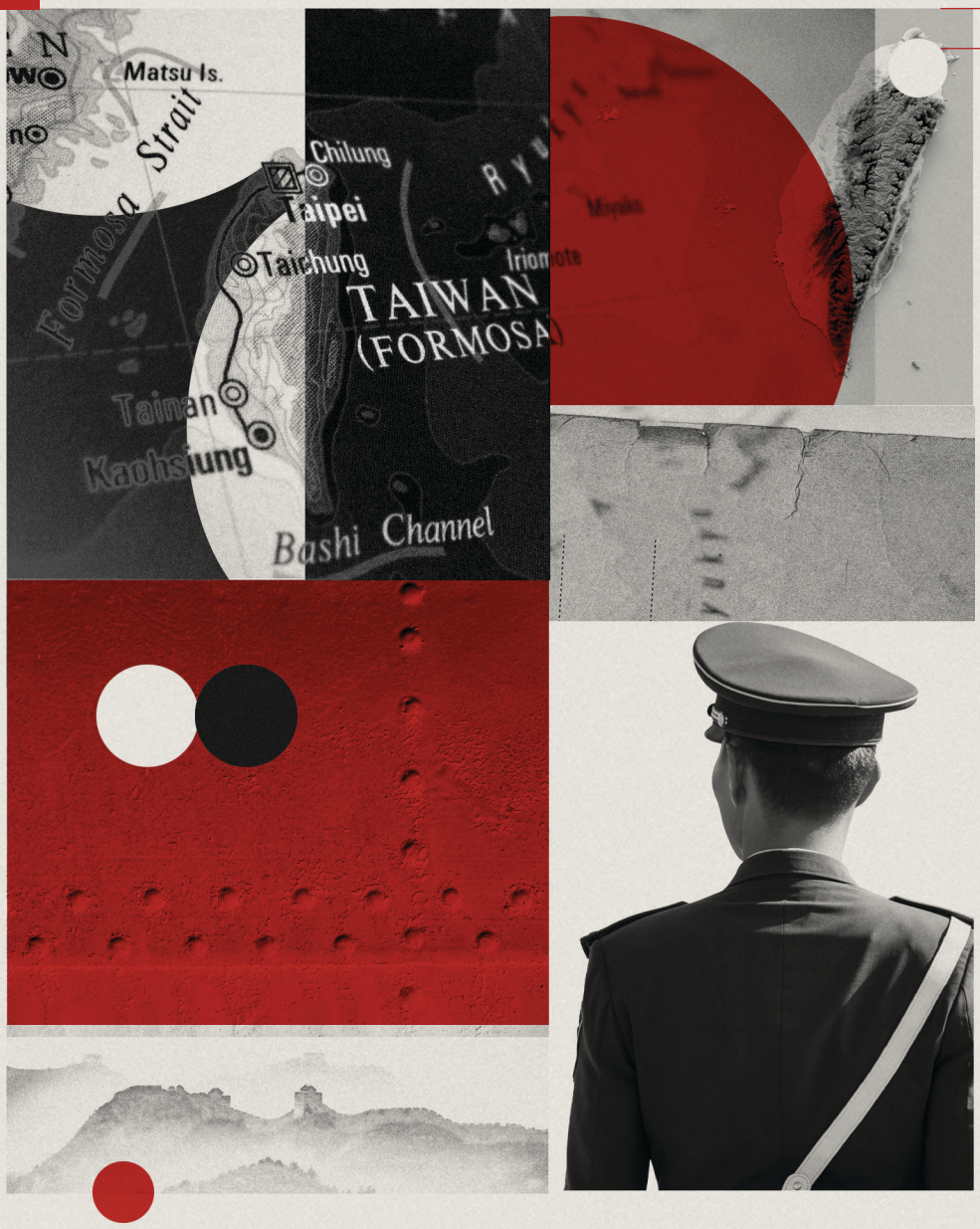
THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

November 23, 2022



FROM COERCION TO INVASION:

The Theory and Execution of China's Cyber Activity in Cross-Strait Relations

This report examines how China conceptualizes and executes cyber coercion and cyber warfare, with a focus on Taiwan. It will be of most interest to Taiwan's government and military, governments and militaries active in the Indo-Pacific region, as well as researchers who focus on China's military and cyber activities. The report's authors, Devin Thorne and Zoe Haver, thank Jessica Drun and Joe McReynolds for their generous reviews and support. Information about the authors can be found at the end of the report.

Executive Summary

The leadership of the People's Republic of China (PRC) firmly believes that Taiwan (ROC) belongs to China. Despite the fact that Taiwan has never been part of the PRC, the Chinese party-state has long sought "reunification" with Taiwan, describing "reunification" as "a shared aspiration of all the sons and daughters of the Chinese nation", "indispensable for the realization of China's rejuvenation", and "a historic mission of the Communist Party of China".[1] In support of this objective, China has consistently attempted to influence Taiwan's behavior, including through coercive diplomatic, economic, and military activity.[2]

Furthermore, China's party-state has vowed to oppose "separatist forces" and "external interference" by the United States, emphasizing that China will strive for peaceful "reunification" with Taiwan but "will always be ready to respond with the use of force or other necessary means to interference by external forces or radical action by separatist elements".[3] This is not an empty threat: the People's Liberation Army (PLA) has long prioritized preparations for a full-scale amphibious invasion of Taiwan, and the PLA is actively pursuing the capabilities that it needs to successfully carry out such an invasion.[4]

With a focus on Taiwan scenarios, this report assesses how the PLA and other relevant actors in China conceptualize and execute cyber coercion and cyber warfare. The report analyzes China's theory of cyber coercion in general and in cross-strait relations, as well as China's theory of cyber warfare and cyber activity in cross-strait conflict scenarios. The report then surveys China's network[5] forces and examines China's efforts to prepare for and execute peacetime and wartime cyber activity, focusing on network forces development, network reconnaissance, and network attacks.

We find that, during peacetime, China is very likely to use network coercion to compel the cessation of perceived pro-independence activities or deter any perceived moves by Taiwan toward independence. During wartime joint landing or blockade campaigns against Taiwan, China would almost certainly engage in network warfare to help seize information dominance, with major targets being military and civilian information systems as well as critical infrastructure. We judge that China's efforts to carry out network forces development, network reconnaissance, and network attacks are equally relevant to peacetime cyber coercion and wartime cyber operations. China is leveraging universities, private enterprises, hacking competitions, cyber ranges, and other means in a whole-of-nation effort to develop weapons and talent for use in both peacetime and wartime network operations. China-linked cyber threat actors have also demonstrated a willingness to use network scanning, phishing, domain spoofing, zero-days, and other tools to carry out network reconnaissance, likely aiming to acquire intelligence and prepare for network attacks. Moreover, China-linked cyber threat actors have already carried out ransomware, distributed denial-of-service (DDoS), and defacement attacks against Taiwan during peacetime and have revealed an interest in attacking adversaries' critical infrastructure.

Key Judgments

- China very likely views the use of cyber capabilities as an option for compelling the Taiwanese government or public to cease perceived pro-independence activities or deterring perceived moves toward Taiwanese independence.
- If China decides to use force against Taiwan, cyber capabilities would almost certainly be used to seek information dominance as part of joint landing or blockade campaigns.
- China's network forces available for use in coercion and war include armed forces units, the personnel of civilian government organizations, and civilians in technology enterprises, and likely also "hobbyists" or patriotic hackers.
- China almost certainly views the full range of cyber attack and technical network investigation tools found in the military and civilian spheres as applicable in coercion and war.
- Network weapons and talent development pipelines in China include military weapons development and training programs, civilian educational programs and recruitment, and national efforts to build cyber ranges.
- China very likely views network reconnaissance, including network inspection and espionage, as an ever-present form of struggle, and has considerable capabilities for carrying out such activity.
- Based on observed cases, China's approach to cyber-enabled espionage prioritizes targeting mid-level and high-level telecommunications infrastructure from which threat actors can collect data on a range of more specific targets.
- China's objectives for cyber war and coercion almost certainly include disrupting, damaging, or destroying the function of military and civilian information systems and critical infrastructure, as well as shocking Taiwanese decision-makers and weakening their will to fight.

Table of Contents

Sources

This report is organized around theoretical discussions of China's approach to cyber coercion and warfare as well as evidence of China's cyber capabilities in practice. The theoretical sections of this report draw heavily from authoritative PLA textbooks published by the Academy of Military Science (AMS; 军事科学院) and National Defense University (NDU; 国防大学). These include NDU's *Science of Campaigns* (published in 2006),[6] the 2013 edition of AMS's *Science of Military Strategy* (hereafter SMS 2013),[7] the 2017 edition of NDU's *Science of Military Strategy* (SMS 2017),[8] and the 2020 edition of NDU's *Science of Military Strategy* (SMS 2020).[9]

AMS and NDU are "China's two premier defense institutes", and foreign experts assess their various editions of *Science of Military Strategy* to be core textbooks "for senior PLA officers on how wars should be planned and conducted at the strategic level".[10] The 2001 edition AMS's *Science of Military Strategy* is believed to have been used to "educate senior PLA decision-makers, including those on the [Central Military Commission], as well as officers who may become China's future strategic planners".[11] *Science of Campaigns* has also been an important educational text used for teaching campaign theory.[12] These edited volumes are not official descriptions of China's military doctrine but are generally believed to provide insight into the PLA's evolving thinking on various doctrinal challenges.[13] When possible, we supplement our reading of these major PLA volumes with analysis of journal articles authored by personnel from Chinese cyber-related military and civilian organizations.[14]

Cyber Coercion

This section discusses China's theory of cyber coercion and the potential for China to use cyber coercion against Taiwan in peacetime, which China could very likely use in an effort to counter perceived moves toward Taiwanese independence. Coercion comprises 2 distinct theories of action to change the behavior of a target: deterrence and compellence.[15] Deterrence uses the threat of punishment to prevent undesirable actions, and compellence wields punishment to motivate desirable actions (or cessation of undesirable actions).[16] Coercion can take many forms, including diplomatic, economic, and military. States can also carry out coercion through cyber means, though experts question its effectiveness.[17]

China's Network Coercion Theory

The 2 elements of coercion, compellence and deterrence, are captured by a single word in Mandarin: *weishe* (威慑). The 2001 edition of the *Science of Military Strategy* defines *weishe* as "the military conduct of a state or political group in displaying force or showing the determination to use force to compel the enemy to submit to one's volition and refrain from taking hostile actions or escalating … hostility".[18] Although SMS 2013 is less explicit, the PLA almost certainly continues to view theories of *weishe* as allowing for what foreign observers call compellence rather than deterrence alone.[19] However, official English translations of Chinese military texts and government-issued white papers on defense strategy translate *weishe* only as "deterrence". Below, we use *weishe* for clarity.

Weishe is both a peacetime and wartime activity, though primarily a peacetime activity given that its fundamental aim is to prevent the outbreak of war or escalation of threats. As a foreign PLA expert summarizes, *weishe* "is to be employed both before and after fighting begins, preferably to avoid war, but also to avoid horizontal escalation (to other regions or strategic directions) or vertical escalation (up the spectrum of violence, especially to nuclear war)".[20] SMS 2013 asserts that "the basic goal" of *weishe* is to "contain a possible offensive from the opponent", "maintain the status", or "stop activities that endanger oneself from happening".[21] Crucially, "activities that endanger oneself" (that is, China) almost certainly include threats other than war, such as threats to China's political security and development interests.[22]

Weishe is also an explicitly political endeavor that involves both military and non-military activity. SMS 2013 stresses that *weishe* aims to achieve political goals, is subordinate to politics, and requires the use of diplomatic, political, military, economic, science and technology, and other means.[23] Likewise, SMS 2017 says that "in peacetime, the major role of strategic *weishe* is the application of national military, political, economic, cultural, diplomatic, and other strategic forces" to influence a state of affairs.[24] The implication is that *weishe* is a whole-of-government effort and civilian entities are very likely involved in activities to support "integrated-whole *weishe*" (整体威慑) alongside any action the military may take.[25]

The range of specific issues in response to which the PLA and the Chinese government may conduct *weishe*, whether military or non-military, is not explicitly listed in any texts reviewed by Recorded Future. However, China's 2019 white paper titled "China's National Defense in the New Era", which was issued by the State Council Information Office, identifies the points listed below as goals of national defense broadly.[26] We believe that this represents a relatively comprehensive list of objectives to which coercive capabilities — up to and including the threat of war — could be applied.

- To oppose and contain "Taiwan independence"
- To deter and resist aggression
- To safeguard national political security, the people's security and social stability
- To crack down on proponents of separatist movements such as "Tibet independence" and the creation of "East Turkistan" (that is, an independent Xinjiang)
- To safeguard national sovereignty, unity, territorial integrity, and security
- To safeguard China's maritime rights and interests
- To safeguard China's security interests in outer space, electromagnetic space, and cyberspace
- To safeguard China's overseas interests
- To support the sustainable development of the country

Although China almost certainly views *weishe* as a strategic concept applicable to many threats, the majority of PLA and civilian texts reviewed by Recorded Future define cyber coercion, or network *weishe* (网络威慑), only with regard to the goal of deterring or responding to cyberattacks from an adversary. SMS 2013, for example, asserts that the goal of network *weishe* is specifically to "forcibly prevent the adversary from daring to willfully carry out large-scale network attacks" and "severe sabotage", principally from "hostile nations" or "terrorist organizations".[27] The focus is on *weishe* "in kind … rather than the use of cross-domain" *weishe*.[28] However, SMS 2017 and SMS 2020 also stress that network warfare should be integrated with struggles in the political, diplomatic, economic, and other domains to serve China's overall strategic goals.[29] Likewise, some non-authoritative sources, such as a 2019 article in *China Information Security* (中国信息安全) — which is affiliated with China's leading civilian intelligence service, the Ministry of State Security (MSS; 国家安全部)[30] — explicitly acknowledge that network *weishe* is "a kind of cross-domain *weishe* strategy" naturally integrated with the pursuit of state goals in other domains.[31]

Even if network *weishe* is limited to countering threats in cyberspace, the scope of what constitutes a threat is likely quite large. China's national defense goals include defending the country's "security interests in … cyberspace".[32] Released in 2016 by the Cyberspace Administration of China, China's National Cyberspace Security Strategy offers insight into what types of online threats network *weishe* might address in a section discussing the "severe challenges" facing China. These include threats to China's political system, economy, culture, society, and national defense.[33]

Cyber Coercion in Cross-Strait Relations

China could decide to carry out cyber coercion against Taiwan in an attempt to influence the behavior of the Taiwanese government or Taiwanese political parties, such as to compel the cessation of perceived pro-independence activities or to deter perceived moves toward Taiwanese independence.[34] Indeed, China has likely already carried out cyber coercion against Taiwan, though it is often difficult to conclusively attribute a coercive motive to alleged Chinese cyber activity.[35]

An instance of cyber coercion likely occurred in response to the visit of Nancy Pelosi, the US Speaker of the House of Representatives, to Taiwan in August 2022, when large-scale cyber attacks allegedly emanating from China hit Taiwan.[36] The attackers, who cybersecurity analysts believe were likely hacktivists rather than China's core network forces (discussed further in the **China's Network Forces** section below), reportedly targeted government websites, utility and transportation websites, infrastructure like railway station screens, and screens in 7-Eleven convenience stores with DDoS attacks and other cyberattacks.[37] Cyber threat activity targeting Taiwan reportedly began increasing as early as July 29,[38] 10 days after the possibility of Pelosi's visit was publicly reported and 2 days after the first "on-the-record" confirmation from a member of the US Congress that Pelosi had indeed invited other legislators to join such a trip.[39] Citing Taiwanese Minister of Digital Affairs Audrey Tang, news organizations reported that "the volume of cyber attacks on Taiwan government units on [August 2], before and during Pelosi's arrival, surpassed 15,000 gigabits, 23 times higher than the previous daily record".[40] The Taiwanese authorities did not directly attribute the attacks to the Chinese government but did indicate that the attacks on government websites originated from IP addresses in China and Russia.[41] The attacks reportedly did little damage as a result of Taiwanese cybersecurity mitigations.[42] This cyber activity coincided with more easily attributable, non-cyber forms of coercion such as military exercises and missile tests.[43]

Cyber Warfare

This section analyzes China's theory of cyber warfare and the potential for China to use cyber warfare against Taiwan in conflict scenarios. We find that Chinese military strategists greatly prioritize offensive cyber action and that the PLA would almost certainly use offensive cyber means, such as "computer viruses" and "hackers",[44] to pursue information dominance during joint landing or blockade campaigns against Taiwan.

China's Network Warfare Theory

The 2017 and 2020 editions of *Science of Military Strategy* argue that networks have become the center of the multidimensional battlefield, and that operations in the network space are, without exception, the backbone of winning wars.[45] The goal of network warfare (网络战) and network operations (网络作战) is to degrade an adversary's information environment, prepare to do so through network reconnaissance (网络侦查), and defend one's own information environment.[46] The network domain involves both computer- and internet-based military operations and electromagnetic warfare operations,[47] though this report focuses on the former.[48] PLA writings sometimes conceptualize the network domain alongside other domains like land, sea, air, and space; in other instances, they present it as a component of the broader information domain.[49]

The various editions of SMS largely present a consistent description of network warfare's characteristics. These include emphasis on the following aspects: wide scope, hidden quality, and destructive potential.[50] Other texts reviewed by Recorded Future as well as broader surveys of works by Chinese analysts show these views are often consistent across diverse sources.[51]

- **Wide Scope:** The battlefield scope is massive because information networks are ubiquitous in modern life and because military and civilian networks are interconnected.
- **Hidden Quality:** Attribution of an attacker or where an attack originates is exceedingly difficult to determine because network attacks are unbounded by time, place, or identity.
- **Destructive Potential:** The effects of a network attack can be devastating across military and civilian systems because the scope of the network space is so wide.

SMS 2017 and SMS 2020 particularly highlight the blurred line between peace and war, noting the networks of all countries are being penetrated in peacetime.[52] They further use America's treatment of Iraq following the Gulf War and just prior to the 2003 Iraq War, which they claim entailed significant intelligence collection and psychological operations, as well as the use of the Stuxnet malware that targeted Iran's nuclear program, to highlight how cyber warfare is defined by escalation and de-escalation in the level and scope of damage rather than the commencement and cessation of activity.[53] These examples are also used to highlight how peacetime cyber operations can act as a forerunner to war. In other words, cyber warfare is a constant element of modern statecraft. Ye Zheng (叶征), the first director of AMS's Informatized Warfare Research Office (信息化作战研究室),[54] has gone as far as to argue that China's network warfare forces should be constantly preparing to conduct network warfare operations and be in a "perpetual state of mobilization".[55]

While Chinese military strategists and analysts discuss both the offensive and defensive aspects of network warfare, offensive capability and "striking first" are greatly prioritized, though SMS 2013 says defense should be the primary consideration.[56] Network operations are seen as an asymmetric weapon for a weaker state (as China perceives itself to be in some domains) to effectively oppose a stronger, technologically advanced adversary (namely, the US).[57] The goal of striking first is to seize information dominance, thereby capturing the "initiative" of a conflict.[58] That is, China can use first strikes to gain an advantage over its adversary, and likely in an overall contest, by disrupting the ability of an adversary's information systems' to effectively function. Some Chinese researchers argue that this "ideology of the offensive" was relatively mainstream among strategists until 2008, after which it became more tempered by a prioritization of defense.[59] However, SMS 2017 continues to emphasize that even defense "relies on actively initiated offensive operations" to seize information dominance.[60]

Cyber Activity in Cross-Strait Conflict Scenarios

If China chose to use military force in pursuit of "reunification" with Taiwan, the PLA would very likely carry out joint landing or blockade campaigns.[61] According to PLA campaign writings,[62] a joint landing campaign would almost certainly involve a push for sea and air dominance in the Taiwan Strait, as well as for dominance in the information domain. The campaign would almost certainly also use key-point strikes to disrupt Taiwan's defenses, including its early warning detection systems, runways and hangars, command and communications systems, missile positions, and harbors. Other components would almost certainly include rapid, continual, and concentrated assaults to penetrate Taiwan's coastal defenses and logistics operations to support the amphibious forces that successfully land on Taiwan. A joint blockade campaign would almost certainly aim to sever Taiwan's "sea-air lanes of communication" by blockading enemy ports and navigational routes, carrying out monitoring, spot inspections, seizure, and attacks at sea, and implementing airborne monitoring, expulsion, intercepts, and attacks.[63]

Joint landing or blockade campaigns carried out by China against Taiwan would almost certainly involve cyber activity as part of operations in the information domain. *Science of Campaigns* describes campaign information warfare as permeating the entirety of campaign operations, from beginning to end, and targeting enemy information detection sources, information channels, and information processing and decision-making systems.[64] The textbook stresses that campaign information warfare comprises both information attack and information defense, and that the former includes network, electromagnetic, and psychological attacks, as well as physical destruction.[65] It states that network attacks (mainly via computer viruses and hackers) are invasive and destructive activities that target enemy computers and computer network systems, including command and control systems.[66]

During a joint landing or blockade campaign, the PLA would almost certainly seek information dominance during the early stages of the campaign, which *Science of Campaigns* frames as an essential prerequisite for seizing air and sea dominance.[67] Information dominance in a joint landing campaign requires — among other components — carrying out information suppression, which includes the use of network attacks and other tools to degrade enemy "information systems' information processing and decision centers", "information detection sources and information channels", "navigation and positioning systems", "communications systems", "early-warning detection systems", and "anti-missile interception systems".[68] Information dominance during a joint blockade campaign requires — among other components — carrying out information reconnaissance, which includes network-based information attacks that aim to "infiltrate computer networks", "break enemy information security codes", "steal intelligence", "implement encroachment by computer viruses", "destroy enemy network operations processes", and "paralyze enemy command and information systems".[69]

Preparation and Execution

This section seeks to bridge the gap between theory and execution, surveying China's range of network forces and examining how China conceptualizes and then implements 3 key types of cyber activity: network forces development, network reconnaissance, and network attack. PLA writings strongly indicate that these 3 categories of activity are relevant to both peacetime cyber coercion and wartime cyber operations. SMS 2020 and SMS 2017 contend that, unlike the military struggles in other domains, network domain struggle is not limited to wartime, but is also found during political, economic, military, cultural, and science and technology struggles in peacetime.[70] To this point, they call for the fusion of peace and war, which includes carrying out *weishe*, intimidating the adversary, constraining war, and preparing for war.[71] Based on this evidence and observed patterns in China's behavior, the content discussed in this section is almost certainly applicable to Chinese cyber activity that could target Taiwan before and during a war.

China's Network Forces

China's network forces include military, government, and non-governmental entities, a combination of which is very likely to participate in a conflict over Taiwan and the preparation for such a conflict. SMS 2013 identifies 3 types of forces for network operations.[72]

First are professional network warfare forces, which are specially trained military units such as those within the Strategic Support Force's (SSF) Network Systems Department (战略支援部队网络系统部) and other parts of the PLA.[73] Network militias also provide a cyber capability within China's armed forces.[74]

Second are authorized forces, which are "local strengths" that can be approved by the military to carry out network operations, such as the MSS and the Ministry of Public Security (MPS).[75]

Third are civilian forces, which are non-governmental entities that can "spontaneously carry out network attack and defense" or be mobilized for network operations.[76] SMS 2017 and SMS 2020 specify that network-electromagnetic forces can include personnel from civilian enterprises and "even some hobbyists with specialized technical skills".[77] In 2015, a researcher affiliated with AMS's Combat Theory and Regulations Research Department (作战理论和条令研究部) described this arrangement of forces as "small core, big periphery" (小核心、大外围), calling for network militias, network police, patriotic hackers, and technical personnel from commercial enterprises to complement China's military strength.[78] [79]

Notably, the entities named in this section are the same seen in real-world examples of peacetime cyber activities emanating from China, including cyber-enabled espionage carried out by the MSS[80] and cyber coercion carried out by likely hacktivists (see Figure 1 below).[81]

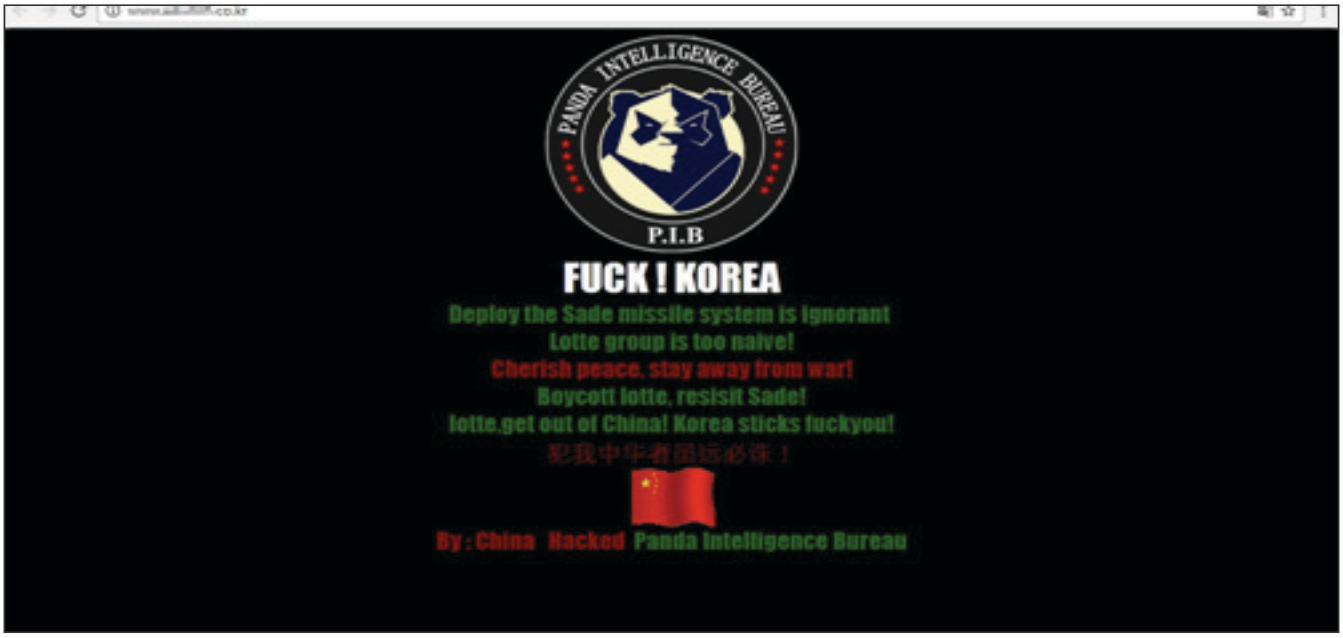


Figure 1: *Defacement attack carried out by self-described patriotic hacking group Panda Intelligence Bureau during the 2017 China-South Korea THAAD dispute (Source: Boan News;[82] Panda Intelligence Bureau[83])*

Network Forces Development

Any significant cyber action that China's military or intelligence forces might take against Taiwan, or in preparation for a Taiwan conflict, would be predicated on the availability of capable forces and effective cyber weapons. While much attention is paid to newly discovered cyber intrusions targeting Taiwan, there are lessons to be learned about China's cyber capability, force strength and identity, and plans by investigating talent and weapons development pipelines. This section briefly outlines the preparation of China's network forces and tools through authoritative sources and real-world examples.

The various editions of *Science of Military Strategy* discuss development of network warfare capabilities from the perspectives of both technical research and talent cultivation, though more detail is provided for the latter. With regard to network warfare weapons, these texts urge readers (presumably PLA officers and other relevant decision-makers) to "plan in advance" and prepare by studying "frontier trends" in technology.[84] Specific types of capabilities to develop are not discussed beyond a call for "'trump card' [撒手锏] means",[85] but those listed in the **Network Reconnaissance** section below and those that would facilitate China's network attack objectives (discussed in the **Network Attack** section) are very likely candidates.

These textbooks, particularly SMS 2017 and SMS 2020, devote more time to the higher-level concern of talent cultivation. They call for training "high-quality network confrontation talent" with a strong understanding of technology and tactics.[86] They further identify 4 types of network warfare talent: 1) "advanced network command talent" for preparing war plans; 2) "staff officer talent" for carrying out network confrontation tasks; 3) "advanced professional talent" with special skills and the ability to develop network weapons; and 4) "network support talent" for operational maintenance and security.[87] According to these textbooks, China's network warfare forces should focus on strategy and strengthen their proactiveness, flexibility, and creativity.[88]

Whole-of-Nation Solutions

All editions of *Science of Military Strategy* reviewed for this study emphasize the importance of military-civil linkages in preparing for, and carrying out, struggle in the network domain.[89] SMS 2017 and SMS 2020 stress drawing on "specialized technical talent" from government departments, enterprises, and society in fostering talented personnel and conducting research relevant to network warfare.[90]

In practice, the SSF's talent development pipeline largely relies on military technical universities and research institutes, with recruitment from civilian universities also being an important avenue of talent acquisition.[91] Network weapons development is contracted by the PLA and military educational institutions to civilian universities and information technology companies, but "the massive scale of the SSF's information warfare programs requires a more controlled and regularized workforce that can only be properly maintained in-house".[92]

The MSS appears to rely relatively more heavily on external contractors, though it has an important in-house capability as well.[93] For example, a professor in Hainan University's (海南大学) Information Security Department allegedly worked with intelligence officers of the Hainan Province State Security Department (海南省国家安全厅) to recruit and manage contract hackers for APT40.[94] The professor reportedly helped establish at least one technology front company, orchestrated password cracking competitions with real-world applications among Hainan University students, and was a point of contact for recruited hackers on managerial issues like pay and benefits.[95]

Examining military-civil and broader government-society coordination in support of China's network capabilities and talent development for military and intelligence purposes reveals numerous real-world examples. A selection of these demonstrating coordination among academia, business, the military, and government are discussed below. Actors from all of these sectors could play a role in a Taiwan wartime scenario, based on the conception of China's network forces found in SMS 2013 discussed above.

In academia, 100,000 cadres from Shanghai's government and defense enterprises are learning "secrets theft and anti-secrets theft" skills through a training platform built by the Ministry of Education Engineering Research Center for Network Information Security Management and Services (网络信息安全管理监控与服务教育部工程研究中心) at Shanghai Jiao Tong University (上海交通大学).[96] Separately, the Southwest University of Science and Technology Net Emergency Response Team (SNERT; 西南科技大学校园网络应急响应小组) in Mianyang, Sichuan, is actually a network militia that organizes training for other militia forces that involve building battlefield local area networks, reconnaissance of enemy system services and permissions, and intelligence interception.[97]

Among businesses, the technology enterprise-sponsored 2018 Tianfu Cup hacking competition led to the discovery of a "chain of exploits" in iPhones that enabled China's intelligence apparatus to spy on members of the Uyghur ethnic community between November 2018 and January 2019 (when Apple issued a fix).[98] Qihoo 360 Technology Co., Ltd. (奇虎360科技有限公司), a cybersecurity company deeply involved in military-civil fusion programs and one of the Tianfu Cup sponsors,[99] has at least one Beijing-based network security militia responsible, in part, for researching (and presumably carrying out if needed) forms of offensive and defensive network operations.[100]

In military and government efforts, PLA Unit 61419 sought the purchase of multiple versions of English-language antivirus software, such as McAfee Total Protection and BitDefender Total Security, in 2019, likely for the purpose of developing their cyber capabilities.[101] The China National Vulnerability Database of Information Security (CNNVD; 中国信息安全漏洞库), which is affiliated with the MSS,[102] has also likely delayed public disclosure of high-threat vulnerabilities exploited by China-linked APT groups.[103] Relatedly, national regulations likely facilitate opportunistic cyber espionage by requiring enterprises and other entities to report any discovered vulnerabilities to the government within 2 days.[104] The use of zero-day vulnerabilities by China-based threat actors has reportedly increased since these regulations were enacted.[105]

Training Infrastructure: Cyber Ranges

A specific means of developing network weapons and network warfare talent that is discussed in authoritative sources is the use of network (cyber) ranges (网络靶场). These are virtual environments for training and testing cyber capabilities. The construction of network ranges is a focus area for China's government,[106] and they are considered national defense mobilization resources.[107] In addition to defensive uses, their offense-oriented use is to examine new network warfare weapons and methods, research tactics, and conduct network confrontation exercises, according to SMS 2017 and SMS 2020.[108] In particular, they can support simulations for "target scouting, information theft, network intrusion, information theft, information or service destruction, and other attack methods", as well as for evaluating the "attack effects" of various attacks.[109]

A July 2022 tender from a PLA entity,[110] likely the Xinjiang Military District (新疆军区),[111] offers a clear example of how cyber ranges are being used to develop network attack and defense skills for jamming enemy communications, infecting different operating systems, and possibly attacking critical infrastructure. The tender was for a "network attack and defense range" (网络攻防靶场) to support team-based combat training. A stated requirement was the capability to simulate communications systems, signal patterns, and anti-jamming methods of foreign military ultrashort wave and microwave communications equipment. The cyber range was also supposed to include "mobile communications network reconnaissance implanting software" (移动通信网侦察植入软件) that would support real-time precise interception of the calls and texts of 4G mobile phones, trojan implantation, traffic hijacking, tampering, and vulnerability analysis, among other functions. The range would further support roughly 200 virtual targets including operating systems, databases, and security equipment; around 100 common attack vectors such as vulnerability exploitation, cross-site scripting, and privilege escalation; proof of concept (PoC)-based automatic attacks (基于poc的自动攻击); and simulated scenarios such as standard enterprise structures in civil aviation, telecommunications, and transportation.[112]

Network Reconnaissance

In line with the assessment that network penetration is a defining feature of the peacetime environment and Ye Zheng's aforementioned call for constant preparation and mobilization,[113] the newest versions of *Science of Military Strategy* assert that intelligence collection via cyberspace is "the most prominent form" of confrontation during times of peace.[114] In advance of a Taiwan scenario, whether a joint landing campaign, joint blockade, or both, China would almost certainly seek to gather up-to-date intelligence from government, military, and other targets in Taiwan. In fact, China's penetration of Taiwan's networks for a range of purposes is likely near constant. As early as 2003, Taiwan's government leaders reported that hackers in China had used 23 different trojans to infiltrate 10 technology companies, from which they infected 50 more companies and 30 government agencies.[115]

SMS 2013 defines cyber-enabled intelligence collection, or network reconnaissance, as the use of nondestructive network exploitation to acquire private information for the purpose of preparing future network attack and defense operations.[116] Network reconnaissance entails reconnoitering an adversary's C4ISRK,[117] electromagnetic, and weapons control systems through network penetration (called "network secrets theft" [网络窃密]) and the retrieval of physical information storage devices with the aid of spies, third-party sellers, and other means (called "media secrets theft" [介质窃密]).[118] SMS 2017 and SMS 2020 provide additional insight as to the intelligence to be targeted for acquisition, specifying the need for information on the enemy's network systems (including structure and configuration [配置]), information capabilities, critical nodes, vulnerabilities, strategic plans, forces, methods, and potential courses of action.[119] Network reconnaissance, therefore, includes both technical investigation of the enemy's systems and espionage, which itself is also a broader objective of network attack. Both technical reconnaissance and espionage are discussed in this section.

Tools of Reconnaissance

SMS 2013 emphasizes that although their goals are different, the methods of network attack and defense are the same as those for network reconnaissance at the technical level.[120] Specific network reconnaissance tactics acknowledged in this textbook include password cracking, information interception, and the use of spyware to acquire locally stored information. SMS 2017 and SMS 2020 are more vague, asserting that network reconnaissance is carried out using "viruses, trojan horses, hacker software".[121]

A 2020 paper by authors affiliated with the AMS Warfare Research Institute (中国人民解放军军事科学院战争研究院) and PLA Unit 31003, which may be the Joint Staff Department Network-Electronic Bureau (联合参谋部网络电子局),[122] identifies more than 20 "common network attack methods".[123] The paper is defense-oriented but likely reflects awareness within major Chinese military institutions of these options for probing the technical features of adversary networks. Other authors associated with AMS have explicitly advocated that some of the same tools, including sniffers and vulnerability scanners, be developed for network reconnaissance.[124] Methods listed in the 2020 paper include:

- Network sniffers (嗅探器), including for full text and account passwords
- Network scanners (网络扫描), including for location, vulnerabilities, and services
- Information service exploitation (信息服务利用), including Finger and LDAP services
- Social engineering (社会工程)
- Network interception (网络拦截) through various methods
- Network phishing (网络欺骗), including through IP and DNS deception, ARP attack, and email phishing

Looking beyond theory, such tools are used by China-linked threat actor groups in the real world. In a 2020 indictment released by the US Department of Justice (DoJ), several cyber actors (including 2 of those involved with APT41) are alleged to have used commercially available network vulnerability scanning tools such as Acunetix and SQLMap.[125] The indictment loosely links APT41 to the MSS.[126] TA413 and TAG-22 (Earth Lusca) likewise use the open-source tool FScan.[127] In addition to using off-the-shelf options, APT41-associated actors also use custom software and malware to understand their targets, such as the queryable social media repository SonarX and MESSAGETAP, which intercepts and analyzes mobile phone text messages.[128]

Illuminating the link between China's strategic interests and network scanning, in 2018, Recorded Future discovered an IP address from Tsinghua University that made over 1 million connections to companies and agencies in Alaska as part of a bulk port scanning operation that immediately followed an Alaskan government delegation to China.[129] A goal of the delegation was to negotiate a potential Alaska-China gas pipeline, and scanned targets included the Alaska Department of Natural Resources, State of Alaska Government, and various Alaskan telecommunications companies. In Taiwan, the deputy director of the Cyber Security Investigation Office of the Investigation Bureau of the Ministry of Justice (台湾法务部调查

局网络安全调查办公室), Liu Chia-zung (劉家宗), warned in 2020 of China's "omnipresent infiltration" efforts.[130] He asserted that since 2018, "at least 10 government agencies and the email accounts of some 6,000 officials" had been targeted with the goal of acquiring "important government documents and data".[131]

Other tactics on the list above have also been observed in the wild. For instance, during the 2020 US presidential election, MSS-linked RedBravo (APT31/Zirconium)[132] "targeted [Joe Biden and Donald Trump] campaign staffers' personal emails with credential phishing emails and emails containing tracking links".[133] TA423 (APT40) has been observed using social engineering tactics, posing, for example, as journalists from "Australian Morning News" and using email subjects like "Sick Leave" and "Request Cooperation".[134] More broadly, over the past 3 years, RedAlpha has been "registering and weaponizing hundreds of domains spoofing organizations such as the International Federation for Human Rights (FIDH), Amnesty International, the Mercator Institute for China Studies (MERICS), Radio Free Asia (RFA), the American Institute in Taiwan (AIT)". This activity is very likely in pursuit of establishing initial access to sources of intelligence in Taiwan and elsewhere.[135]

Modes of Espionage

A prominent trend in China's cyber espionage activities, which can support technical reconnaissance as well, is the exploitation of mid-level and upper-level telecommunications infrastructure from which threat actors can pivot to more specific targets. APT41's MESSAGETAP, for example, was installed in the Short Message Service Center (SMSC) servers of network operators.[136] Similarly, China-based threat actors target managed service providers (MSPs) globally, cloud computing infrastructure, and virtual private network (VPN) providers.[137] According to a June 2022 advisory from the US Cybersecurity & Infrastructure Security Agency, China state-sponsored threat actors also target network devices like SOHO routers and network-attached storage (NAS) devices as midpoints from which to pivot attacks toward other entities.[138] A non-telecommunications analogue of this supply chain-oriented cyber-enabled espionage activity is China's targeting of law firms, where acquisition of their clients' data is the intended objective.[139]

An extreme example of the trend described above is the compromise of at least 30,000 organizations by the MSS and other China-linked groups exploiting a combination of zero-days in Microsoft Exchange.[140] [141] Beginning in late February 2021, thousands of attacks per day were launched to gain access to the email servers of Microsoft's customers.[142] While initially attributed to one threat activity group (HAFNIUM), multiple known and unknown China-based groups also acted on the vulnerabilities before a patch was made public, including APT27, Calypso, Websiic, and Tick Group.[143] Tick Group has been tentatively identified as affiliated with PLA Unit 61419.[144] Tonto Team, which is also reportedly affiliated with the PLA, began exploiting the vulnerability chain after the patch was issued.[145] The Microsoft Exchange intrusion highlights another trend in China's reconnaissance activity: rushing to exploit disclosed vulnerabilities before organizations can issue fixes, as also seen after the 2018 Tianfu Cup.[146] The rapid exploitation of the Microsoft Exchange vulnerabilities by multiple groups, including those associated with the PLA and MSS, also lends further credence to the theory that a "digital quartermaster" ecosystem exists within China's security apparatus to distribute shared capabilities.[147]

Network Attack

Should China decide to apply its cyber capabilities in a Taiwan wartime scenario, the force building, weapons development, and ongoing network reconnaissance activities discussed above would almost certainly culminate in destructive cyber operations against vital government, military, and civilian targets on the island. This section explores how authoritative Chinese sources conceptualize network attack and understand target selection, with lessons for where China's network forces might strike.

Attack Objectives

In addition to extracting intelligence (discussed in the **Network Reconnaissance** section), the various editions of *Science of Military Strategy* describe the principle purpose of network attack as impairing an adversary's information systems. In language highly similar to the aforementioned details of *Science of Campaigns*, which identifies network attack as a type of information attack, SMS 2013 asserts the goal is to degrade system functions through sabotage.[148] SMS 2017 and SMS 2020 likewise advocate destroying and paralyzing an enemy's networks for command and control, communication, and the computer systems of their weapons equipment.[149] A 2015 article in *China Information Security* argues there are 3 levels of attack with increasing severity: "reduced services", "damaged applications", and "paralyzed systems".[150]

Network attacks would almost certainly support China's pursuit of information dominance in a Taiwan scenario, especially at the start of the conflict, with the goal being to cripple the island's ability to accurately assess the battlespace and effectively mobilize resources against threats. Indeed, the 2001 version of *Science of Military Strategy* theorizes about an "electronic Pearl Harbor" scenario in which "a network-electromagnetic strike disables an adversary's ability to engage

in conventional warfare" by disrupting the enemy's information flows through network attacks and other means.[151] The aforementioned Ye Zheng has further argued for integrating network and conventional weapons "in the early stages of war" to strike "links in the enemy's communications chain".[152]

At the tactical level, SMS 2013 describes using worms, trojans, and logic bombs, overtaxing or altering enemy information resources and networks, and transmitting false information to enemy networks.[153] To the latter point, *Science of Campaigns* discusses altering command and control instructions, causing "deviations" in positioning and navigation systems, and targeting weapons systems directly.[154] SMS 2017 and SMS 2020 identifies the "main shape" of network attack as the use of viruses to paralyze enemy systems, steal data, tamper with an enemy's information materials, disrupt networks, and implant fake intelligence.[155] These latest textbooks also reference "chip weapons" (芯片武器),[156] though the meaning is not clear. Other sources like the aforementioned defense-oriented paper by authors affiliated with the AMS Warfare Research Institute and PLA Unit 31003 acknowledge more specific attack methods and typologies such as the use of malicious procedures and scripts (for example, ShellCode), authentication attacks, defense system vulnerabilities in defense systems (such as firewalls and UTM services), software, protocols, and operations, protocol flooding, DDoS, and DNS DDoS.[157]

Although focus is placed on degrading or destroying information systems, various sources also discuss the role of cyber capabilities in manipulating perception, highlighting the relationship between cyber operations and the psychological and cognitive aspects of information warfare. For example, *Science of Campaigns* identifies "special technical warfare" as including actions to insert "manufactured broadcasts and images in the enemy's radio and television stations".[158] In 2016, an AMS-affiliated author likewise argued that examples of network *weishe* include actions to penetrate the enemy's communications networks, distribute propaganda via text messages to citizens, and broadcast propaganda via prime-time television.[159] SMS 2017 and SMS 2020 also raise the example of how, prior to the 2003 Iraq War, thousands of Iraqi military and government personnel received emails from the US military urging surrender".[160] The link between cyber operations and psychological impact is further highlighted in discussions of target selection.

Attack Targets

According to SMS 2017 and SMS 2020, network-electromagnetic warfare "mainly targets the opposite side's psychology, cognitive domain, and decision-making systems" as well as vital and politically sensitive information infrastructure.[161] The objective is to cause a change in the decisions and actions of enemy leaders, thereby changing the "overall situation" of the conflict.[162] Specific targets these textbooks name include ground, air, and space-based "infrastructure network equipment" as well as enemy armed forces, equipment systems, mobilization response mechanisms, and overall support systems.[163] Other targets mentioned include "strategic warning systems" and "military information systems".[164]

The focus is not solely on the adversary's military targets, but extends to civilian critical infrastructure. SMS 2017 and SMS 2020 assert that "major targets" of network warfare also include national decision-makers, as well as "the information systems of energy, transportation, and other national information infrastructure".[165] Without necessarily advocating this as an intentional approach to cyber operations, SMS 2017 and SMS 2020 further observe that network attacks can damage or cause the collapse of an economy, cause political, economic, and social chaos, and "even shake [the enemy's] will to war".[166]

Other sources are more explicit in proposals to target some forms of critical infrastructure. The aforementioned 2016 article by an author affiliated with AMS suggests causing "short-period large-scale blackouts in important enemy cities" as a form of network *weishe*.[167] Further, the procurement activities of Chinese government entities and state-owned enterprises, as well as research by analysts affiliated with the PLA and other organizations, demonstrate at least a defensive interest in Russia's 2015 cyberattack against Ukraine's power grid and follow-on attacks.[168] Some of China's cyber ranges with links to defense contractors and PLA academic institutions simulate industrial control systems as well.[169]

If China's network forces were able to successfully apply their capabilities in a Taiwan wartime context as described by the sources discussed above, the island's telecommunications would very likely be degraded, transportation and energy networks (including the power grid) disrupted, government and military communications networks highly impaired or manipulated with false information, and citizens and warfighters subject to demoralizing propaganda regarding the conflict.

Incidents of Attack

Compared with real-world instances of reconnaissance and espionage, there are fewer concrete examples for China's destructive cyber capability. This is not evidence that China lacks the requisite abilities, but that, as of this writing, authorities have chosen not to use them. That said, China's network forces have indeed targeted an adversary's critical infrastructure on multiple occasions. Several such incidents, including one in Taiwan, are outlined below:

- During the mid-2020 border skirmishes between China and India, RedEcho targeted at least 4 Regional Load Despatch Centres and 2 State Load Despatch Centres in India, which are major elements of India's electrical grids.[170] They also targeted a high-voltage transmission substation and a coal-fired thermal power plant.[171] This activity was likely a form of pre-positioning to support a potential future attack against this critical infrastructure or signal China's capability.[172]
- Taiwan's state-owned energy company CPC Corporation was targeted in a mid-2020 ransomware attack by individuals named in the aforementioned 2020 US DoJ indictment of APT41 that suggests loose links to the MSS.[173] The attack followed President Tsai Ing-wen's victory in Taiwan's 2020 presidential elections. Although ransomware attacks are typically financially motivated, there is some evidence that no demand for payment was made and that the attack was intended to be destructive.[174] The attack encrypted and deleted company files and, as a result, impaired customer's payment options at CPC fuel pumps.[175] [176] We note that cyber threat actors likely connected to Russia and Iran have also reportedly used destructive malware posing as ransomware.[177]
- In late 2011 and late 2012, various unspecified China-linked threat actors and APT1, which is reportedly PLA Unit 61398 of the former General Staff Department Third Department, successfully breached 13 American natural gas pipeline operators and stole information related to a pipeline management system, likely in support of developing capabilities to "physically damage pipelines or disrupt pipeline operations". [178]

At the lower end of the coercive spectrum, China's confrontations with both Taiwan and South Korea over issues of political and geostrategic concern have been marked by a similar pattern of cyber attacks from China-based threat actors to deface and degrade the functioning of foreign government and non-governmental organizations. With regard to Taiwan, China's response to Nancy Pelosi's August 2022 visit was accompanied by a wave of DDoS and defacement attacks against government and public venues as discussed above.[179] This is highly similar to events following South Korea's decision to accept a Terminal High Altitude Area Defense (THAAD) battery from the US in 2017. The South Korean Ministry of Foreign Affairs experienced a surge of DDoS and other cyberattacks and hacking attempts in the period before and after the decision.[180] Websites belonging to the business that agreed to supply land for the THAAD deployment, Lotte Group, and its affiliates also suffered from DDoS and defacement attacks.[181] At the time, a Wall Street Journal article published an interview with FireEye's director of counterespionage analysis, who asserted that Tonto Team (reportedly PLA), APT10 (reportedly associated with the MSS[182]), and patriotic hackers were behind a "variety of attacks against South Korea's government [and] military, defense companies and a big conglomerate [almost certainly Lotte Group]".[183] The attacks against Taiwan have been assessed as likely the work of patriotic hackers.[184] Other potential patriotic hacktivism has also been observed in China's maritime and territorial disputes with the Philippines and Vietnam in the South China Sea.[185]

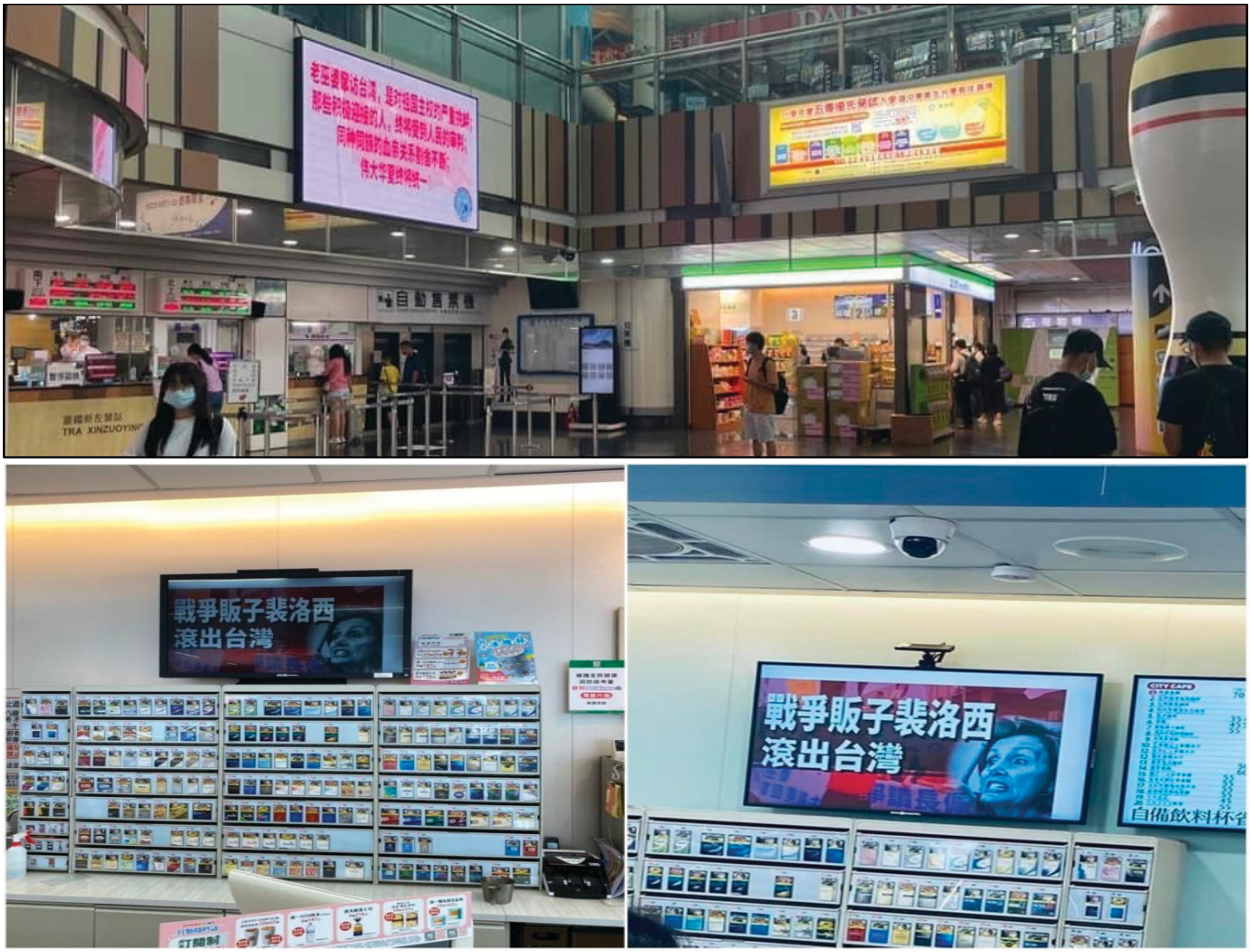


Figure 2: *Defacement attack carried out on public TV screens in response to Nancy Pelosi's visit to Taiwan in August 2022. Top: Screen in a Taiwan Railways Administration station declares the visit a "serious challenge" to China's sovereignty and warns that those who welcome Pelosi will be "judged by the people". Bottom: Screens in 7-Eleven read "Warmonger Pelosi get the fuck out of Taiwan" (Source: Taiwan News[186])*

Outlook

We recommend that cybersecurity organizations and military planners in Taiwan, the US, and other relevant countries heighten defenses against Chinese network reconnaissance and prepare for attacks during both peacetime and wartime. Peacetime Chinese cyber threat activity targeting Taiwan will very likely include coercive efforts intended to prevent perceived moves toward Taiwanese independence; wartime Chinese cyber threat activity will almost certainly include cyber warfare efforts intended to seize information dominance as part of broader joint landing or blockade campaigns against Taiwan. Regarding network reconnaissance, cybersecurity and military planners should prepare for Chinese network reconnaissance operations that use network scanning, phishing, domain spoofing, zero-days, and other tools in an effort to gather intelligence and prepare for future network attacks. Regarding network attacks, planners should prepare for threats that aim to disrupt, damage, or destroy the functions of military and civilian information systems as well as critical infrastructure. As part of their preparations, cybersecurity and military planners should monitor China's whole-of-nation efforts to develop the network forces and weapons, as these efforts will affect the characteristics and effectiveness of Chinese network reconnaissance and attacks.

About the Authors

Devin Thorne
Senior Threat Intelligence Analyst, Insikt Group®

Devin Thorne is part of Insikt Group's Global Issues Team. His research seeks to explain China's security strategies through primary-language sources, with an emphasis on propaganda work, maritime security, military-civil fusion, and national defense mobilization. He holds a bachelors from the University of Alabama at Birmingham and a masters from the Hopkins–Nanjing Center for Chinese and American Studies. He speaks Mandarin.

Zoe Haver
Threat Intelligence Analyst, Insikt Group®

Zoe Haver is part of Insikt Group's Global Issues team. Her research focuses on the South China Sea disputes, maritime security, the People's Liberation Army, public security, and other China-related security issues. She has worked on these topics for Radio Free Asia, the Center for Advanced China Research, SOSi's Center for Intelligence Research and Analysis, the US Naval War College China Maritime Studies Institute, C4ADS, and other organizations. She received her BA from George Washington University and is proficient in Mandarin Chinese.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.

Endnotes

1 "Full Text: The Taiwan Question and China's Reunification in the New Era", PRC State Council Information Office, August 10, 2022, https://archive.ph/AkL5w.
2 Mathieu Duchâtel, "An Assessment of China's Options for Military Coercion of Taiwan", in Joel Wuthnow, Derek Grossman, Phillip C. Saunders, Andrew Scobell, and Andrew N.D. Yang, eds., Crossing the Strait: China's Military Prepares for War with Taiwan (National Defense University Press, 2022), https://ndupress.ndu.edu/Publications/Books/Crossing-the-Strait/; Richard C. Bush, From persuasion to coercion: Beijing's approach to Taiwan and Taiwan's response (Brookings, November 2019), https://www.brookings.edu/research/from-persuasion-to-coercion-beijings-approach-to-taiwan-and-taiwans-response/; Jessica Drun and Bonnie S. Glaser, The Distortion of UN Resolution 2758 and Limits on Taiwan's Access to the United Nations (German Marshall Fund, March 2022), https://www.gmfus.org/news/distortion-un-resolution-2758-and-limits-taiwans-access-united-nations; Brian Hioe, "Following China's Military Drills, Taiwan Settles Into New Normal", The Diplomat, August 16, 2022, https://thediplomat.com/2022/08/following-chinas-military-drills-taiwan-settles-into-new-normal/; Murray Scot Tanner, Chinese Economic Coercion Against Taiwan: A Tricky Weapon to Use (RAND, 2007), https://www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG507.pdf.
3 "The Taiwan Question and China's Reunification in the New Era".
4 "Quick Look Report: 'Large-Scale Amphibious Warfare in Chinese Military Strategy'", China Maritime Studies Institute, June 14, 2021, https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/China%20Maritime%20Studies%20Institute/NWC_CMSI_Conference_Quick%20Look_20210614_Large-Scale%20Amphibious%20Warfare%20in%20Chinese%20Military%20Strategy.pdf?sv=2017-04-17&sr=b&si=DNNFileManagerPolicy&sig=4j5oeE7jvn%2B4MMG%2B3js4JuRG5TRnALIdHS5Zupz7OC8%3D.
5 When discussing cyber activity, Chinese sources typically use the word "network" (网络) rather than "cyber" (赛博), such as "network warfare" or "network reconnaissance". Due to our heavy usage of Chinese-language sources, we generally use "network" when discussing Chinese cyber activity in this report.
6 In Their Own Words: Foreign Military Thought: Science of Campaigns (2006) (China Aerospace Studies Institute and Project Everest, 2020), https://www.airuniversity.af.edu/CASI/Display/Article/2421219/in-their-own-words-plas-science-of-campaigns/.
7 In Their Own Words: Foreign Military Thought: Science of Military Strategy (2013) (China Aerospace Studies Institute and Project Everest, 2021), https://www.airuniversity.af.edu/CASI/Display/Article/2485204/plas-science-of-military-strategy-2013/.
8 Xiao Tianliang [肖天亮], Lou Yaoliang [楼耀亮], Kang Wuchao [亢武超], and Cai Renzhao [蔡仁照], eds., Science of Military Strategy (2017 Revision) [战略学(2017年修订)] (Beijing: National Defense University Press [国防大学出版社], 2017).
9 Xiao Tianliang [肖天亮], Lou Yaoliang [楼耀亮], Kang Wuchao [亢武超], and Cai Renzhao [蔡仁照], eds. Science of Military Strategy (2020 Revision) [战略学(2020年修订) (Beijing: National Defense University Press [国防大学出版社], 2020).
10 Joel Wuthnow, "What I Learned From the PLA's Latest Strategy Textbook", China Brief 21, no. 11 (May 2021), https://jamestown.org/program/what-i-learned-from-the-plas-latest-strategy-textbook/.
11 Andrew S. Erickson, "The Science of Military Strategy", Naval War College Review 60, no. 3, 2007, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1865&context=nwc-review.
12 "Science of Campaigns", p. 729.
13 Wuthnow, "What I Learned From the PLA's Latest Strategy Textbook".
14 The sections of this report that bridge the gap between theory and capabilities leverage a range of open-source materials. These include PLA procurement records, Chinese government websites and documents, information from Chinese companies, foreign research and reporting, US Department of Justice indictments, and information from the Recorded Future Platform.
15 Tami Davis Biddle, "Coercion Theory: A Basic Introduction for Practitioners", Texas National Security Review 3, no. 2 (2020), https://tnsr.org/2020/02/coercion-theory-a-basic-introduction-for-practitioners/; Ketian Zhang, "Cautious Bully: Reputation, Resolve, and Beijing's Use of Coercion in the South China Sea", International Security 44, no 1. (2019), pp. 120-122, https://direct.mit.edu/isec/article-abstract/44/1/117/12241/Cautious-Bully-Reputation-Resolve-and-Beijing-s?redirectedFrom=fulltext.
16 Biddle, "Coercion Theory".
17 Whether cyber coercion is an effective choice is debated. Reservations about revealing capabilities may make countries hesitant to engage in cyber coercion, and the difficulty of attributing any cyberattack to a specific actor may undermine the credibility of attempted coercion because it is inherently less explicit than other forms. The deterrence component of cyber coercion in particular may not be effective for this reason. In other words, the victim must be able to identify who is trying to coerce them in order to understand what actions they are being pressured to cease, and difficulties in attributing cyberattacks to a particular actor can make this unclear. Still, some researchers argue that cyber coercion, like other means, provides numerous options to target the military, economic, and political institutions of an adversary while controlling escalation of tensions and attack severity. See: Daniel R. Flemming and Neil C Rowe, "Cyber Coercion: Cyber Operations Short of Cyberwar", 10th International Conference on Cyber Warfare and Security (2015), https://faculty.nps.edu/ncrowe/oldstudents/flemming_iccws15.htm; Yavuz Akdag, Cyber Deterrence against Cyberwar between the United States and China: A Power Transition Theory Perspective (University of South Florida, 2017), https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=8190&context=etd; Martin C. Libicki, Cyberdeterrence and Cyberwar (RAND, 2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf; Mark B. Manantan, "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea", Issues & Studies 56, no. 3 (2020); Erica D. Lonergan and Grace B. Mueller, "What Are the Implications of the Cyber Dimension of the China-Taiwan Crisis?", Council on Foreign Relations, August 15, 2022, https://www.cfr.org/blog/what-are-implications-cyber-dimension-china-taiwan-crisis.
18 As cited in Dennis J. Blasko, "Chapter 10: China's Evolving Approach to Strategic Deterrence", in Joe McReynolds, ed., China's Evolving Military Strategy (Jamestown Foundation, 2017), p. 340.
19 Blasko, "China's Evolving Approach to Strategic Deterrence", p. 341.
20 Blasko, "China's Evolving Approach to Strategic Deterrence". p. 344.
21 Science of Military Strategy (2013), pp. 168.
22 Blasko, "China's Evolving Approach to Strategic Deterrence", pp. 342, 345.
23 Science of Military Strategy (2013), p. 167-168.
24 Science of Military Strategy (2017). p. 127.

25 Science of Military Strategy (2013), p. 167.
26 "Full Text of 2019 Defense White Paper: 'China's National Defense in the New Era' (English & Chinese Versions)", Andrew S. Erickson, July 24, 2019, https://www.andrewerickson.com/2019/07/full-text-of-defense-white-paper-chinas-national-defense-in-the-new-era-english-chinese-versions/; "China's National Defense in the New Era" White Paper (Full Text) [《新时代的中国国防》白皮书（全文）], PRC State Council Information Office, July 24, 2019, https://archive.ph/CTjjI.
27 Science of Military Strategy (2013), pp. 243-244.
28 Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion", in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds., China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (Oxford University Press, 2015), p. 148.
29 Science of Military Strategy (2020), p. 239; Science of Military Strategy (2017), p. 231.
30 China Information Security (中国信息安全) is a publication managed by the China Information Technology Security Evaluation Center (CNITSEC; 中国信息安全测评中心). CNITSEC is believed to be the public face of the MSS' 13th Bureau, which specializes in network security and exploitation. See Peter Mattis and Matthew Brazil, Chinese Communist Espionage: An Intelligence Primer (Naval Institute Press, 2019), p. 56.
31 Jiang Tianjiao [江天骄], "Cross-Domain Coercion and Network Space Strategic Stability" [跨域威慑与网络空间战略稳定], China Information Security [中国信息安全] 8 (2019); Jiang Tianjiao [江天骄], Cross-Domain Coercion and Network Space Strategic Stability" [跨域威慑与网络空间战略稳定], Security Internal Report [安全内参], October 7, 2019, https://archive.ph/QI7O5.
32 "China's National Defense in the New Era".
33 "National Cyberspace Security Strategy" Full Text [《国家网络空间安全战略》全文], Cyberspace Administration of China Information Office [国家互联网信息办公室], December 27, 2016, https://archive.ph/Qvavf.
34 As noted previously China widely uses diplomatic, economic, and military means to coerce Taiwan. See Duchâtel, "An Assessment of China's Options for Military Coercion of Taiwan"; Bush, From persuasion to coercion: Beijing's approach to Taiwan and Taiwan's response; Drun and Glaser, The Distortion of UN Resolution 2758; Hioe, "Following China's Military Drills, Taiwan Settles Into New Normal"; Tanner, Chinese Economic Coercion Against Taiwan.
35 For example, in May 2020, security officials in Taiwan reportedly told journalists that China-linked ransomware attacks against Taiwanese petrochemical companies could have been timed to coincide with President Tsai Ing-wen's second term inauguration. "Cyberattacks on Democratic Taiwan Set to Rise Ahead of President's Inauguration", Radio Free Asia, May 7, 2020, https://www.rfa.org/english/news/china/cyberattacks-05072020140817.html.
36 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/; Shelly Shan, "Record number of cyberattacks reported", Taipei Times, August 5, 2022, https://www.taipeitimes.com/News/taiwan/archives/2022/08/05/2003783012; Lonergan and Mueller. "What Are the Implications of the Cyber Dimension of the China-Taiwan Crisis?"; Tim Starks and Aaron Schaffer, "Those Pelosi-inspired cyberattacks in Taiwan probably weren't all they were cracked up to be", The Washington Post, August 3, 2022, https://www.washingtonpost.com/politics/2022/08/03/those-pelosi-inspired-cyberattacks-taiwan-probably-werent-all-they-were-cracked-up-be/; Yimou Lee and Christopher Bing, "Attacks on Taiwan websites likely work of Chinese 'hacktivists' - researchers", Reuters, August 2, 2022, https://www.reuters.com/world/attacks-taiwan-websites-likely-work-chinese-hacktivists-researchers-2022-08-02/.
37 Wu and Baptista. "From 7-11s to train stations, cyber attacks plague Taiwan over Pelosi visit".
38 Jonathan Greig, "Cyberattacks on Taiwan started several days before Pelosi arrival: report", The Record, September 30, 2022, https://therecord.media/cyberattacks-on-taiwan-started-several-days-before-pelosi-arrival-report/.
39 Demetri Sevastopulo, "Nancy Pelosi to visit Taiwan next month amid China tensions", Financial Times, July 29, 2022, https://www.ft.com/content/09669099-1565-4723-86c9-84e0ca465825; Scott Wong, "Pelosi has invited senior lawmakers to join Taiwan trip, top Republican", NBC News, July 27, 2022, https://www.nbcnews.com/politics/congress/pelosi-invited-senior-lawmakers-join-taiwan-trip-top-republican-says-rcna40242
40 Wu and Baptista. "From 7-11s to train stations, cyber attacks plague Taiwan over Pelosi visit".
41 Wu and Baptista. "From 7-11s to train stations, cyber attacks plague Taiwan over Pelosi visit"; Lee and Bing. "Attacks on Taiwan websites likely work of Chinese 'hacktivists' - researchers".
42 Shan, "Record number of cyberattacks reported".
43 Lilly Kuo, "China's military extends drills near Taiwan after Pelosi trip", The Washington Post, August 8, 2022, https://www.washingtonpost.com/world/2022/08/08/taiwan-china-military-exercises-pelosi/; Emily Feng, "China fires waves of missiles over the Taiwan Strait, raising tensions in the region", NPR, August 4, 2022, https://www.npr.org/2022/08/04/1115550972/china-taiwan-missile-exercises.
44 Chinese sources tend to refer to "viruses" and "hackers", which we interpret as meaning "malware" and "cyber threat actors".
45 Science of Military Strategy (2020), p. 150; Science of Military Strategy (2017), p. 147.
46 Science of Military Strategy (2013); pp. 241-243.
47 Science of Military Strategy (2013), pp. 241-243.
48 However, some quotes from authoritative sources reflect the link between network and electromagnetic operations.
49 John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support Force: A 'Joint' Force for Information Operations", in Joe Wuthnow,, Arthur S. Ding, Phillip C. Saunders, Andrew Scobell, and Andrew N.D. Yang, eds., The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context (National Defense University Press, 2021), p. 153, https://ndupress.ndu.edu/Publications/Books/PLA-Beyond-Borders/; Science of Military Strategy (2020), p. 142; Science of Military Strategy (2013), pp. 117-118; Science of Campaigns, p. 175-182; Science of Military Strategy (2017), p. 152.
50 Science of Military Strategy (2013), pp. 237-241; Science of Military Strategy (2017), pp. 148-150; Science of Military Strategy (2020), pp. 150-152.
51 Pollpeter, "Chinese Writings on Cyberwarfare and Coercion", pp. 139-162; Science of Campaigns, p. 180
52 Science of Military Strategy (2017), p. 148; Science of Military Strategy (2020), p. 150.
53 Science of Military Strategy (2017), p. 148; Science of Military Strategy (2020), p. 150.
54 Ye Zheng [叶征], "Future Warfare, New-Type Ground Forces, and the Need for Space Information Technology" [未来战争、新型陆军及对空间信息技术需求], Security Internal Report [安全内参], January 6, 2020, https://archive.ph/S2eCH.
55 Joe McReynolds, "Chapter 7: China's Military Strategy for Network Warfare", in McReynolds, China's Evolving Military Strategy, p. 217.

56 Science of Military Strategy (2013), p. 246.
57 Pollpeter, "Chinese Writings on Cyberwarfare and Coercion", pp. 139-143.
58 Science of Military Strategy (2013), p. 160.
59 Jiang Tianjiao, "From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar", Chinese Journal of International Review, 1, no. 2 (2019), pp. 9-15. https://www.worldscientific.com/doi/pdf/10.1142/S2630531319500021.
60 Science of Military Strategy (2017), p. 152.
61 Michael Casey, "Firepower Strike, Blockade, Landing: PLA Campaigns for a Cross-Strait Conflict", in Wuthnow, Grossman, Saunders, Scobell, and Yang, eds., Crossing the Strait.
62 Christopher Yung and Zoe Haver, "The Six Pillars of PLA Amphibious Doctrine", chapter in a forthcoming edited volume; Science of Campaigns, pp. 351-373.
63 Science of Campaigns, p. 344.
64 Science of Campaigns, pp. 175, 178.
65 Science of Campaigns, pp. 178-179.
66 Science of Campaigns, p. 180.
67 Science of Campaigns, pp. 337, 352, 354; Yung and Haver, "The Six Pillars of PLA Amphibious Doctrine"; Casey, "PLA Campaigns for a Cross-Strait Conflict".
68 Science of Campaigns, pp. 358-359.
69 Science of Campaigns, pp. 339.
70 Science of Military Strategy (2020), p. 153; Science of Military Strategy (2017), p. 150.
71 Science of Military Strategy (2020), p. 240; Science of Military Strategy (2016), p. 232.
72 Science of Military Strategy (2013), p. 247
73 Science of Military Strategy (2013), p. 247; John Costello and Joe McReynolds, China's Strategic Support Force: A Force for a New Era, China Strategic Perspectives 13 (Center for the Study of Chinese Military Affairs, 2018), https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf; Dennis J. Blasko, China Maritime Report No. 20: The PLA Army Amphibious Force (China Maritime Studies Institute, April 2022), p. 1, https://digital-commons.usnwc.edu/cmsi-maritime-reports/20/.
74 Devin Thorne, Inside China's National Defense Mobilization Reform: Capacity Surveys, Mobilization Resources, and "New-Type" Militias (Recorded Future, 2022), https://go.recordedfuture.com/hubfs/reports/ta-2022-0310.pdf; see also Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias", in Lindsay, Cheung, and Reveron, eds., China and Cybersecurity.
75 Science of Military Strategy (2013), p. 247; Zoe Haver, The Role of US Technology in China's Public Security System (Recorded Future, 2022), https://www.recordedfuture.com/the-role-of-us-technology-in-china-public-security-system.
76 Science of Military Strategy (2013), p. 247.
77 Science of Military Strategy (2020), p. 237; Science of Military Strategy (2017), p. 229.
78 Yuan Yi [袁艺], "Building a Strong Network Country Requires Planning to Win Network Wars" [建设网络强国必须谋划打赢网络战争], CCP News Net [中国共产党新闻网], March 19, 2015, https://web.archive.org/web/20220921155654/http://theory.people.com.cn/n/2015/0319/c386965-26716789.html.
79 While the sources here reference "hobbyists" and "patriotic hackers", some research suggests that collaborations between the PLA and such groups are "relics of the past, at least at the level of official policy". Joe McReynolds and LeighAnn Luce, "China's Human Capital Ecosystem for Network Warfare", in Roy Kamphausen, ed., The People of the PLA 2.0 (US Army War College Press, 2021), pp. 366-367, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1940&context=monographs.
80 "United States of America v. Zhu Hua and Zhang Shilong", US Department of Justice, December 17, 2018, https://www.justice.gov/opa/press-release/file/1121706/download; "United States of America vs. Yanjun Xu", US Department of Justice, April 4, 2018, https://www.justice.gov/opa/press-release/file/1099876/download.
81 Jonathan Cheng and Josh Chin, "China Hacked South Korea Over Missile Defense, U.S. Firm Says", Wall Street Journal, April 21, 2017, https://www.wsj.com/articles/chinas-secret-weapon-in-south-korea-missile-fight-hackers-1492766403.
82 "[Emergency] Chinese Hacker Organization Indiscriminately Hacking Korean Websites" [[긴급] 중국 해커조직, 한국 웹사이트 무차별 해킹 공격중], Boan News [보안뉴스], March 7, 2017, https://archive.ph/EmLEr.
83 "Panda Intelligence Bureau Panda Intelligence Bureau (PIB) Established" [熊貓情報局 Panda Intelligence Bureau (PIB)成立], Panda Intelligence Bureau [熊貓情報局], September 21, 2016, https://archive.ph/jr0un
84 Science of Military Strategy (2020), p. 239; Science of Military Strategy (2017), p. 231.
85 Science of Military Strategy (2020), p. 240; Science of Military Strategy (2017), p. 232.
86 Science of Military Strategy (2020), p. 412; Science of Military Strategy (2017), p. 411.
87 Science of Military Strategy (2020), p. 412; Science of Military Strategy (2017), p. 411.
88 Science of Military Strategy (2020), p. 240; Science of Military Strategy (2017), p. 232.
89 Science of Military Strategy (2013), pp. 247-248.
90 Science of Military Strategy (2020), p. 240; Science of Military Strategy (2017), p. 232.
91 McReynolds and Luce, "China's Human Capital Ecosystem for Network Warfare".
92 McReynolds and Luce, "China's Human Capital Ecosystem for Network Warfare", p. 370.
93 For example, see the careers of Wu Shizhong (吴世忠) and He Dequan (何德全). In 2009, Wu Shizhong was head of the MSS' Technology Bureau (国家安全部科技局). As late as 2016, Wu was very likely still employed with the MSS. Between at least 2005 and 2013, Wu was also the director of CNITSEC. Wu was also the secretary of CNITSEC's Chinese Communist Party committee between at least 2014 and 2018. As previously noted, CNITSEC is believed to be the public face of the MSS' 13th Bureau specializing in network security and exploitation. He Dequan is an expert in information technology and information security whose employment history strongly suggests MSS employment. This history includes advancement within a list of obfuscated "security departments" (某安全部门) before and after the MSS' creation in 1983 and suspected MSS front organizations, including an advisory role at CNITSEC toward the end of his career. In 1989, He received a "Ministry of State Security Science and

Technology Advancement Award" (国家安全部科技进步奖). See "Notice on the Establishment of a National Standardization Systems Construction Work Organization Standardization Administration of China Comprehensive [2009] No. 42)" [关于成立国家标准化体系建设工作机构的通知 (国标委综合[2009]42号)], Civil Affairs Technology and Standardization Information Platform [民政科技与标准化信息平台], June 2, 2011, https://web.archive.org/web/20190720013714/http://kjbz.mca.gov.cn/article/mzbzhzcwj/201106/20110600157934.shtml; Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3", Recorded Future, May 17, 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3; "China Information Security Product Evaluation and Certification Center Shenzhen, Xinan, and Yunnan Evaluation Centers are Officially Inaugurated" [中国信息安全产品测评认证中心深圳、西南、云南测评中心正式揭牌], China Information Technology Security Evaluation Center [中国信息安全测评中心], March 8, 2005, https://web.archive.org/web/20221102002419/http://www.itsec.gov.cn/zxxw/200503/t20050308_15173.html; "The Ten-Year Review of 'Document No. 27' and the 2013 'Information Security and Communication Secrecy' Editorial Committee was Successfully Held in Beijing" ["27号文"发布十年回顾暨2013《信息安全与通信保密》编委会在京成功举办], Soolun [搜论], January 2014, https://archive.ph/PLd4n; "China Information Technology Security Evaluation Center Party Committee Secretary Wu Shizhong: Implement the Rule by Law Spirit in Cyberspace Goverance" [中国信息安全测评中心党委书记吴世忠：在网络空间治理中落实依法治国精神], Xinhuanet [新华网], November 5, 2014, https://archive.ph/MNui1; Lu Zehua [卢泽华], "Ninety Percent of Online Fraud is Due to Information Leaks, Experts: Urgent Need to Improve Privacy Awareness" [九成网络诈骗因信息泄露 专家：急需提升隐私安全意识], Xinhuanet [新华网], March 28, 2013, https://web.archive.org/web/20200808220056/http://www.xinhuanet.com/2018-03/28/c_1122600133.htm; "He Dequan" [何德全], China Knowledge Centre for Engineering Sciences and Technology [中国工程科技知识中心], https://archive.ph/n9KLo; "He Dequan" [何德全], Archives of Tsinghua University [清华大学档案馆], May 21, 2009, https://archive.ph/AgjVF; "China Trade Association for Anti-Counterfeiting Quality Tracing Research Center Construction Plan" [中国防伪行业协会质量追溯研究中心建设方案], China Trade Association for Anti-Counterfeiting [中国防伪行业协会], https://archive.ph/KuZWX.

94 "Who is Mr Gu?", Intrusion Truth, January 10, 2020, https://intrusiontruth.wordpress.com/2020/01/10/who-is-mr-gu/; "APT40 is run by the Hainan department of the Chinese Ministry of State Security", Intrusion 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/; "United States of America v. Ding Xiaoyang, Cheng Qingmin, Zhu Yunmin, Wu Shurong", US Department of Justice, May 28, 2021, https://www.justice.gov/opa/press-release/file/1412916/download.

95 "What is the Hainan Xiandun Technology Development Company?", Intrusion Truth, January 9, 2020, https://intrusiontruth.wordpress.com/2020/01/09/what-is-the-hainan-xiandun-technology-development-company/; "United States of America v. Ding Xiaoyang, Cheng Qingmin, Zhu Yunmin, Wu Shurong".

96 Source documents held by Recorded Future.

97 Thorne, Inside China's National Defense Mobilization Reform.

98 Patrick Howell O'Neil, "How China turned a prize-winning iPhone hack against the Uyghurs", MIT Technology Review, May 6, 2021, https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/.

99 "State Administration for Science, Technology and Industry for National Defense and 360 Enterprise Security Sign Strategic Cooperation Agreement" [国防科工局信息中心与360企业安全签署战略合作协议], Huanqiu Net [环球网], April 19, 2018, https://archive.ph/q5PKK; O'Neil, "How China turned a prize-winning iPhone hack against the Uyghurs".

100 Thorne, Inside China's National Defense Mobilization Reform.

101 "China's PLA Unit 61419 Purchasing Foreign Antivirus Products, Likely for Exploitation", Recorded Future, May 5, 2021, https://www.recordedfuture.com/china-pla-unit-purchasing-antivirus-exploitation.

102 CNNVD is run by CNITSEC. See "Frequently Asked Questions" [常见问题], China National Vulnerability Database of Information Security [国家信息安全漏洞库], https://web.archive.org/web/20220501130153/https://www.cnnvd.org.cn/web/xxk/cjwt.tag.

103 Priscilla Moriuchi and Dr. Bill Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications", Recorded Future, November 16, 2017, https://www.recordedfuture.com/chinese-mss-vulnerability-influence.

104 Devin Thorne and Samantha Hoffman, "China's vulnerability disclosure regulations put state security first", The Strategist, August 31, 2021, https://www.aspistrategist.org.au/chinas-vulnerability-disclosure-regulations-put-state-security-first/.

105 Microsoft Digital Defense Report 2022 (Microsoft, November 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us.

106 Dakota Cary, "Downrange: A Survey of China's Cyber Ranges" (Center for Security and Emerging Technology, September 2022), pp. 4-5, https://cset.georgetown.edu/publication/downrange-a-survey-of-chinas-cyber-ranges/.

107 Thorne, Inside China's National Defense Mobilization Reform.

108 Science of Military Strategy (2020), p. 410; Science of Military Strategy (2017), p. 409.

109 Science of Military Strategy (2020), p. 410; Science of Military Strategy (2017), p. 409.

110 Source documents held by Recorded Future.

111 The tender did not identify the PLA entity, but further open-source investigation revealed that the entity in question was likely a component of the Xinjiang Military District, which falls under the PLA Ground Force in the Western Theater Command.

112 Source documents held by Recorded Future.

113 McReynolds, "China's Military Strategy for Network Warfare", p. 217.

114 Science of Military Strategy (2017), p. 148, 150; Science of Military Strategy (2020), p. 150, 153.

115 Ko Shu-ling, "Cabinet says computers under attack", Taipei Times, September 4, 2003, https://web.archive.org/web/20210920201544/http://www.taipeitimes.com/News/front/archives/2003/09/04/2003066387.

116 Science of Military Strategy (2013), pp. 241-242.

117 C4ISRK stands for Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance, and Kill.

118 Science of Military Strategy (2020), p. 405; Science of Military Strategy (2017), p. 403.

119 Science of Military Strategy (2020), p. 239; Science of Military Strategy (2017), p. 231.

120 Science of Military Strategy (2013), pp. 241-242.

121 Science of Military Strategy (2020), p. 153; Science of Military Strategy (2017), p. 150.

122 Costello and McReynolds, China's Strategic Support Force, p. 62.

123 Kong Rui [孔睿] and He Shaojun [He Shaojun], "Research on Network Attack Classification Based on Effects and Experience Terminology" [基于效果和经验术语的网络攻击分类研究], Network Security Technology & Application [网络安全技术与应用] 5 (2018), pp. 39-42.

124 Yuan, “Building a Strong Network Country Requires Planning to Win Network Wars”.
125 “United States of America v. Jiang Lizhi, Qian Chuan, Fu Qiang”, US Department of Justice, May 7, 2019, https://www.justice.gov/opa/press-release/file/1317206/download.
126 “United States of America v. Jiang Lizhi, Qian Chuan, Fu Qiang”.
127 Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets (Recorded Future, September 2022), https://go.recordedfuture.com/hubfs/reports/cta-2022-0922.pdf; Joseph C Chen, Kenney Lu, Gloria Chen, Jaromir Horejsi, Daniel Lunghi, and Cedric Pernet, Delving Deep: An Analysis of Earth Lusca’s Operations (Trend Micro, January 2022), https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf.
128 “United States of America v. Jiang Lizhi, Qian Chuan, Fu Qiang”; Raymond Leong, Dan Perez, and Tyler Dean, “MESSAGETAP: Who’s Reading Your Text Messages?”, Mandiant, October 31, 2019, https://www.mandiant.com/resources/blog/messagetap-who-is-reading-your-text-messages.
129 Chinese Cyberespionage Originating From Tsinghua University Infrastructure (Recorded Future, 2018), https://go.recordedfuture.com/hubfs/reports/cta-2018-0816.pdf.
130 Yimou Lee, “Taiwan says China behind cyberattacks on government agencies, emails”, Reuters, August 19, 2020, https://www.reuters.com/article/us-taiwan-cyber-china-idUKKCN25F0JK.
131 Lee, “Taiwan says China behind cyberattacks on government agencies”.
132 “UK and allies hold Chinese state responsible for pervasive pattern of hacking”, National Cyber Security Centre, July 19, 2021, https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking.
133 Shane Huntley, “How we’re tackling evolving online threats” Google, October 16, 2020, https://blog.google/threat-analysis-group/how-were-tackling-evolving-online-threats/.
134 Michael Raggi and Sveva Scenarelli, “Rising Tide: Chasing the Currents of Espionage in the South China Sea”, proofpoint, August 30, 2022, https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea/.
135 RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations (Recorded Future, August 2022), https://go.recordedfuture.com/hubfs/reports/ta-2022-0816.pdf.
136 Leong, Perez, and Dean, “MESSAGETAP: Who’s Reading Your Text Messages?”.
137 “Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information”, US Department of Justice, December 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion; Ben Koehl and Joe Hannon, “Microsoft Security—detecting empires in the cloud”, Microsoft, September 24, 2020, https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/; Brian Fung and Geneva Sands, “Suspected Chinese hackers exploited Pulse Secure VPN to compromise ‘dozens’ of agencies and companies in US and Europe”, CNN, April 21, 2021, https://www.cnn.com/2021/04/20/politics/fireeye-pulse-secure-vpn-exploit/index.html.
138 “Alert (AA22-158A): People’s Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices”, Cybersecurity & Infrastructure Security Agency, June 7, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-158a.
139 “NCSC Director Warns of Nation-State Cyber Threats to Law Firms in June 4 Remarks at ILTA LegalSEC Summit 2019”, Office of the Director of National Intelligence, June 7, 2019, https://www.dni.gov/index.php/ncsc-newsroom/item/2002-ncsc-director-warns-of-nation-state-cyber-threats-to-law-firms-in-june-4-remarks-at-ilta-legalsec-summit-2019.
140 Alex Hern, “What is the Hafnium Microsoft hack and why has the UK linked it to China?”, The Guardian, July 19, 2021, https://www.theguardian.com/world/2021/jul/19/what-is-the-hafnium-microsoft-hack-and-why-has-the-uk-linked-it-to-china.
141 “UK and allies hold Chinese state responsible for pervasive pattern of hacking”.
142 “China’s Microsoft Hack May Have Had A Bigger Purpose Than Just Spying”, NPR, August 26, 2021, https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.
143 Matthieu Faou and Mathieu Tartare, “Exchange servers under siege from at least 10 APT groups”, welivesecurity, March 10, 2021, https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/.
144 “China’s PLA Unit 61419 Purchasing Foreign Antivirus Products, Likely for Exploitation”.
145 Nalani Fraser and Kelli Vanderlee, Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions (FireEye, 2019), https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf.
146 O’Neil, “How China turned a prize-winning iPhone hack against the Uyghurs”.
147 This theory originally arose from observations of shared custom tooling among a range of China’s state-sponsored threat actors, including ShadowPad, Winnti, PlugX, and ProxyLogon. For more information on the digital quartermaster theory, see Supply Chain Analysis: From Quartermaster to SunshopFireEye (FireEye, 2014), https://www.mandiant.com/sites/default/files/2021-09/rpt-malware-supply-chain.pdf.
148 Science of Military Strategy (2013), p. 242.
149 Science of Military Strategy (2020), p. 153; Science of Military Strategy (2017), p, 151.
150 Long Zaiye [龙在野], “China’s Thinking on the Construction of Deterrence Balance Capability in Cyberspace” [网络空间威慑制衡能力建设的中国思考], China Information Security [中国信息安全] 11 (2015), p. 38. Note that the source document says “Cyberspace Strategy Forum (网络空间战略论坛)” rather than China Information Security. This is a section of China Information Security. See “Journal Introduction” [期刊简介], China Information Security [中国信息安全], https://web.archive.org/web/20220927182209/http://zgxxaq.ckan.cn/.
151 As cited in McReynolds, “China’s Military Strategy for Network Warfare”, p. 232.
152 As cited in McReynolds, “China’s Military Strategy for Network Warfare”, p. 236.
153 Science of Military Strategy (2013), p. 243.
SMS 2013 - CASI Translation - 243:
154 Science of Campaigns, p. 221.
155 Science of Military Strategy (2020), pp. 405-406; Science of Military Strategy (2017), p, 404.
156 Science of Military Strategy (2020), p. 237; Science of Military Strategy (2017), p. 230.
157 Kong and He, “Research on Network Attack Classification Based on Effects and Experience Terminology”, pp. 39-42.

158 Science of Campaigns, p. 221.
159 Yuan Yi [袁艺], "Analyzing the Characteristics, Types, and Application Main Points of Network Space Coercion" [浅析网络空间威慑的特征、类型和运用要点], CCP News Net [中国共产党新闻网], January 4, 2016, https://archive.ph/LKKj2.
160 Science of Military Strategy (2020), p. 150; Science of Military Strategy (2017), p. 148.
161 Science of Military Strategy (2020), p. 236; Science of Military Strategy (2017), p. 229.
162 Science of Military Strategy (2020), p. 236; Science of Military Strategy (2017), p. 229.
163 Science of Military Strategy (2020), p. 235; Science of Military Strategy (2017), p. 227.
164 Science of Military Strategy (2020), pp, 235-236; Science of Military Strategy (2017), p. 227-228.
165 Science of Military Strategy (2020), pp. 235-235; Science of Military Strategy (2017), pp. 227-228.
166 Science of Military Strategy (2020), p. 153; Science of Military Strategy (2017), p. 151. SMS 2017 uses a slightly different wording.
167 Yuan, "Analyzing the Characteristics, Types, and Application Main Points of Network Space Coercion".
168 Zoe Haver, "China's Government Is Learning From Russia's Cyberattacks Against Ukraine", Recorded Future, March 18, 2022, https://www.recordedfuture.com/chinas-government-is-learning-from-russias-cyberattacks-against-ukraine.
169 Cary, "Downrange", p. 14.
170 China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions (Recorded Future, February 2021), https://www.recordedfuture.com/redecho-targeting-indian-power-sector.
171 China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions.
172 China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions.
173 "United States of America v. Jiang Lizhi, Qian Chuan, Fu Qiang".
174 Same Cloak, More Daggers: Decoding How the People's Republic of China Uses Cyberattacks (Booz Allen Hamilton, 2022), p. 31, https://www.boozallen.com/content/dam/home/pdf/natsec/china-cyber-report.pdf.
175 "United States of America v. Jiang Lizhi, Qian Chuan, Fu Qiang".
176 CyCraft Technology Corp, "China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware", Medium, June 1, 2021, https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5.
177 "Destructive malware targeting Ukrainian organizations", Microsoft Security, January 15, 2022, https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/; Sean Lyngaas, "Suspected Iranian hackers pose as ransomware operators to target Israeli organizations", CyberScoop, May 25, 2021, https://www.cyberscoop.com/iran-ransomware-israel-sentinelone/.
178 Same Cloak, p. 30.
179 Wu and Baptista. "From 7-11s to train stations, cyber attacks plague Taiwan over Pelosi visit"; Shan. "Record number of cyberattacks reported"; Lonergan and Mueller. "What Are the Implications of the Cyber Dimension of the China-Taiwan Crisis?"; Starks and Schaffer, "Those Pelosi-inspired cyberattacks in Taiwan probably weren't all they were cracked up to be"; Lee and Bing, "Attacks on Taiwan websites likely work of Chinese 'hacktivists' - researchers".
180 "Korean foreign ministry gets several DDoS attacks from China", The Korea Herald, March 28, 2017, https://archive.ph/Z3Zth; "Cyberattack Attempts from China on S. Korean Foreign Ministry Surge This Year", KBS World, September 10, 2017, https://archive.ph/mqmNX.
181 "Korean foreign ministry gets several DDoS attacks from China"; Joyce Lee and Heekyong Yang, "South Korea's Lotte Duty Free says website crashed after attack from Chinese IPs", Reuters, March 2, 2017, https://archive.ph/rNayN.
182 "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information".
183 Cheng and Chin, "China Hacked South Korea Over Missile Defense, U.S. Firm Says".
184 Anne An, "Cyber Tools and Foreign Policy: A False Flag Chinese 'APT' and Nancy Pelosi's Visit to Taiwan", Trellix, September 29, 2022, https://www.trellix.com/en-us/about/newsroom/stories/research/cyber-tools-and-foreign-policy.html.
185 Same Cloak, pp. 25-28.
186 Keoni Everington, "Chinese suspected of hacking Taiwan 7-Eleven, TRA signs to mock Pelosi", Taiwan News, August 3, 2022, https://www.taiwannews.com.tw/en/news/4615238/