Testimony Before the U.S.-China Economic and Security Review Commission

Hearing on “China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States”

Thursday, February 17, 2022

John Chen
Lead Analyst
Center for Intelligence Research and Analysis
Exovera

Introduction

The People's Republic of China (PRC) has worked steadily to improve its capabilities for cyberwarfare over the past decades, especially within the armed wing of the ruling Chinese Communist Party (CCP), the People's Liberation Army (PLA). The PLA's Strategic Support Force (SSF) is a direct beneficiary of those efforts. Formed during the sweeping 2016 reorganization of the PLA, the SSF has the mandate, the organization, and the combined capabilities to prosecute layered strategic cyberwarfare operations to deny, destroy, disrupt, and degrade an adversary's critical infrastructure in pursuit of broader political and societal effects. PLA theorists have extolled the virtues of combining multiple different types of information operations in strategic cyberwarfare, and the SSF's organization combines cyber intrusion and espionage forces with psychological operations units accordingly to field a more effective force capable of waging and winning a modern conflict.

This testimony reviews the PRC's military capabilities for cyberwarfare, focusing on the organizational features and capabilities of the SSF. It begins with an overview of the PRC's main cyber actors and command authorities, before proceeding to a description of the SSF's organization and command and control. It then describes some of the SSF's emerging capabilities for both cyberwarfare and psychological operations and concludes with a brief discussion of recommendations for mitigating this threat.

The PRC's Cyber Actors

The PRC relies upon a vast constellation of bureaucracies to carry out its state-sponsored cyber operations. Among the most prominent of these are three civilian and military organizations: the Ministry of Public Security (MPS), the Ministry of State Security (MSS), and the People's Liberation Army's Strategic Support Force ((战略支援部队; SSF). The Ministry of Public Security (MPS)'s provincial Network Security Protection Detachments (网络安全保卫总队), for instance, secure the PRC's domestic network infrastructure by looking for intrusions and investigating internet crimes, the latter of which includes removing what the Chinese Communist Party (CCP) deems "harmful information."[1] The MSS runs cyber-enabled espionage and counter-espionage operations against all manner of foreign government agencies, companies, and dissidents through its provincial departments (国安厅), supported by penetration testers and tool developers housed within the various provincial and functional offshoots of its central-level 13th Bureau, otherwise known as the China Information Technology Evaluation Center (中国信息安全测评中心; CNITSEC).[2] For its part, the SSF prosecutes strategic information support and information operations to secure information dominance and enhance the PLA's ability to fight and win a modern war.[3]

Other agencies are charged with developing the infrastructure, human capital, and technology necessary for their sister organizations to do their work. The Ministry of Industry and Informatization Technology (工业和信息化部; MIIT) and its State

Administration of Science, Technology, and Industry for National Defense (国家国防科技工业局; SASTIND) together orchestrate a vast effort to equip the PRC's cyber agencies with leading-edge technology and supply them with elite talent. Perhaps the most visible aspect of this mission the MIIT and SASTIND administration of a web of research universities with close ties to the PRC's defense industry, including the so-called Seven Sons of National Defense (国防七子).[4]

At the apex of this cyber officialdom is a cluster of leadership organs responsible for directing and coordinating activities in the cyber domain according to the wishes of the PRC's highest leadership. The Central Military Commission (中共中央军事委员会; CMC) oversees the activities of the PRC's military cyber forces, namely the SSF.[5] The CCP Central Committee's Network Security and Informatization Commission (中共中央网络安全和信息化委员会) takes an expansive view of its remit to secure CCP rule by governing both cultural and technical aspects of information security, and acts through its associated office (办公室), which is also known by its equivalent state moniker the Cyberspace Administration of China (国家互联网信息办公室; CAC).[6] The CCP Central Committee's National Security Commission (中共中央国家安全委员会, NSC), a more opaque organizational actor, is likely also involved in directing the PRC's cyber activities to head off emerging national security threats.[7] Each of these bodies are headed by Xi Jinping, illustrating the emphasis with which Xi and the CCP view cyber activities in the context of regime and national security.

SSF Organization and Command and Control

Of the various PRC actors carrying out cyber operations, however, only the SSF has an openly acknowledged mandate to generate effects using the cyber domain expressly to win a conflict with a nation-state adversary. PLA theorists argue that the strategic cyberspace operations to be executed by the SSF are meant to affect an adversary's politics, economy, science and technology, culture, and foreign affairs.[8] Specifically, instructors from the SSF Information Engineering University and the PLA Academy of Military Sciences note that strategic cyber (or network) warfare is directed at the stability of an adversary's sovereignty and governance system, with clear political objectives that transcend the mere destruction or weakening of an opponent's military capability. To that end, they also argue that this strategic cyber warfare should focus on a wide range of targets in pursuit of desired political effects, including economic, political, and societal networks, as well as critical information infrastructure that supports a population's livelihood like the finance, transportation, and electrical power sectors.[9]

The far-reaching ramifications associated with this brand of strategic cyber warfare suggest that the SSF should answer to a highly centralized, tightly held civilian command authority. PLA instructors argue that strategic cyber warfare is a "severe escalation of interstate conflict (国家冲突严重升级)" concerning the overall national strategic situation, to be employed only when diplomatic, economic, and other methods are not effective. As

a result, the ultimate decision authority to undertake strategic cyber warfare should only reside at the highest level of national civilian leadership, rather than with military command (由国家最高领导层而非军方掌控),[10] which places Xi Jinping firmly as the final arbiter of strategic cyberwarfare operations. While the SSF's most potent cyberwarfare formations, namely technical reconnaissance bureaus with advanced persistent threat (APT) capabilities subordinate to the SSF Network Systems Department, frequently target defense industry, media, telecommunications, and other organizations to support the PRC's peacetime cyber and economic espionage campaigns,[11] they would likely prosecute more sensitive missions against political or infrastructural targets at the sole behest of Xi Jinping through the CMC, in keeping with the desire for tight, centralized control over these capabilities.[12]

The SSF's civilian master theoretically commands a sprawling array of diverse organizational assets amalgamated specifically to meet the wide-ranging demands of achieving strategic effects against an adversary in cyberspace. PLA instructors prize the integration of multiple cyber-related disciplines within a strategic cyber force, writing that a convergence of intelligence collection, public opinion warfare, and psychological warfare forces is necessary to field a "combined national force" (国家合力) that can prevail in all-out conflict.[13] Many of these theoretical postulates are borne out in the SSF's force structure: the SSF's cyber forces come in a bewildering variety of flavors. The SSF's Network Systems Department likely oversees and supports centrally-led bases (基地) and bureaus (局) for psychological warfare (311 Base) and network intrusions, regionally-aligned (and possibly Theater Command affiliated) technical reconnaissance bases overseeing administrative divisions (处) and offices (科) as well as operational detachments (大队) and teams (队), and apparently jointly-manned electronic warfare and information communications brigades (旅).[14] The SSF can call upon regular, uniformed military organizations with a variety of service affiliations to execute cyberwarfare missions at strategic, operational, and tactical levels of conflict.

Beyond regular military assets, the SSF also avails itself of civilian resources to accomplish its objectives. Much of this activity can be grouped under military-civil fusion (MCF) efforts to develop and obtain cutting edge technologies. For instance, the SSF's Network Systems Department is a stakeholder in drafting technical standards with dual-use applications,[15] and its technical personnel regularly confer with academics and defense industry researchers to discuss best technical practices.[16] Researchers at the SSF Information Engineering University (SSF-IEU), a premier SSF training ground for its network warfare personnel, work with counterparts at MIIT-run universities on information security topics, among other collaborators and subjects.[17] When domestic MCF efforts prove insufficient to the tasks at hand, SSF units are not shy about procuring Western and other foreign products like antivirus software to support their efforts.[18]

The SSF's cyber forces also lean heavily upon civilian society to staff their ranks. Though it draws much of its human capital from PLA educational institutions like SSF-IEU, the SSF's cyber warfare component (through its pre-reform predecessor the 3PLA) also has

a long history of recruiting technical talent from the PRC's top academic institutions, through special programs, rotational commitments from undergraduate students, and specialized information security competitions.[19] The SSF is also primed to take advantage of the new civilian personnel (文职人员) recruitment system that has replaced the occasionally maligned civilian cadre (文职干部) system.[20] When it is comparatively less able to exploit talent from top universities thanks to competition from the MSS, the SSF can also make use of part-time militia and reserve units, which are typically comprised of civilian personnel from government agencies like MIIT, MPS, and MSS, as well as academic researchers and specialists from state-owned telecoms and other private corporations.[21] In other, unspecified circumstances, the SSF may call upon "authorized forces" (授权力量) drawing from similar civilian entities to augment its capabilities, though details on the logistics and employment of these forces remain elusive.[22]

The SSF's ability to generate its desired effects in cyberspace is therefore reliant upon a well-coordinated but highly centralized command infrastructure capable of wielding both PLA and civilian assets for strategic cyberwarfare missions. PLA-authored texts depict notional coordination responsibilities between the SSF and its sister agencies, with central and local CAC, MPS, and MSS organizations coordinating their activities with strategic SSF components operating under the direct command of the CMC.[23] These support and coordination mechanisms are meant to ensure that the PRC's various cyber actors act in concert when strategic cyberwarfare is underway.

The SSF defied easy comparison to U.S. cyber forces when it was first stood up as part of the 2016 PLA reforms, but recent changes suggest that the SSF may be taking on organizational features more familiar to U.S. observers. For instance, analysts initially characterized the SSF as a distinct military quasi-service with some similarities to U.S. Strategic Command (USSTRATCOM), U.S. Cyber Command (USCYBERCOM), and eventually the U.S. Space Command (USSPACECOM).[24] In some ways, these comparisons still hold true: the SSF's Network Systems Department carries out many of the same functions that USCYBERCOM does, while the SSF's control over military space assets are somewhat similar to the responsibilities held by USSTRATCOM and USSPACECOM. The recent appearance of jointly manned SSF formations, however, could indicate that the organization is inching towards becoming a joint force command rather than a dedicated, distinct military service: the SSF apparently draws personnel from multiple PLA services, including the Air Force and Navy.[25]

The plainest and arguably most consequential difference between the SSF and U.S. cyber forces, however, is that the SSF is organized as the single, unified force within the PLA for seizing and maintaining information dominance, combining space, long-range technical sensing, cyber intrusion, and psychological warfare capabilities into a single force. This combination profoundly shapes the character of the cyberwarfare threat the SSF poses to the United States, as described below.

A "Boosted" Threat Profile

Assessing the SSF's cyberwarfare capabilities is difficult, as operational secrecy is a vital determinant of the effectiveness of cyber intrusions, online influence operations, and other information warfare capabilities. Nevertheless, the SSF's reliance on civilian personnel and infrastructure means that some of its researchers publish their work in academic and technical fora. These works can shed light on topics of interest within the SSF's cyber forces, giving observers a sense (however limited) of the SSF's peacetime cyber activities and its priorities in offensive and psychological operations.

In peacetime, the SSF engages in substantial information security research, occasionally of an obvious defensive bent, though much of this work is inherently dual use. In 2019, one SSF researcher specializing in industrial control systems published research on defensive methods that could be used to detect intrusions in electrical power infrastructure—a topic with clear offensive implications in attacking an adversary's systems.[26] Others specialize in studying methods for monitoring social media: over the last four years, SSF-IEU graduate students have studied spambot detection,[27] user identification across different social media networks,[28] and algorithmic detection of social media communities,[29] topics with cited applications for monitoring the PRC's domestic information environment during peacetime but also obvious applications for influencing foreign social media environments.

Decades of sustained investment, a seemingly endless trail of carnage left in the wake of cyber intrusions attributed to the SSF, and a robust research ecosystem supporting the development of tactics, techniques, and procedures (TTPs) indicate that the SSF's offensive cyberwarfare capabilities are formidable and improving. Perhaps one of the more significant indicators of the SSF's attempts to improve its TTPs is its persistent and progressively advancing interest in algorithmic research to support automation in its cyber intrusion methods. SSF-IEU researchers, for example, are apparently actively working on applying adversarial machine learning to cyber intrusion techniques. The academic works of one research cluster demonstrates a typical pattern of research and development surrounding these techniques: in 2019, SSF-IEU researchers surveyed adversarial example generation techniques for malware[30] and by September 2020, had demonstrated a publishable technique for spoofing network traffic using adversarial examples.[31]

While far less is publicly known about the SSF's capability for waging psychological warfare, evidence suggests it is also working to adapt machine learning and artificial intelligence to enhance social media influence operations. In 2016, a former SSF-IEU professor moved to a university run by the United Front Work Department, known for its overseas influence operations, and began publishing a series of articles on automated models for propagating propaganda messages as part of a broader psychological warfare campaign. His co-author was a researcher from the PLA 61716 Unit, also known as the 311 Base specializing in psychological operations.[32] Others have contributed to a large existing body of work on sentiment analysis in foreign languages, including a March 2021

article analyzing the tweets of selected U.S. cabinet members, members of Congress, and governors.[33] While these studies do not explicitly describe offensive applications of their research findings as part of a sustained campaign of online psychological warfare, they provide insights into areas of interest for the SSF's cyber operators.

Though SSF advances in each of these respective fields of information operations merit close observation, the potential use of these distinct types of operations together as part of a sequence of attacks may be much more effective than their application alone. When executed with the appropriate timing, combining different kinds of information operations like cyber intrusions and psychological operations can amplify or "boost" the effects of an initial network compromise and subsequent attack, generating fear, uncertainty, and doubt that can set off chain reactions and larger political consequences.[34] For instance, a single hypothetical cyberattack on Taipei's subway infrastructure could shut down popular transit lines, while a discrete social media influence campaign accusing subway officials of corruption could trigger outcry and political pressure among an engaged public. Launching intermittent cyberattacks against subway infrastructure amid a sustained online influence campaign tarnishing public transit officials during election season, however, would not only destroy hard infrastructure, but also undermine public confidence in a fare-dependent subway system, cratering its revenues and delaying needed repairs. The resultant public outcry over degraded service and perceived corruption could also trigger political repercussions at the polls. In examples like these, human cognition and responses are more important targets for SSF cyber operations than any network infrastructure.

The PLA's theoretical views of strategic cyberwarfare and the mixture of capabilities and responsibilities housed within the SSF's cyber forces suggest a strong emphasis on this kind of "boosted" or amplified *modus operandi*. SSF and PLA theorists focus not only on the development of technical capabilities, but also on the seamless application of multiple technical means to generate political effects far more consequential than the mere hacking of network infrastructure. Some note this emphasis explicitly, stating that strategic cyberwarfare is aimed at "a society's psychological and political system," and that the integration of "Three Warfares" specialists with technical network personnel to carry out public opinion warfare, psychological warfare, and legal warfare will only increase in pace and scope in the future.[35]

Key Determinants and Implications

The success and effectiveness of the SSF's cyber forces depend on several key determinants, some of which were direct results of the sweeping 2016 reforms of the PLA. As reforms were underway to enhance the Party center's (read: Xi Jinping) control over the PLA,[36] the official narrative surrounding the SSF made clear that it and its assets were to be controlled primarily by the CMC. This tightly held control could bear fruit for the PRC's leaders in a conflict by funneling all strategic reconnaissance information and sensors to a single centrally controlled organization, which could theoretically engender greater peacetime control over PLA activities. Closeness to the Party center could also

improve coordination between the SSF and the PRC's other cyber actors. On the other hand, however, this tight central control could severely hamstring military operations by forcing PLA Theater Commanders to rely on the CMC to access the SSF's strategic reconnaissance capabilities. This conundrum has likely been partially resolved with the establishment of regionally aligned SSF technical reconnaissance bases, but the concentration of strategic cyber reconnaissance and warfare capabilities at the center may yet hinder the PLA's ability to fight and win a modern conflict.

A second determinant of success was also precipitated by the 2016 reforms. The consolidation of disparate cyber intrusion and espionage units with psychological warfare formations under the SSF may improve its ability to plan and prosecute "boosted" strategic information operations for favorable political effect. The integration of psychological operations units with cyber forces as part of the 2016 PLA reform effort to build a more unified force for information warfare, and the SSF's gradual embrace of a joint force construct will likely provide more routine and diverse planning opportunities for "boosted" strategic cyberwarfare activities. On the other hand, this integration almost certainly kicked off organizational disruptions and bitter bureaucratic rivalry between PLA services that did not want to surrender their cyber forces to another organization.

Better planning and smoother operations aside, the effectiveness of "boosted" cyberwarfare is dependent upon effective political work. The ability to quickly agree upon the desired political outcomes of a conflict and empower trusted actors to achieve these goals is vital for a successful "boosted" cyberattack. Unfortunately for Xi Jinping and the Party center, the PLA's pre-2016 political work system was not exactly a paragon of a healthy and effective principal-agent relationship.[37] The degree to which the 2016 reforms were able to rehabilitate political loyalty to the Chinese Communist Party within the PLA will be a key determinant for success in using cyber operations to achieve favorable political outcomes.

Beyond the changes set in motion by the 2016 reforms, the SSF's success will also depend in large part on its ability to effectively access civilian resources, but the jury is still out on this factor. While the SSF surely makes successful use of its civilian talent and infrastructure, some of this capability is manifested in legal mechanisms with decidedly mixed or unclear results. For instance, legal justifications for commandeering data and processing capabilities stemming from the PRC's National Intelligence Law are reportedly wielded frequently by state authorities but generate dissatisfaction among private sector employees,[38] while the legal pathways (and effectiveness) for using "authorized forces" remain unclear. Compounding the problem, the SSF's cyber militias and reserve units have not necessarily acquitted themselves well, lacking sufficient talent and struggling to integrate into operational-level exercises.[39]

Recommendations

The PRC boasts a vast array of highly capable cyber actors, each with distinct responsibilities and missions. Perhaps the most potent actor in the PRC's cyberwarfare activities is the SSF, which is organized and equipped to execute layered, "boosted" information operations against an adversary's society to generate political effects that can lead to victory in a conflict. While many experts rightly suggest measures to improve network security as a counter to cyberwarfare threats, the U.S. government will also need to assure societal resilience and better defend the human terrain upon which the SSF will attempt to create its most damaging effects. Congress can begin to address this threat in the following ways:

- **Establish an integrated public early warning capability.**

Congress should direct the Department of Homeland Security and other interagency partners to develop a public alert system for describing information operations level of threat to the nation. This system should include warnings about state-directed disinformation efforts and work in close cooperation with warning efforts about cyber intrusions generated by National Cyber Awareness System. A transparent, easily comprehensible, and discrete assessment of the information operations threat level against the United States could activate additional resources for information security and sensitize the public to the likelihood of specific disruptions to their communities, enabling better advance preparation and incident response.

- **Promote public affairs and civil defense outreach efforts.**

Congress should direct funds to local and state governments to improve both public communications capabilities to debunk or "pre-bunk" misinformation, as well as civil defense preparedness if cyberattacks destroy or degrade critical infrastructure. More frequent training exercises and distribution of emergency preparedness information, especially during times of heightened alert, can blunt the broader societal impact of "boosted" information operations.

- **Fund transparency, media literacy, and fact-checking partnerships in civil society.**

Congress should provide grant funding to non-governmental organizations to detect, label, debunk, or "pre-bunk" state-directed disinformation efforts. Think tanks, academic institutions, non-profits, community associations, and other organizations working to expose online influence operations can mitigate the impacts of a sustained state-backed disinformation campaign.

[1] For one example of provincial detachment responsibilities, see “Henan Provincial Public Security Department Network Security Protection Detachment [河南省公安厅网络安全保卫总队], Zhengzhou City Internet Crime and Harmful Information Reporting Platform [郑州市互联网违法和不良信息举报平台], June 24, 2016, http://www.zhengzhoujubao.com/detail.aspx?id=1477

[2] The Guangdong Information Technology Security Evaluation Center [广东信息安全测评中心] is one example of a provincial counterpart to the central CNITSEC. See Insikt Group, “Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3,” May 17, 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3/.

[3] John Costello and Joe McReynolds, “China’s Strategic Support Force: A Force for a New Era,” *China Strategic Perspectives* 13 (NDU Press: Washington, D.C.), pp. 35-44.

[4] Australian Strategic Policy Institute, “China Defence Universities Tracker,” accessed on February 6, 2022 at https://unitracker.aspi.org.au/.

[5] John Costello and Joe McReynolds, “China’s Strategic Support Force: A Force for a New Era,” *China Strategic Perspectives* 13 (NDU Press: Washington, D.C.), p. 1.

[6] For a discussion of the CAC’s expanding roles, see Jamie Tarabay and Coco Liu, “Obscure Cyber Agency Becomes Nemesis of China’s Tech Giants,” Bloomberg, July 13, 2021, https://www.bloomberg.com/news/articles/2021-07-13/xi-elevates-an-obscure-china-regulator-to-take-on-didi-big-tech.

[7] Joel Wuthnow, “A New Chinese National Security Bureaucracy Emerges,” *China Brief* Vol. 21, no. 23, November 23, 2021, accessed at https://jamestown.org/program/early-warning-brief-a-new-chinese-national-security-bureaucracy-emerges/.

[8] John Chen, Joe McReynolds, and Kieran Green, “The Strategic Support Force: A “Joint” Force for Information Operations,” in Joel Wuthnow et al., eds., *The PLA Beyond Borders* (NDU Press: Washington, D.C., 2021), p. 154.

[9] Li Jidong [李继东] and Chen Zhou [陈舟], “On Strategic Cyber Warfare [试论战略网络战],” *China Military Science* 2017, no. 6, p. 47. Li is an instructor at the SSF Information Engineering University, and Chen Zhou is a researcher at the Academy of Military Sciences Warfare Research Institute.

[10] Ibid.

[11] For examples, see Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units,” February 19, 2013, and Crowdstrike, “Putter Panda,” available at https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf.

[12] For theoretical explications of how this chain of command might work, see Wang Jinsong [王劲松], Wang Nanxing [王南星], and Ha Junxian [哈军贤], “Research on Cyberspace Operational Command System” [网络空间作战指挥体系研究], *Journal of Academy of Armored Force Engineering* [装甲兵工程学院学报], no. 5 (2016), p. 3., and Fan Yongtao [樊永涛], Wang Jinsong [王劲松], and Li Shikai [李世楷], “Problems and Solutions to the Cyberspace Operational Command Pattern” [网络空间作战指挥方式面临的问 题及对策], Journal of Academy of Armored Force Engineering, no. 5 (2017), 9.

[13] Li Jidong [李继东] and Chen Zhou [陈舟], “On Strategic Cyber Warfare [试论战略网络战],” *China Military Science* 2017, no. 6, p. 47.

[14] See John Chen, Joe McReynolds, and Kieran Green, “The Strategic Support Force: A “Joint” Force for Information Operations,” in Joel Wuthnow et al., eds., *The PLA Beyond Borders* (NDU Press: Washington, D.C., 2021), p. 166, and Kaifeng City Education Bureau [开封市教育局], “2017-2020 List of National Group Physical Education Advanced Units [2017-2020 年度全国群众体育先进单位名单],” September 26, 2021.

[15] Standards Administration of China [国家标准化管理委员会] and Central Military Commission Equipment Development Department [中央军委装备发展部], “Notice Regarding Specifications for Drafting Process of National Military-Civilian Dual-Use Standards [关于规范军民通用的国家标准制定程序的通知],” December 22, 2020, https://gkml.samr.gov.cn/nsjg/bzjss/202012/W020201230622946248292.pdf.

[16] “Military Measurement Unified Textbook Seminar Convenes at China Jiliang University [《军事计量统编教材》研讨会在我校召开],” China Jiliang University [中国计量大学], January 16, 2017, http://www.hmscxh.com/info/1133/10463.htm.

[17] For one example, see Yuan Qingjun [袁庆军] et. al., "An Improved Template Analysis Method Based on Power Traces Preprocessing with Manifold Learning [基于流形学习能量数据预处理的模板攻击优化方法]," *Journal of Electronics and Information Technology 电子与信息学报* 42, no. 8, pp. 1853-1861.
[18] Insikt Group, "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/.
[19] Joe McReynolds and LeighAnn Luce, "China's Human Capital Ecosystem for Network Warfare," in Roy Kamphausen, ed., *The People in the PLA 2.0* (Carlisle: PA, 2021), pp. 361-364.
[20] Ibid., p. 355
[21] Zuo Juan [左娟] and Jia Jie [贾杰], "Thoughts on Constructing and Strengthening Network Militias" [加强网络民兵建设的思考], National Defense [国防], no. 3 (2019), 58.
[22] Academy of Military Sciences Strategy Research Department [军事科学院战略研究部], eds., *The Science of Military Strategy* [战略学] (Beijing: Military Science Press, 2013), p. 196.
[23] See Wang Jinsong [王劲松], Wang Nanxing [王南星], and Ha Junxian [哈军贤], "Research on Cyberspace Operational Command System" [网络空间作战指挥体系研究], *Journal of Academy of Armored Force Engineering* [装甲兵工程学院学报], no. 5 (2016), p. 3., and Fan Yongtao [樊永涛], Wang Jinsong [王劲松], and Li Shikai [李世楷], "Problems and Solutions to the Cyberspace Operational Command Pattern" [网络空间作战指挥方式面临的问 题及对策], Journal of Academy of Armored Force Engineering, no. 5 (2017), 9.
[24] John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," *China Strategic Perspectives* 13 (NDU Press: Washington, D.C.), p. 9, Elsa Kania and John Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review*, Spring 2018, p. 108.
[25] For examples, see "Bearing in Mind Their Glorious History, the Military and People Build a Dream Together" [铭记光辉历史·军民同心筑梦], Shandong Network [山东网], July 21, 2018, available at http://www.sdwltv.com/soc/20180721/80281.html and "City Leaders Visit Officers and Soldiers Living Under Special Care Conditions" [州领 导走访慰问部队官兵和优抚对象], Yanbian Broadcasting and Television Station [延边广播电视 台], July 31, 2019, available at http://www.yb983.com/p/98894.html.
[26] Zhang Zhigang [张之刚], "Research on Smart Electrical Power Monitoring and Control Sensors [电力监控网络安全态势智能感知方法研究]," PhD degree dissertation, PLA Strategic Support Force Information Engineering University [战略支援部队信息工程大学], 2019.
[27] Qu Qiang [曲强], "Research on Spam User Detection on Social Networks [社交网络垃圾用户检测关键技术研究]," Master's degree dissertation, PLA Strategic Support Force Information Engineering University [战略支援部队信息工程大学], 2019.
[28] Guo Xiaoyu [郭晓宇], "Research on User Identification Across Social Networks [跨社交网络用户身份识别技术研究],"Master's degree dissertation, PLA Strategic Support Force Information Engineering University [战略支援部队信息工程大学], 2020.
[29] Ma Xiaofeng [马晓峰], "Research on Community Detection Algorithms in Social Networks [社交网络中的社区检测算法研究]," PhD dissertation, PLA Strategic Support Force Information Engineering University [战略支援部队信息工程大学], 2018.
[30] Wang Shuwei [王树伟] et al., "Review of Malware Adversarial Sample Generation on Generative Adversarial Networks [基于生成对抗网络的恶意软件对抗样本生成综述]," *Journal of Information Engineering University 信息工程大学学报* 20, no. 5, 2019, pp. 616-621.
[31] Hu Yongjin [胡永进] et al., "Method to Generate Cyber Deception Traffic Based on Adversarial Sample, [基于对抗样本的网络欺骗流量生成方法]," *Journal on Communications 通信学报* 41, no. 9, September 2020, pp. 59-70.
[32] Li Bicheng [李弼程], Hu Huaping [胡华平], and Xiong Yao [熊尧], "Intelligent Agent Model for Network Public Opinion Guidance [网络舆情引导智能代理模型]," *National Defense Technology 国防科技* 40, no. 3, June 2019, pp. 73-77.
[33] Chang Chengyang [常城扬], Wang Xiaodong [王晓东], and Zhang Shenglei [张胜磊], "Polarity Analysis of Dynamic Political Sentiments from Tweets with Deep Learning Method [基于深度学习方法对特定群体

推特的动态政治情感极性分析]," *Data Analysis and Data Discovery 数据分析与知识发现* 51, no. 3, March 2021, pp. 121-131. The study examined the Twitter posts of John Bolton, Donald Trump, Mike Pence, Robert O'Brien, Mike Pompeo, Steve Mnuchin, Frank Palone, Eric Swalwell, Richard Blumenthal, Joe Biden, Adam Schiff, Bernie Sanders, Nancy Pelosi, Gretchen Whitmer, Kamala Harris, Lawrence Summers, Andrew Cuomo, Sally Yates, Maria Cantwell, Edward Markey, and Elizabeth Warren.

[34] For a succinct explanation of this concept, see Joe Slowik, "Full-Spectrum Information Ops for Critical Infrastructure Attacks & Disruption," Cyberwarcon, November 19, 2019, https://www.youtube.com/watch?v=n7XqxRXwFZ4.

[35] Li Jidong [李继东] and Chen Zhou [陈舟], "On Strategic Cyber Warfare [试论战略网络战]," *China Military Science* 2017, no. 6, p. 55.

[36] Phillip C. Saunders and Joel Wuthnow, "Large and In Charge: Civil-Military Relations Under Xi Jinping," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms* (Washington, DC: NDU Press, 2019)

[37] James Mulvenon, "So Crooked They Have to Screw Their Pants On – Part 3: The Guo Boxiong Edition," *China Leadership Monitor* 48 (Fall 2015), accessible at https://www.hoover.org/sites/default/files/research/docs/clm48jm.pdf.

[38] Zach Dorfman, "Tech Giants Are Giving China a Vital Edge in Espionage," *Foreign Policy*, December 23, 2020, https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/.

[39] Zuo Juan [左娟] and Jia Jie [贾杰], "Thoughts on Constructing and Strengthening Network Militias" [加强网络民兵建设的思考], National Defense [国防], no. 3 (2019), pp. 58-59.