* (Washington, DC: USCC, April 7, 2015), https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%201%2C%20Section%204%20-%20Commercial%20Cyber%20Espionage%20and%20Barriers%20to%20Digital%20Trade%20in%20China.pdf.

66 Evanina, *Hearing Concerning the Comprehensive Threat to America*.

67 Eric Geller, "Chinese Nationals Charged for Anthem Hack, 'One of the Worst Data Breaches in History,'" *Politico*, May 9, 2019, https://www.politico.com/story/2019/05/09/chinese-hackers-anthem-data-breach-1421341; California Department of Insurance, "Anthem Data Breach. and United States of America v. Fujie Wang a/k/a "Dennis Wang" and John Doe a/k/a "Deniel Jack," a/k/a "Kim Young," a/k/a "Zhou Zhihong," 1:19-cr-00153-JRS-MJD (U.S. District Court, Southern District of Indiana, Indianapolis Division, May 7, 2019), https://www.justice.gov/opa/press-release/file/1161466/dl?inline=.

68 Jones et al., *Competing without Fighting; Dina Temple-Raston*, "China's Microsoft Hack May Have Had a Bigger Purpose Than Just Spying," All Things Considered, NPR, August 26, 2021, https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying; and Taylor Telford and Craig Timberg, "Marriott Discloses Massive Data Breach Affecting up to 500 Million Guests," Washington Post, November 30, 2018, https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/.

69 Seth G. Jones, Joseph S. Bermudez Jr., Danika Newlee , and Nicholas Harrington, "Iran's Threat to Saudi Critical Infrastructure: The Implications of U.S.-Iranian Escalation," CSIS, *CSIS Brief,* August 5, 2019, https://www.csis.org/analysis/irans-threat-saudi-critical-infrastructure-implications-us-iranian-escalation; Zhanna L. Malekos Smith, "A Power Struggle over Ukraine's Electrical Grid," CSIS, *Commentary*, March 9, 2022, https://www.csis.org/analysis/power-struggle-over-ukraines-electrical-grid; and Christian Vasquez and AJ Vicens, "Russian hackers disrupted Ukrainian electrical grid last year," CyberScoop, November 9, 2023, https://cyberscoop.com/sandworm-russia-ukraine-grid/.

70 Chinese Hackers Infiltrated Plane, Train," *The Guardian*.

71 Interview with the Australian National University's National Security College, January 25, 2024.

72 Interview with ACSC, January 25, 2024.

73 "Cyber and Information Operations," International Committee of the Red Cross, n.d., https://www.icrc.org/en/law-and-policy/cyber-and-information-operations; "Introduction to the Law of Armed Conflict," University of North Carolina School of Law, n.d., https://guides.lib.unc.edu/militarylaw/armedconflict; and Patryk Pawlak and Aude Géry, "Why the World Needs a New Cyber Treaty for Critical Infrastructure," Carnegie Endowment for International Peace, March 28, 2024, https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en&center=europe.

74 Interview with ACSC, January 25, 2024.

75 Australian Signals Directorate (ASD), *ASD Cyber Threat Report*, 2022–2023 (Canberra, Australia: ASD, 2023), https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf.

76 "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Cybersecurity and Infrastructure Security Agency (CISA), July 21, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a.

77 Christian Vasquez and Blake Sobczak, "China Hacking Threat Prompts Rare U.S. Pipeline Warning," E&E News, July 21, 2021, https://www.eenews.net/articles/china-hacking-threat-prompts-rare-u-s-pipeline-warning/; and "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Joint Cybersecurity Advisory, CISA, July 20, 2021, https://www.cisa.gov/sites/default/files/publications/AA21-201A_Chinese_Gas_Pipeline_Intrusion_Campaign_2011_to_2013%20(1).pdf.

78 Vasquez and Sobczak, "China Hacking Threat."

79 Ibid.

80 ODNI, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: ODNI, February 2024), https://www.intelligence.senate.gov/sites/default/files/hearings/unclassified_2024_ata_report_0.pdf; Sergiu Gatlan, "CISA: Vendors Must Secure SOHO Routers Against Volt Typhoon Attacks," Bleeping Computer, January 31, 2024, https://www.bleepingcomputer.com/news/security/cisa-vendors-must-secure-soho-routers-against-volt-typhoon-attacks/; and "Chinese Hackers Infiltrated Plane, Train," *The Guardian*.

81 Vasquez and Sobczak, "China Hacking Threat."

82 David Southwell, "Chinese power play: The astonishing number of Australian energy assets totally owned by China—as Aussies are forced to pay high prices and experts warn Beijing can 'turn out the lights'," *Daily Mail*, June 5, 2023, https://www.dailymail.co.uk/news/article-12113647/Chinese-ownership-Australian-energy-assets-Aussies-pay-high-power-prices-China-profits.html.

83 Interview with U.S. embassy in Canberra, January 25, 2024.

84 Khalil Al-Anani, "Egypt's Strategic Partnership with China: Opportunities and Implications," Arab Center Washington DC, January 27, 2023, https://arabcenterdc.org/resource/egypts-strategic-partnership-with-china-opportunities-and-implications/; Tamer El-Ghobashy and Esther Fung, "Soft Power: China Backs Egypt's New $45 Billion Capital," *Wall Street Journal*, May 3, 2016, https://www.wsj.com/articles/big-chinese-developer-pushes-overseas-ambitions-with-egypt-project-1462267802; and Devianti Faridz, "China Emerging as One of the Key Foreign Investors in Indonesia's New Capital City," VOA News, March 4, 2021, https://www.voanews.com/a/china-emerging-as-one-of-the-key-foreign-investors-in-indonesia-s-new-capital-city/7514058.html.

85 ODNI, *Annual Threat Assessment*, 2024.

86 ASD, ASD Cyber Threat Report.

87 Dorothy Denning and the Conversation US, "How the Chinese Cyberthreat Has Evolved," *Scientific American*, October 7, 2017, https://www.scientificamerican.com/article/how-the-chinese-cyberthreat-has-evolved/. Patriotic hackers were a relatively new phenomenon for China, emerging on the scene the year before in response to violence against ethnic Chinese in Indonesia, and they continued something resembling vigilante justice against perceived slights to China.

88 Kevin Collier, "Taiwanese Websites Hit with DDoS Attacks as Pelosi Begins Visit," NBC News, August 2, 2022, https://www.nbcnews.com/tech/security/taiwanese-websites-hit-ddos-attacks-pelosi-begins-visit-rcna41144; Sarah Wu and Eduardo Baptista, "From 7-11s to Train Stations, Cyber Attacks Plague Taiwan over Pelosi Visit," Reuters, August 4, 2022, https://www.reuters.com/technology/7-11s-train-stations-cyber-attacks-plague-taiwan-over-pelosi-visit-2022-08-04/; and CrowdStrike, *2023 Global Threat Report*.

89 U.S. Department of the Treasury, "Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure," press release, March 25, 2024, https://home.treasury.gov/news/press-releases/jy2205; and Mandiant, *APT1: Exposing One of China's Cyber Espionage Unit*s (Reston, VA: Mandiant, October 25, 2004), https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf.

90 Alex Joske, "State Security Departments: The Birth of China's Nationwide State Security System," *Deserepi: Studies in Chinese Communist Party External Work* (2023), https://deserepi.org/0/joske_ssd.pdf; and Alex Joske, "China's State Security Departments and Nationwide System," interview by Mercy A. Kuo, The Diplomat, November 9, 2023, https://thediplomat.com/2023/11/chinas-state-security-departments-and-nationwide-system/.

91 Joske, "State Security Departments"; and Joske, interview.

92 AJ Vicens, "Feds: Chinese Hacking Operations Have Been in Critical Infrastructure Networks for Five Years," CyberScoop, February 7, 2024, https://cyberscoop.com/feds-chinese-hacking-operations-have-been-in-critical-infrastructure-networks-for-five-years/.

93 Denning and the Conversation US, "How the Chinese Cyberthreat."

94 "APT41 Compromised Six U.S. State Government Networks," FortiGuard Labs, n.d., https://www.fortiguard.com/threat-signal-report/4449/apt41-compromised-six-u-s-state-government-networks; and Rufus Brown et al., "Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments," Google Cloud, March 8, 2022, https://cloud.google.com/blog/topics/threat-intelligence/apt41-us-state-governments/.

95 Interview with ACSC, January 25, 2024.

96 Ibid.

97 Ibid.

98 Lyu, "What Are China's Cyber Capabilities?"; and IISS, "China."

99 Lyu, "What Are China's Cyber Capabilities?"; and IISS, "China."

100 Pradyot Mallick, "Transforming the PLA: A Decade of Reorganisation from SSF to ISF," Strategic Study India, 2024, https://www.academia.edu/123531977/Transforming_the_PLA_A_Decade_of_reorganisation_from_SSF_to_ISF.

101 Interview with ACSC, January 25, 2024.

102 OSD, *Military and Security Developments*, 2021.

103 Richards, "Evolution of China's."

104 Ying Yu Lin and Tzu-Hao Liao, "RIP, SSF: Unpacking the PLA's Latest Restructuring," *The Diplomat*, April 23, 2024, https://thediplomat.com/2024/04/rip-ssf-unpacking-the-plas-latest-restructuring/; and Tenzin Younten, "China's Latest Military Reorganization Terminates the PLA SSF & launches Three New Arm Forces Based on It: Strategic Implications of the PLA's Latest Reforms and Structural Changes," Usanas Foundation, April 26, 2024, https://usanasfoundation.com/chinas-latest-military-reorganization-terminates-the-pla-ssf-launches-three-new-arm-forces-based-on-it-strategic-implications-of-the-plas-latest-reforms-and-structural-changes.

105 Lin and Liao, "RIP, SSF"; and Younten, "China's Latest Military Reorganization."

106 Nouwens, "China's New Information."

107 Lin and Liao, "RIP, SSF"; Younten, "China's Latest Military Reorganization"; and Nouwens, "China's New Information."

108 Younten, "China's Latest Military Reorganization"; and Lin and Liao, "RIP, SSF."

109 Lin and Liao, "RIP, SSF"; and Younten, "China's Latest Military Reorganization."

110 Nouwens, "China's New Information."

111 Younten, "China's Latest Military Reorganization"; Lin and Liao, "RIP, SSF"; Nouwens, "China's New Information"; Wang Xinjuan ed., "Information Support Force: A Brand-New Strategic Arm of the PLA," Ministry of National Defense of the People's Republic of China, April 19, 2024, http://eng.mod.gov.cn/xb/News_213114/TopStories/16302051.html; and Matt Bruzzese and Peter W. Singer, "Farewell to China's Strategic Support Force. Let's Meet Its Replacements," *Defense One*, April 28, 2024, https://www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143/.

112 Nouwens, "China's New Information."

113 Younten, "China's Latest Military Reorganization."

114 Lin and Liao, "RIP, SSF"; and Younten, "China's Latest Military Reorganization."

115 Lin and Liao, "RIP, SSF."

116 Ibid.; and Younten, "China's Latest Military Reorganization."

117 Nouwens, "China's New Information."

118 Younten, "China's Latest Military Reorganization"; and Lin and Liao, "RIP, SSF."

119 Lin and Liao, "RIP, SSF."

120 Nouwens, "China's New Information."

121 Ibid.; and Lin and Liao, "RIP, SSF."

122 Mandiant, *APT1*; USCC, "Section 2: China's Cyber Capabilities"; and Office of Public Affairs, 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," press release, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

123 "The Role of PLA Base 311 in Political Warfare Against Taiwan (Part 3)," Global Taiwan Institute, *Global Taiwan Brief*, vol. 2, no. 7, February 15, 2017, https://globaltaiwan.org/2017/02/the-role-of-pla-base-311-in-political-warfare-against-taiwan-part-3/; and Coline Chavane and TDR team, *A Three-Beat Waltz: The Ecosystem Behind Chinese State-Sponsored Cyber Threats* (Rennes, France: Sekoia, November 2024), https://t7f4e9n3.rocketcdn.me/wp-content/uploads/2024/11/A-three-beat-waltz-The-ecosystem-behind-Chinese-state-sponsored-cyber-threats.pdf.

124 "PLA Eastern Theater Command Army SIGINT Operations Targeting Taiwan," *Taiwan Link*, August 8, 2016, https://thetaiwanlink.blogspot.com/2016/08/pla-eastern-theater-command-army-sigint.html; and Chavane and TDR team, *A Three-Beat Waltz*.

125 Mandiant, *APT1*; USCC, "Section 2: China's Cyber Capabilities."; "Comment Crew, APT 1," Electronic Transactions Development Agency, n.d., https://apt.etda.or.th/cgi-bin/showcard.cgi?u=b99367ed-e483-40a3-98d0-8d3a2102a4ab. and "APT Group: Putter Panda, APT 2," Electronic Transactions Development Agency, n.d., https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Putter%20Panda%2C%20APT%202.

126 Mandiant, *APT1*.

127 Ibid.

128 Ibid.

129 Mandiant, APT1 and CrowdStrike, *CrowdStrike Intelligence Report: Putter Panda* (Austin, TX: CrowdStrike, n.d.) https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf.

130 J. Michael Dahm, "A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force," Jamestown Foundation, *China Brief*, vol. 24, no. 9, April 26, 2024, https://jamestown.org/program/a-disturbance-in-the-force-the-reorganization-of-peoples-liberation-army-command-and-elimination-of-chinas-strategic-support-force/; and Younten, "China's Latest Military Reorganization."

131 Nouwens, "China's New Information"; and Younten, "China's Latest Military Reorganization."

132 Chavane and TDR team, *A Three-Beat Waltz*.

133 Tom Uren, "The PLA's Cyber Operations Go Dark," Lawfare, November 22, 2024, https://www.lawfaremedia.org/article/the-pla's-cyber-operations-go-dark.

134 Chavane and TDR team, *A Three-Beat Waltz*; and Uren, "The PLA's Cyber Operations."

135 Chavane and TDR team, *A Three-Beat Waltz*.

136 "APT Group: Comment Crew," Electronic Transactions Development Agency; Mandiant, *APT1*; and USCC, "Section 2: China's Cyber Capabilities."

137 Mandiant, *APT1*.

138 Tom Uren and Patrick Gray, host, *Srsly Risky Biz*, podcast, "The PLA's Cyber Operations Go Dark," November 20, 2024, https://risky.biz/SRB102/; and Mandiant, *APT1*.

139 U.S. Cyber Command Public Affairs, "CYBER 101 - Cyber Mission Force," U.S. Cyber Command, November 1, 2022, https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/.

140 Joey Cheng, "Cyber Conflict Escalates: Second Chinese PLA Hacking Group Accused," *Defense One*, June 10, 2014, https://www.defenseone.com/defense-systems/2014/06/cyber-conflict-escalates-second-chinese-pla-hacking-group-accused/193841/; Mandiant, APT1; and Aliya Sternstein, "The PLA, China Telecom and Huawei Golden Triangle," NextGov, February 21, 2013, https://www.nextgov.com/cybersecurity/2013/02/pla-china-telecom-and-huawei-golden-triangle/61428/.

141 Mandiant, *APT1*; and USCC, "Section 2: China's Cyber Capabilities."

142 USCC, "Section 2: China's Cyber Capabilities"; Mandiant, APT1; Tsung-Han Wu and Chia-Ling Hung, eds., "Chapter 8: Cyber Warfare Capabilities of the PLA Strategic Support Force (SSF)," in *2021 Report on the Defense Technology Trend Assessment –Assessment of the NewGeneration of Chinese Communist Party's Military Technology* (Taipei: Institute for National Defense and Security Research, June 2022), https://indsr.org.tw/uploads/enindsr/files/202206/64b998f3-d906-46a4-b78e-08c06eb28c3e.pdf; and Mandiant, *APT1*.

143 Mandiant, *APT1*.

144 Ibid.

145 Ibid.

146 USCC, "Section 2: China's Cyber Capabilities."

147 Ibid.; and U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers."

148 USCC, "Section 2: China's Cyber Capabilities"; and Mandiant, *APT1*.

149 "APT Group: Putter Panda," Electronic Transactions Development Agency.

150 USCC, "Section 2: China's Cyber Capabilities."

151 Cheng, "Cyber Conflict Escalates"; USCC, "Section 2: China's Cyber Capabilities"; and Wu and Hung, "Chapter 8: Cyber Warfare Capabilities."

152 Cheng, "Cyber Conflict Escalates"; and Dahm, "A Disturbance in the Force."

153 CrowdStrike, "CrowdStrike Intelligence Report."

154 "APT12," MITRE/ATT&CK, n.d., https://attack.mitre.org/groups/G0005/; and USCC, "Section 2: China's Cyber Capabilities."

155 Cheng, "Cyber Conflict Escalates."

156 Jr Ng, "China Broadens Cyber Options," *Asian Military Review*, January 15, 2020, https://www.asianmilitaryreview.com/2020/01/china-broadens-cyber-options/; Jones et al., *Competing without Fighting*; James Marinero, "Careers: The Chinese Foreign Intelligence Organisation," Vocal.Media, 2023, https://vocal.media/journal/careers-the-chinese-foreign-intelligence-organisation; Joe Leahy, "China's Feared Spy Agency Steps Out of the Shadows," *Financial Times*, January 23, 2024, https://www.ft.com/content/f78c7243-2ff5-4f77-93d0-91c20f6b5548; and Nectar Gan, "China Sees Foreign Threats 'Everywhere' as Powerful Spy Agency Takes Center Stage," CNN, April 21, 2024, https://www.cnn.com/2024/04/21/china/china-spy-agency-public-profile-intl-hnk/index.html.

157 Marinero, "Careers: The Chinese Foreign"; Leahy, "China's Feared Spy Agency"; and Gan, "China Sees Foreign Threats."

158 Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *Washington Post*, June 8, 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.

159 Ibid.

160 "Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity," CISA, October 24, 2020, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-258a.

161 Ibid.

162 B. K. Williams, "Evaluating China's Road to Cyber Super Power," Lawrence Livermore National Laboratory, November 15, 2021, https://www.osti.gov/servlets/purl/1830481.

163 U.S. Department of the Treasury, "Treasury Sanctions China-Linked Hackers."

164 "APT40 Is Run by the Hainan Department of the Chinese Ministry of State Security," Instrusion Truth, January 16, 2020, https://intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/.

165 Joske, interview.; Marinero, "Careers: The Chinese Foreign"; Leahy, "China's Feared Spy Agency"; and "Ministry of State Security Headquarters," Intelligence Resource Program, Federation of American Scientists, n.d., https://irp.fas.org/world/china/facilities/xiyuan.htm.

166 Joske, interview.

167 Joske, "State Security Departments."

168 Joske, interview.

169 "APT Group: Flax Typhoon," Electronic Transactions Development Agency, October 23, 2024, https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Flax%20Typhoon; Joske, "State Security Departments"; Insikt Group, "Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation," Recorded Future, June 24, 2024, https://go.recordedfuture.com/hubfs/reports/cta-cn-2024-0624.pdf; and "Recorded Future Exposes RedJuliett Cyber-Espionage Campaign, Targeting Taiwan and Expanding Globally," Industrial Cyber, June 27, 2024, https://industrialcyber.co/ransomware/recorded-future-exposes-redjuliett-cyber-espionage-campaign-targeting-taiwan-and-expanding-globally/.

170 Joske, "State Security Departments"; and Joske, interview.

171 Joske, interview.

172 Joske, "State Security Departments."

173 FireEye iSIGHT Intelligence, "APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat," Google Cloud, April 6, 2017, https://cloud.google.com/blog/topics/threat-intelligence/apt10-menupass-group/.

174 USCC, "Section 2: China's Cyber Capabilities."

175 Ibid.

176 FireEye iSIGHT Intelligence, "APT10 (MenuPass Group)."

177 Edward Millington and Michael Cox, "menuPass," MITRE ATT&CK, May 31, 2017, https://attack.mitre.org/groups/G0045/; and United States of America v. Zhu Hua, a/k/a "Afwar," a/k/a "CVNX," a/k/a "Alayos," a/k/a "Godkiller," and Zhang Shilong, a/k/a "Baobeilong," a/k/a "Zhang Jianguo," a/k/a "Atreexp," 18

CRIM 891 (United States District Court Southern District of New York, December 17, 2018), https://www.justice.gov/opa/page/file/1122671/dl.

178 Jack Stubbs, Joseph Menn, and Christopher Bing, "Inside the West's failed fight against China's 'Cloud Hopper' hackers," *Reuters*, June 26, 2019. https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/. and 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," Press Release, December 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

179 Moss, "US Charges Chinese Hackers."

180 Dominik Breitenbacher, "Unmasking MirrorFace: Operation LiberalFace Targeting Japanese Political Entities," Welivesecurity, December 14, 2022, https://www.welivesecurity.com/2022/12/14/unmasking-mirrorface-operation-liberalface-targeting-japanese-political-entities/; and "APT Group: Operation LiberalFace, MirrorFace," Electronic Transactions Development Agency, December 27, 2022, https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Operation%20LiberalFace%2C%20MirrorFace.

181 "Deep Panda," Council on Foreign Relations, n.d., https://www.cfr.org/cyber-operations/deep-panda; and "APT group: APT 19, Deep Panda, C0d0so0," Electronic Transactions Development Agency (ETDA), March 10, 2024. https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2019%2C%20Deep%20Panda%2C%20C0d0so0.

182 "APT Group: APT 19," Electronic Transactions Development Agency; "FBI Liaison Alert System #A-000049-MW," Krebs on Security, n.d., https://krebsonsecurity.com/wp-content/uploads/2015/02/FBI-Flash-Warning-Deep-Panda.pdf; Jeremy Wagstaff, "Hunt for Deep Panda Intensifies in Trenches of U.S.-China Cyberwar," Reuters, June 20, 2015, https://www.reuters.com/article/technology/hunt-for-deep-panda-intensifies-in-trenches-of-us-china-cyberwar-idUSKBN0P1023/; and Nakashima, "Security Firm Finds Link."

183 Nakashima, "Security Firm Finds Link"; Catalin Cimpanu, "Chinese Universities Connected to Known APTs Are Conducting AI/ML Cybersecurity Research," *The Record*, March 10, 2021, https://therecord.media/chinese-universities-connected-to-known-apts-are-conducting-ai-ml-cybersecurity-research; and "The Anthem Hack: All Roads," ThreatConnect.

184 Nakashima, "Security Firm Finds Link."

185 Kelli Young, "Cyber Case Study: Anthem Data Breach," Coverlink Insurance, September 27, 2021, https://coverlink.com/case-study/anthem-data-breach/; and California Department of Insurance, "Anthem Data Breach," n.d., https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm.

186 Nakashima, "Security Firm Finds Link"; Cimpanu, "Chinese Universities Connected"; and "The Anthem Hack: All Roads," ThreatConnect.

187 "Did the Chinese Government Hack Anthem?," Healthcare Finance News, March 3, 2015, https://www.healthcarefinancenews.com/news/did-chinese-government-hack-anthem.

188 James Andrew Lewis, "The New Executive Order on Personal Data," CSIS, *Commentary*, March 6, 2024, https://www.csis.org/analysis/new-executive-order-personal-data; Brian Naylor, "OPM: 21.5 Million Social Security Numbers Stolen From Government Computers," NPR, July 9, 2015, https://www.npr.org/sections/thetwo-way/2015/07/09/421502905/opm-21-5-million-social-security-numbers-stolen-from-government-computers; Khandelwal, "United Airlines Hacked"; "22 Million Affected by OPM Hack, Officials Say," ABC News, July 9, 2015, https://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731; California Department of Insurance, "Anthem Data Breach"; and "Deep Panda," Council on Foreign Relations.

189 Khandelwal, "United Airlines Hacked"; "22 Million Affected by OPM Hack," ABC News; California Department of Insurance, "Anthem Data Breach"; and "Deep Panda," Council on Foreign Relations.

190 Thomas Brewster, "Forbes.com Hacked in November, Possibly By Chinese Cyber Spies," Forbes, February 10, 2015, https://www.forbes.com/sites/thomasbrewster/2015/02/10/forbes-com-hacked-in-november-possibly-by-chinese-cyber-spies/.

191 Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure"; and "Chinese Hackers Infiltrated Plane, Train," *The Guardian*.

192 Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure"; and "Chinese Hackers Infiltrated Plane, Train," *The Guardian*.

193 "APT Group: Volt Typhoon," Electronic Transactions Development Agency, December 28, 2024, https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Volt%20Typhoon; and Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure."

194 Dominique Mendez, "Volt Typhoon Takedown: FBI Successfully Combats Chinese Cyberattacks on Critical Infrastructure, but Cyber Warfare Is Far from Over," University of Maryland Center for Health and Homeland Security (CHHS), March 20, 2024, https://www.mdchhs.com/2024/03/20/volt-typhoon-takedown-fbi-successfully-combats-chinese-cyberattacks-on-critical-infrastructure-but-cyber-warfare-is-far-from-over/.

195 Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure."

196 "Chinese Hackers Infiltrated Plane, Train," *The Guardian*.

197 Helen Davidson and Agencies, "Explainer: What Is Volt Typhoon and Why Is it the 'Defining Threat of Our Generation?'," *The Guardian*, February 13, 2024, https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer.

198 Vicens, "Feds: Chinese Hacking Operations Have Been in Critical Infrastructure"; Paul Rosenzweig, "Volt Typhoon and the Disruption of the U.S. Cyber Strategy," Lawfare, March 5, 2024, https://www.lawfaremedia.org/article/volt-typhoon-and-the-disruption-of-the-u.s.-cyber-strategy; and "Joint Cybersecurity Advisory," CISA, February 7, 2024, https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf.

199 "Business as Usual: Falcon Complete MDR Thwarts Novel VANGUARD PANDA (Volt Typhoon) Tradecraft," CrowdStrike, June 22, 2023, https://www.crowdstrike.com/en-us/blog/falcon-complete-thwarts-vanguard-panda-tradecraft/; Bart Lenaerts-Bergmans, "What Are Living off the Land (LOTL) Attacks?," CrowdStrike, February 22, 2023, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/living-off-the-land-attack/; and Davidson and Agencies, "Explainer: What is Volt Typhoon?"

200 "Business as Usual," CrowdStrike; Lenaerts-Bergman, "What Are Living off the Land?"; and Davidson and Agencies, "Explainer: What Is Volt Typhoon?"

201 Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure"; and Office of Public Affairs, U.S. Department of Justice, "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure," press release, January 31, 2024, https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical.

202 Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure."

203 "Cybersecurity, Volt Typhoon, and the Grid," Architecture Technology Corporation, n.d., https://www.atcorp.com/products/cyrin/newsletter/cybersecurity-volt-typhoon-and-the-grid/.

204 Ravie Lakshmanan, "After FBI Takedown, KV-Botnet Operators Shift Tactics in Attempt to Bounce Back," Hacker News, February 7, 2024, https://thehackernews.com/2024/02/after-fbi-takedown-kv-botnet-operators.html; Vicens, "Feds: Chinese Hacking Operations Have Been in Critical Infrastructure"; and Office of Public Affairs, U.S. Department of Justice, "U.S. Government Disrupts Botnet."

205 Office of Public Affairs, U.S. Department of Justice, "U.S. Government Disrupts Botnet."

206 Gatlan, "CISA: Vendors Must Secure"; and "Chinese Hackers Infiltrated Plane, Train," *The Guardian*.

207 "Chinese Hackers Infiltrated Plane, Train," *The Guardian*.

208 "APT Group: Leviathan, APT 40, TEMP.Periscope," Electronic Transactions Development Agency, August 26, 2024, https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Leviathan%2C%20APT%2040%2C%20TEMP%2EPeriscope&n=1; and "APT40 Is Run by the Hainan Department.

209 USCC, "Section 2: China's Cyber Capabilities."

210 Ibid.; and Office of Public Affairs, 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," press release, July 19, 2021, https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

211 Office of Public Affairs, U.S. Department of Justice, "Four Chinese Nationals"; USCC, "Section 2: China's Cyber Capabilities"; and Volz, "Chinese Hackers Target Universities."

212 USCC, "Section 2: China's Cyber Capabilities"; and "Potential for China Cyber Response to Heightened U.S.–China Tensions," CISA, October 20, 2020, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-275a.

213 USCC, "Section 2: China's Cyber Capabilities"; and "APT Group: Leviathan," Electronic Transactions Development Agency.

214 Office of Public Affairs, U.S. Department of Justice, "Four Chinese Nationals."

215 Catalin Cimpanu, "US Indicts Four Members of Chinese Hacking Group APT40," *The Record*, July 18, 2021, https://therecord.media/us-indicts-four-members-of-chinese-hacking-group-apt40; Martin Matishak, "White House Formally Blames China's Ministry of State Security for Microsoft Exchange Hack," *The Record*, July 18, 2021, https://therecord.media/white-house-formally-blames-chinas-ministry-of-state-security-for-microsoft-exchange-hack; USCC, "Section 2: China's Cyber Capabilities"; and Gareth Corfield, "UK and Chums Call Out Chinese Ministry of State Security for Hafnium Microsoft Exchange Server Attacks," *The Register*, July 19, 2021, https://www.theregister.com/2021/07/19/hafnium_china_state_security/.

216 Corfield, "UK and Chums Call Out"; Cimpanu, "US Indicts Four Members"; USCC, "Section 2: China's Cyber Capabilities"; and Matishak, "White House Formally Blames China's Ministry."

217 Axel F. and Pierre T., "Leviathan: Espionage Actor Spearphishes Maritime and Defense Targets," Proofpoint, October 16, 2017, https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets; and USCC, "Section 2: China's Cyber Capabilities."

218 Volz, "Chinese Hackers Target Universities"; Axel F. and Pierre T., "Leviathan: Espionage Actor Spearphishes"; and "APT Group: Leviathan," Electronic Transactions Development Agency.

219 Office of Public Affairs, U.S. Department of Justice, "Four Chinese Nationals."

220 Ibid.

221 Ibid.

223 "APT Group: APT 41," Electronic Transactions Development Agency, December 27, 2024, https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2041; "HC3: Threat Profile," Office of Information Security; U.S. Department of Health and Human Services, August 16, 2023, https://www.hhs.gov/sites/default/files/china-based-threat-actor-profiles-tlpclear.pdf; United States of America v. Jiang Lizhi, Qian Chuan, and Fu Qiang, case: 1:20-cr-00158 (U.S. District Court for the District of Columbia, May 7, 2019), https://www.justice.gov/opa/press-release/file/1317206/dl; and Natto Team, "i-SOON: Another Company in the APT41 Network," Natto Thoughts (blog), October 26, 2023, https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41.

224 "Threat Signal Report: APT41 Compromised Six U.S. State Government Networks," FortiGuard Labs, March 10, 2022, https://www.fortiguard.com/threat-signal-report/4449/apt41-compromised-six-u-s-state-government-networks; and USCC, "Section 2: China's Cyber Capabilities."

225 Office of Public Affairs, 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," press release, September 16, 2020, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer; Chris Jaikaran, *Cybersecurity: Selected Cyberattacks, 2012-2024*, CRS Report No. R46974 (Washington, DC: Congressional Research Service, January 8, 2025), https://crsreports.congress.gov/product/pdf/R/R46974; and USCC, "Section 2: China's Cyber Capabilities."

226 USCC, "Section 2: China's Cyber Capabilities."

227 Sarah Fitzpatrick and Kit Ramgopal, "Hackers Linked to Chinese Government Stole Millions in Covid Benefits, Secret Service Says," NBC News, December 5, 2022. https://www.nbcnews.com/tech/security/chinese-hackers-covid-fraud-millions-rcna59636.

228 "APT Group: APT 41," Electronic Transactions Development Agency.

229 "Threat Signal Report: APT41 Compromised," FortiGuard Labs; Brown et al., "Does This Look Infected?"; and "APT Group: APT 41," Electronic Transactions Development Agency.

230 Fitzpatrick and Ramgopal, "Hackers Linked to Chinese Government Stole Millions."

231 "APT Group: APT 31, Judgment Panda, Zirconium," Electronic Transactions Development Agency, August 27, 2024, https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2031%2C%20Judgment%20Panda%2C%20Zirconium; U.S. Department of the Treasury, "Treasury Sanctions China-Linked Hackers for Targeting"; AJ Vicens and Derek B. Johnson, "US and UK Accuse China of Cyber Operations Targeting Domestic Politics," CyberScoop, March 25, 2024, https://cyberscoop.com/china-indictments-apt31-surveillance/; and "APT Group: APT 31," Electronic Transactions Development Agency.

232 "APT Group: APT 31," Electronic Transactions Development Agency; U.S. Department of the Treasury, "Treasury Sanctions China-Linked Hackers for Targeting"; and Vicens and Johnson, "US and UK Accuse China of Cyber Operations."

233 Rewards for Justice, "APT31/Wuhan Xiaoruizhi Science & Technology Company, Ltd.," U.S. Department of State, n.d., https://rewardsforjustice.net/rewards/apt31-wuhan-xiaoruizhi-science-technology-company-ltd/; Vicens and Johnson, "US and UK Accuse China of Cyber Operations"; and James Pomfret and Yew Lun Tian, "APT31: the Chinese Hacking Group Behind Global Cyberespionage Campaign," Reuters, March 26, 2024, https://www.reuters.com/technology/cybersecurity/apt31-chinese-hacking-group-behind-global-cyberespionage-campaign-2024-03-26/.

234 Tom Burt, "New Cyberattacks Targeting U.S. Elections," *Microsoft on the Issues* (blog), Microsoft, September 10, 2020, https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/; Vicens and Johnson, "US and UK Accuse China of Cyber Operations"; USCC, "Section 2: China's Cyber Capabilities"; and "APT Group: APT 31," Electronic Transactions Development Agency.

235 Vicens and Johnson, "US and UK Accuse China of Cyber Operations"; and USCC, "Section 2: China's Cyber Capabilities."

236 Derek B. Johnson, "Chinese Hackers Target Family Members to Surveil Hard Targets," CyberScoop, March 26, 2024, https://cyberscoop.com/china-hacking-family-members/.

237 Ibid.

238 USCC, "Section 2: China's Cyber Capabilities"; and "APT Group: APT 31," Electronic Transactions Development Agency.

239 USCC, "Section 2: China's Cyber Capabilities"; Sergiu Gatlan, "Google: Chinese Hackers Target Gmail Users Affiliated with US Govt," Bleeping Computer, March 8, 2022, https://www.bleepingcomputer.com/news/security/google-chinese-hackers-target-gmail-users-affiliated-with-us-govt/; and "APT Group: APT 31," Electronic Transactions Development Agency.

240 Pomfret and Tian, "APT31: the Chinese Hacking Group Behind"; and James Pearson, Raphael Satter, and Christopher Bing, "US, UK Accuse China of Cyberespionage That Hit Millions of People," Reuters, March 25, 2024, https://www.reuters.com/technology/cybersecurity/us-sanctions-chinese-cyberespionage-firm-saying-it-hacked-us-energy-industry-2024-03-25/.

241 Pearson, Satter, and Bing, "US, UK Accuse China"; and Pomfret and Tian, "APT31: the Chinese Hacking Group Behind."

242 Pearson, Satter, and Bing, "US, UK Accuse China"; and Pomfret and Tian, "APT31: the Chinese Hacking Group Behind."

243 Aardvark Infinity, "Comprehensive Profile of APT3 (Boyusec)," Medium, August 1, 2024, https://medium.com/aardvark-infinity/comprehensive-profile-of-apt3-boyusec-d0f0626fcfaf; and "APT Group: APT 3, Gothic Panda, Buckeye," Electronic Transactions Development Agency, September 12, 2022, https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%203%2C%20Gothic%20Panda%2C%20Buckeye.

244 Bill Gertz, "Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service," Washington Free Beacon, November 29, 2016, https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/; Aarvark Infinity, "Comprehensive Profile"; Josh Chin, "Chinese Cybersecurity Firm Allegedly Behind Moody's, Siemens Hacks Has Folded," MarketWatch, November 28, 2017, https://www.marketwatch.com/story/chinese-cybersecurity-firm-allegedly-behind-moodys-siemens-hacks-has-folded-2017-11-28?siteid=bigcharts&dist=bigcharts; Jai Vijayan, "APT3 Threat Group a Contractor for Chinese Intelligence Agency," DarkReading, May 18, 2017, https://www.darkreading.com/cyberattacks-data-breaches/apt3-threat-group-a-contractor-for-chinese-intelligence-agency; and "APT3 Is Boyusec, a Chinese Intelligence Contractor," Intrusion Truth, May 9, 2017, https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/.

245 USCC, "Section 2: China's Cyber Capabilities."

246 Ibid.

247 USCC, "Section 2: China's Cyber Capabilities"; and Dan Goodin, "Stolen NSA Hacking Tools Were Used in the Wild 14 Months Before Shadow Brokers Leak," Ars Technica, May 7, 2019, https://arstechnica.com/information-technology/2019/05/stolen-nsa-hacking-tools-were-used-in-the-wild-14-months-before-shadow-brokers-leak/.

248 "APT group: APT 3," Electronic Transactions Development Agency; and USCC, "Section 2: China's Cyber Capabilities."

249 "APT group: APT 3," Electronic Transactions Development Agency; and USCC, "Section 2: China's Cyber Capabilities."

250 Office of Public Affairs, U.S. Department of Justice, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," press release, November 27, 2017, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

251 Microsoft Threat Intelligence, "Flax Typhoon Using Legitimate Software to Quietly Access Taiwanese Organizations," *Microsoft Security* (blog), Microsoft, August 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/; and "APT Group: Flax Typhoon," Electronic Transactions Development Agency.

252 Microsoft Threat Intelligence, "Flax Typhoon Using Legitimate Software."

253 Recorded Future, *Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation* (Somerville, MA: Insikt Group, Recorded Future, June 2024), https://go.recordedfuture.com/hubfs/reports/cta-cn-2024-0624.pdf; "APT Group: Flax Typhoon," Electronic Transactions Development Agency; and "Recorded Future Exposes RedJuliett," Industrial Cyber.

254 "APT Group: Flax Typhoon," Electronic Transactions Development Agency; Recorded Future, *Chinese State-Sponsored RedJuliett*; and "Recorded Future Exposes RedJuliett," Industrial Cyber.

255 Microsoft Threat Intelligence, "Flax Typhoon Using Legitimate Software."

256 Joe Warminsky, "FBI Says It Recently Dismantled a Second Major China-Linked Botnet," *The Record*, September 18, 2024, https://therecord.media/fbi-dismantles-flax-typhoon-china-linked-botnet-wray-aspen.

257 Microsoft Threat Intelligence, "Flax Typhoon Using Legitimate Software."

258 "APT Group: Flax Typhoon," Electronic Transactions Development Agency.

259 Recorded Future, *Chinese State-Sponsored RedJuliett* and APT Group: Flax Typhoon," Electronic Transactions Development Agency.

260 Agence France Presse, "Hackers Stole 'Sensitive' Data from Taiwan Telecom Giant: Ministry," Tech Xplore, March 1, 2024, https://techxplore.com/news/2024-03-hackers-stole-sensitive-taiwan-telecom.html.

261 Recorded Future, *Chinese State-Sponsored RedJuliett*.

262 Ionut Ilascu, "AT&T, Verizon Reportedly Hacked to Target US Govt Wiretapping Platform," Bleeping Computer, October 7, 2024, https://www.bleepingcomputer.com/news/security/atandt-verizon-reportedly-hacked-to-target-us-govt-wiretapping-platform/.

263 Ellen Nakashima, "China Hacked Major U.S. Telecom Firms in Apparent Counterspy Operation," *Washington Post*, October 6, 2024, https://www.washingtonpost.com/national-security/2024/10/06/salt-typhoon-china-espionage-telecom/; and Ilascu, "AT&T, Verizon Reportedly Hacked."

264 Ilascu, "AT&T, Verizon Reportedly Hacked"; and "Threat Group: GhostEmperor," Electronic Transactions Development Agency (ETDA), n.d., https://apt.etda.or.th/cgi-bin/showcard.cgi?g=GhostEmperor.

265 Krouse et al., "U.S. Wiretap Systems Targeted"; and Ilascu, "AT&T, Verizon Reportedly Hacked."

266 Sarah Krouse, Robert McMillan, and Dustin Volz, "China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack," *Wall Street Journal*, September 26, 2024, https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835?mod=article_inline; and Krouse et al., "U.S. Wiretap Systems Targeted."

267 Krouse et al., "U.S. Wiretap Systems Targeted"; Lawrence Abrams, "T-Mobile Confirms It Was Hacked in Recent Wave of Telecom Breaches," Bleeping Computer, November 16, 2024, https://www.bleepingcomputer.com/news/security/t-mobile-confirms-it-was-hacked-in-recent-wave-of-telecom-breaches/; Ilascu, "AT&T, Verizon Reportedly Hacked"; Collins, "FBI Confirms Chinese Hackers Accessed US Government"; and Ellen Jennings-Trace, "Chinese Hackers Allegedly Hit US Wiretap Systems to Hit Broadband Networks," TechRadar, October 7, 2024, https://www.techradar.com/pro/chinese-hackers-allegedly-hit-us-wiretap-systems-to-hit-broadband-networks.

268 Krouse, McMillan, and Volz, "China-Linked Hackers Breach U.S. Internet Providers."

269 Mercy A. Kuo, "How China's 'Salt Typhoon' Hackers Broke Into US Telecoms," *The Diplomat*, October 29, 2024, https://thediplomat.com/2024/10/how-chinas-salt-typhoon-hackers-broke-into-us-telecoms/; Ilascu, "AT&T, Verizon Reportedly Hacked"; and Benedict Collins, "FBI Confirms Chinese Hackers Accessed US Government Official Devices, Networks," TechRadar, November 14, 2024, https://www.techradar.com/pro/fbi-confirms-chinese-hackers-accessed-us-government-official-devices-networks.

270 Nakashima, "Top Senator Calls Salt Typhoon"; and Devlin Barrett, Jonathan Swan, and Maggie Haberman, "Chinese Hackers Are Said to Have Targeted Phones Used by Trump and Vance," *New York Times*, October 25, 2024, https://www.nytimes.com/2024/10/25/us/politics/trump-vance-hack.html.

271 Krouse et al., "U.S. Wiretap Systems Targeted"; and Ilascu, "AT&T, Verizon Reportedly Hacked."

272 Insikt Group, "China's New Cybersecurity Measures Allow State Police to Remotely Access Company Systems," Recorded Future, February 8, 2019, https://www.recordedfuture.com/research/china-cybersecurity-measures; Minxin Pei, "Piercing the Veil of Secrecy: The Surveillance Role of China's MSS and MPS," China Leadership Monitor, February 29, 2024, https://www.prcleader.org/post/piercing-the-veil-of-secrecy-the-surveillance-role-of-china-s-mss-and-mps; and "Ministry of Public Security," State Council: The People's Republic of China, August 25, 2014, https://english.www.gov.cn/state_council/2014/09/09/content_281474986284154.htm.

273 "China: Structure of the Public Security Police; Whether Witness Protection Programs Exist for Those Fearing Organized Crime Groups (2014)," United Nations High Commissioner for Refugees, October 10, 2014, https://webarchive.archive.unhcr.org/20230521014955/https:/www.refworld.org/docid/54648cbd4.html; and "Ministry of Public Security Headquarters," Intelligence Resource Program, Federation of American Scientists, n.d., https://irp.fas.org/world/china/facilities/mps_hq.htm.

274 Insikt Group, "China's New Cybersecurity Measures."

275 Ibid.

276 Ibid.

277 Ibid.

278 Ibid.

279 Ibid.

280 USCC, "Section 2: China's Cyber Capabilities."

281 Ibid.

282 Chavane and TDR team, *A Three-Beat Waltz*; and Uren, "The PLA's Cyber Operations."

283 Microsoft Threat Intelligence, *Digital Threats from East Asia Increase in Breadth and Effectiveness* (Redmond, WA: Microsoft, September 2023), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW; Chavane and TDR team, A Three-Beat Waltz; and Jones et al., *Competing without Fighting*.

284 Office of Public Affairs, U.S. Department of Justice, "40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents," press release, April 17, 2023, https://www.justice.gov/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us; Microsoft Threat Intelligence, *Digital Threats from East Asia*; and Ryan Atkinson, "Artificial Intelligence in Modern Warfare: Strategic Innovation and Emerging Risks," Army University Press, *Military Review*, September–October 2024, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/SO-24/SO-24-Artificial-Intelligence-Strategic-Innovation-and-Emerging-Risks/.

285 Office of Public Affairs, U.S. Department of Justice, "40 Officers of China's National Police"; United States Attorney's Office, Eastern District of New York, U.S. Department of Justice, "34 Officers of People's Republic of China National Police Charged with Perpetrating Transnational Repression Scheme Targeting U.S. Residents," press release, April 17, 2023, https://www.justice.gov/usao-edny/pr/34-officers-peoples-republic-china-national-police-charged-perpetrating-transnational; and Rohan Goswami, "Chinese Social Media Campaigns Are Successfully Impersonating U.S. Voters, Microsoft Warns," CNBC, September 7, 2023, https://www.cnbc.com/2023/09/07/china-campaigns-target-us-elections-on-social-media-microsoft-report.html.

286 Jones et al., *Competing without Fighting*.

287 Ibid.

288 "Cyberspace Administration of China (CAC)," Thomson Reuters; and Jamie P. Horsley, "Behind the Facade of China's Cyber Super-Regulator," DigiChina, Stanford University, August 8, 2022, https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/

289 Cyberspace Administration of China (CAC), "General Secretary Xi Jinping's Introduction to Important Ideology Regarding China as a Cyber Powerhouse," Interpret: China, Center for Strategic and International Studies, July 1, 2023, https://interpret.csis.org/translations/general-secretary-xi-jinpings-introduction-to-important-ideology-regarding-china-as-a-cyber-powerhouse-chapter-5-building-a-durable-national-cybersecurity-barrier/.

290 Ng, "China Broadens Cyber."

291 Horsley, "Behind the Facade."; and Cyberspace Administration of China (CAC), "General Secretary Xi Jinping's Introduction."

292 "Cyberspace Administration of China (CAC) (国家互联网信息办公室)," Thomson Reuters, n.d., https://uk.practicallaw.thomsonreuters.com/8-618-2325?transitionType=Default&contextData=(sc.Default)&firstPage=true.

293 Horsley, "Behind the Facade."

294 Ibid.

295 Ibid.

296 Ibid.

297 Ibid.

298 Jones et al., *Competing without Fighting*, 34.

299 Ibid.

300 Christopher K. Tong, "China Turns to Private Hackers as it Cracks Down on Online Activists on Tiananmen Square Anniversary," University of Maryland, Baltimore County, June 7, 2024, https://umbc.edu/stories/china-private-hackers-tiananmen-square-anniversary/; and Jones et al., *Competing without Fighting*, 31.

301 Jones et al., *Competing without Fighting*, 31.

302 Ibid., 34.

303 Ibid.

304 Collier, "Taiwanese Websites Hit with DDoS Attacks"; Wu and Baptista, "From 7-11s to Train Stations"; CrowdStrike, *2023 Global Threat*; and "Pelosi's Taiwan Visit Widens Taipei-Beijing Rift," Cyble, August 10, 2022, https://cyble.com/blog/pelosis-taiwan-visit-widens-taipei-beijing-rift/.

305 Wu and Baptista, "From 7-11s to Train Stations."

306 Chang, *Warring State*.

307 Raud, *China and Cyber*.

308 Ibid.

309 Eves, "Chinese Nationalist Groups"; and Raud, *China and Cyber*.

310 Lewis Eves, "Chinese Nationalist Groups Are Launching Cyber-Attacks – Often Against the Wishes of the Government," *The Conversation*, May 14, 2024, https://theconversation.com/chinese-nationalist-groups-are-launching-cyber-attacks-often-against-the-wishes-of-the-government-229785.

311 Dina Temple-Raston, "China's Microsoft Hack May Have Had a Bigger Purpose Than Just Spying," *All Things Considered*, NPR, August 26, 2021, https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.

312 *United States of America v. Fujie Wang and John Doe*.

313 Kelli Young, "Cyber Case Study: Anthem Data Breach," CoverLink Insurance, September 27, 2021, https://coverlink.com/case-study/anthem-data-breach/.

314 Young, "Cyber Case Study"; and California Department of Insurance, "Anthem Data Breach."

315 Young, "Cyber Case Study."

316 Nakashima, "Security Firm Finds Link"; and Cimpanu, "Chinese Universities Connected."

317 Nakashima, "Security Firm Finds Link"; and Cimpanu, "Chinese Universities Connected."

318 Nakashima, "Security Firm Finds Link"; Cimpanu, "Chinese Universities Connected."

319 "Compromise at the Office of Personnel Management," Council on Foreign Relations, n.d., https://www.cfr.org/cyber-operations/compromise-office-personnel-management.

320 Josh Fruhlinger, "The OPM Hack Explained: Bad Security Practices Meet China's Captain America," CSO Online, February 12, 2022, https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

321 Eric Tucker, "Missed Opportunities Detailed Ahead of Personnel Agency Hack," AP News, September 7, 2016, https://apnews.com/united-states-government-general-news-42ddc084ce184218bb3d83d706d71ea2; Committee on Oversight and Government Reform, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation* (Washington, DC: U.S. House of Representatives, 114th Cong., September 7, 2016), https://oversight.house.gov/wp-con-

tent/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf; and Fruhlinger, "The OPM Hack Explained."

322 Fruhlinger, "The OPM Hack Explained."

323 Ibid.

324 Fruhlinger, "The OPM Hack Explained"; and Andy Greenberg, "OPM Now Admits 5.6m Feds' Fingerprints Were Stolen by Hackers," *Wired*, September 23, 2015, https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/.

325 Naylor, "OPM: 21.5 Million"; Fruhlinger, "The OPM Hack Explained"; and "22 Million Affected by OPM Hack," ABC News.

326 "22 Million Affected by OPM Hack," ABC News; and David E. Sanger, "Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says," *New York Times*, September 23, 2015, https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html.

327 "22 Million Affected by OPM Hack," ABC News.

328 Jones et al., *Competing without Fighting*.; Temple-Raston, "China's Microsoft Hack"; and Taylor Telford and Craig Timberg, "Marriott Discloses Massive Data Breach Affecting up to 500 Million Guests," *Washington Post*, November 30, 2018, https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/.

329 Hamza Shaban and Hayley Tsukayama, "Equifax asks consumers for personal info, even after massive data breach," *Washington Post*, September 8, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/after-data-breach-equifax-asks-consumers-for-social-security-numbers-to-see-if-theyve-been-affected/. and Jones et al., Competing without Fighting, 29.

330 "Did the Chinese Government," Healthcare Finance News.

331 In 2021, the UK government formally linked Silk Typhoon with another MSS-affiliated group, Kryptonite Panda.

332 Josh Grunzweig et al., "Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities," Volexity, March 2, 2021, https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/; and Brian Carlson, "The Microsoft Exchange Server Hack: A Timeline," CSO Online, May 6, 2021, https://www.csoonline.com/article/570653/the-microsoft-exchange-server-hack-a-timeline.html.

333 Carlson, "The Microsoft Exchange Server Hack."

334 "ED 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities," CISA, March 3, 2021, https://www.cisa.gov/news-events/directives/ed-21-02-mitigate-microsoft-exchange-premises-product-vulnerabilities; and Carlson, "The Microsoft Exchange Server Hack."

335 Carlson, "The Microsoft Exchange Server Hack."; "A Basic Timeline of the Exchange Mass-Hack," Krebs on Security, March 8, 2021, https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/.; Charlie Osborne, "Everything You Need to Know About the Microsoft Exchange Server Hack," ZDNET, March 26, 2024, https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/; and Jones et al., *Competing without Fighting*.

336 Jones et al., *Competing without Fighting*.

337 Lakshmanan, "After FBI Takedown"; Vicens, "Feds: Chinese Hacking Operations Have Been in Critical Infrastructure"; and Office of Public Affairs, U.S. Department of Justice, "U.S. Government Disrupts Botnet."

338 Office of Public Affairs, U.S. Department of Justice, "U.S. Government Disrupts Botnet"; Gatlan, "CISA: Vendors Must Secure"; and "Chinese Hackers Infiltrated Plane, Train," *The Guardian*.

339 Gatlan, "CISA: Vendors Must Secure"; "Chinese Hackers Infiltrated Plane, Train," *The Guardian*; "Business as Usual," CrowdStrike; Lenaerts-Bergman, "What Are Living off the Land?"; and Davidson and Agencies, "Explainer: What Is Volt Typhoon?"

340 Maine Basan and Meghan Lafferty, "Volt Typhoon Disrupts US Organizations, CISA Issues Alerts," eSecurity Planet, February 16, 2024, https://www.esecurityplanet.com/trends/cisa-issues-alerts-after-volt-typhoon-attacks-us-networks/; Associated Press, "Port of Houston Target of Suspected Nation-State Hack," NBC News, September 24, 2021, https://www.nbcnews.com/tech/security/port-houston-target-suspected-nation-state-hack-rcna2249; and Sophia Fox-Sowell, "Foreign States, Ransomware Threaten U.S. Ports, Says Maritime Security Analyst," StateScoop, March 15, 2024, https://statescoop.com/us-ports-maritime-cybersecurity-threats-2024/.

341 Andy Greenberg and Lily Hay Newman, "China Hacks US Critical Networks in Guam, Raising Cyberwar Fears," *Wired*, May 24, 2023, https://www.wired.com/story/china-volt-typhoon-hack-us-critical-infrastructure/; and Tonya Riley, "Chinese Government-Backed Hackers Infiltrated US Pipeline Companies, FBI Says," CyberScoop, July 20, 2021, https://cyberscoop.com/chinese-government-backed-hackers-infiltrated-us-pipeline-companies-fbi-says/.

342 Microsoft Threat Intelligence, "Volt Typhoon Targets US Critical Infrastructure with Living-off-the-Land Techniques," *Microsoft Security* (blog), Microsoft, May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

343 "Chinese Hackers Infiltrated Plane, Train," *The Guardian*; and Davidson and Agencies, "Explainer: What Is Volt Typhoon?"

344 Vicens, "Feds: Chinese Hacking Operations Have Been in Critical Infrastructure"; Paul Rosenzweig, "Volt Typhoon and the Disruption of the U.S. Cyber Strategy," Lawfare, March 5, 2024, https://www.lawfaremedia.org/article/volt-typhoon-and-the-disruption-of-the-u.s.-cyber-strategy; and "Joint Cybersecurity Advisory," CISA.

345 ODNI, *Annual Threat Assessment*, 2024.

346 Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, April 8, 2009, https://www.wsj.com/articles/SB123914805204099085.

347 "Chinese Hackers Infiltrated Plane, Train," *The Guardian*.

348 Gorman, "Electricity Grid in U.S."

COVER PHOTO LEENA MARTE/CSIS; MOCKO/ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**