Chapter 8

Cyber Warfare Capabilities of the PLA Strategic Support Force (SSF)

Tsung-Han Wu, Chia-Ling Hung*

I. Introduction

The PLA Strategic Support Force (SSF) is responsible for military informationization construction and the defense in cyberspace. According to Xi Jinping's New Three-step Development strategy on the national defense and military development for the era on the 19th National Congress of the Chinese Communist Party, October 18, 2017, it is necessary for the PLA to ensure the realization of basic mechanization and high-degree informationization by 2020, basic modernization of China's national defense and military services by 2035, and the transformation of China's military into a world-class military by the mid-21st century.[1] Regarding cyberspace, on the first Central Cyberspace Affairs Commission meeting in 2014, Xi Jinping has said, "Without cybersecurity, there is no national security. Without informationization, there is no modernization."[2] In July 2019, a white paper entitled "China's National Defense in the New Era" says cyberspace is part of China's sovereignty and major interest in national security; it

* Tsung-Han Wu, Assistant Research Fellow, Division of Cyber Security and Decision-Making Simulation, Institute for National Defense and Security Research; Chia-Ling Hung, Assistant Research Fellow, Division of Cyber Security and Decision-Making Simulation, Institute for National Defense and Security Research.

1 "How to Accelerate National Defense and Military Development? Xi Jinping Emphasizes New Three-steps Strategy," *cpcnews.cn*, March 11, 2021, http://cpc.people.com.cn/xuexi/BIG5/n1/2021/0311/c385474-32049007. html.

2 "Xi Jinping in Charge of China's Cybersecurity," *BBC Chinese*, February 27, 2014, https://www.bbc.com/zhongwen/trad/china/2014/02/140227_china_xi_web_security.

also listed nuclear power and space as high points of China's military strategy. The white paper also indicates that the SSF is importantly responsible for new types of war capabilities. Based on the strategic requirements for system integration and Military-Civil Fusion (MCF), the development of a new type of war capability should be sped up and integrated.[3] All these statements speak of the importance of the SSF.

For a long time and due to data sensitivities, not much was known about the true face of the SSF. While many researchers have put piecemeal information together, knowledge was still fragmented, let alone the whole landscape. Occasional reports or articles published in academic journals focused on the organization, yet many of them were with few details on technologies or techniques.[4] This paper seeks to add to this gap. It examines the SSF by focusing on cyber warfare and cyber operation capabilities. Recent examples of possible operations are provided, and the most updated research literature is summarized.

II. The SSF and its Cyber Warfare Department

The PLA SSF was founded on December 31, 2015, as the PLA's fifth force along with other ground force, navy, air force, and rocket force. The establishment of this additional force signals the PLA's integration of space, cyber, electronic, and even psychological elements into a same battlefield framework. According to the introduction of the Chinese Communist Party's media, the SSF provides the PLA with the "guarantee for information support and strategic support" by serving as an

---

3 "China's National Defense in the New Era (full text)," *The State Council Information Office of the People's Republic of China*, July 24, 2019, http://www.scio.gov.cn/ztk/dtzt/39912/41132/41134/Document/1660318/1660318.htm.

4 John Costello and Joe McReynolds, China's Strategic Support Force: *A Force for a New Era* (2018, Washington: National Defense University Press); Rachael Burton and Mark Stokes, *The People's Liberation Army Strategic Support Force Leadership and Structure* (2018, Project 2049 Institute); Elsa Kania and John Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review (2018)*, pp. 105-121; Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019," *China Brief*, Vol. 19. No. 10, May 2019, https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

"information umbrella" for the whole PLA. It will "integrate into the operation of ground force, navy, air force, and rocket force throughout the war". To be specific, the core mission of the SSF is to engage in battles (strategically) and assist (as support) different forces in joint operations via the cyber and electromagnetic approaches. These operational tasks include reconnaissance, prewarning, communications, command, control, and navigation to achieve victory in warfare.[5]

While the SSF is set up as a military force at the same level as China's ground force, navy, air force, and rocket force, given that it is under the Central Military Commission (CMC) Joint Battle Command Center and also framed by the concept of "the CMC exercising overall leadership, the TCs [Theater Commands] responsible for military operations and the services focusing on developing capabilities," its actual role in the leadership system would change according to the nature of tasks.[6] On the surface, the SSF only provides support and protection. In reality, the initiation of attacks from its intelligence personnel and troops of hackers is rather impressive. Due to the PLA's increasing emphasis on information warfare, psychological warfare, and cognitive warfare, the SSF undertakes relevant tasks.[7] It is worth noting that the SSF is also one of China's cyber warriors, along with the Ministry of Public Security, the Publicity Department of the Communist Party of China, and the Militia of China.

The foundation of the SSF involved the consolidation and integration of the PLA's multiple departments and personnel before and after Xi Jinping's initiation of military reforms. Referring to the media reports and the previous

---

5 Yue Chiou, "Expert: Strategic Support Force (SSF) Throughout the Warfare as Key to Victory," *people.cn*, January 5, 2016, http://military.people.com.cn/BIG5/n1/2016/0105/c1011-28011251.html; Guang-hui Ni, "Unveil the mystery of China's Strategic Support Force (SSF) (perspective and deepening of national defense and reforms of the military)," *people.cn*, January 24, 2016, http://military.people.com.cn/BIG5/n1/2016/0124/c1011-28079245.html.

6 Ying-Yu Lin, "Mission and Scale of China's Strategic Support Force (SSF)," *Prospect & Exploration*, 15(10), 2017, p. 105.

7 Ching-an Wang, "Development of Chinese Cyber Warriors as Threat to Our Military," *Journal of Army Communication Electronic Information*, 127, April 2017, pp. 4-26; "Exploration of PLA Strategic Support Force's Capability in the Context of China's Integrated Network and Electronic Warfare," *Navy Professional Journal*, 54(3), June 2020, pp. 81-92; Changhee Park, "Evaluation of Informatized War Capabilities of the People's Liberation Army: A Scenario of Taiwan," *National Defense Journal*, 36(2), June 2021, pp. 1-50.

studies, the SSF consists of the Aerospace System Department, Network System Department, Electronic/ Electromagnetic System Department, and Military Intelligence Department. Under these departments there are sub divisions which work individually and cooperate with each other. In general, the purpose is to use information technology to link all battle forces for a comprehensive warfare system. Currently, the PLA considers the pursuit of the commanding elevation in cyberspace and across the electromagnetic spectrum an important means of obtaining military advantages. Therefore, the SSF is essential for the PLA's integration of network and electronic warfare.

The Network System Department, formally established in July 2017 as part of the SSF, is responsible for military defense and offense in cyberspace. This department is an integration of the General Staff Department (GSD) Technical Reconnaissance Department (GsD 3rd Department) previously in charge of radio surveillance and reconnaissance, GSD Electronic Confrontation Department (GsD 4th Department) in charge of radar systems, and GSD Informatization Department (GsD 5th Department), whose "information security bureau" was in charge of military defense and offense in cyberspace. In line with this, it is believed that the 12 operational units and troops previously under the Third Department of the People's Liberation Army's GSD are now part of the SSF. According to prior reports by the Kanwa Defense Review, the unit "information warfare force directly under the headquarters" is responsible for gathering the PLA's hackers to develop viruses and logic bombs for cyberattacks. In brief, the Network System Department's activities include R&D, reconnaissance, defense, and offense as a complete link.[8] The basic structure of the SSF and other cyber troops is shown in Figure 8-1.

Neither of the first two commanders in chief of the SSF (i.e., Gao Jin and Li Fengbiao) comes from the information or communications backgrounds, whose appointments may be due to tenures or the PLA's overall planning. However, this is no longer the case. Ju Qiansheng, the commander in chief since July 5, 2021, has

[8] Jun-jie Yin, "On Cyberwars, Kanwa: more hacker troops," *Central News Agency*, January 4, 2016, https://www.cna.com.tw/news/acn/201601040303.aspx.

a technical background, who previously served as the deputy head of the Technical Reconnaissance Department and commander of the Network System Department of the SSF. Highly proficient in cyberwars, his appointment arguably signals the SSF's increasing focus on professional leadership and further integration of internal resources to strengthen concerted battle actions and establish battlefield advantages.

<table>
<tr><td colspan="9">Central Military Commission of the Communist Party of China</td><td>Other departments</td></tr>
<tr><td colspan="9">Army Strategic Support Force</td><td rowspan="3">Other cyber warriors including the Militia, Internet commentators and opinion leaders, and cyber police</td></tr>
<tr><td colspan="2">Aerospace System Department</td><td colspan="2">Network System Department</td><td colspan="2">Electronic/ Electromagnetic System Department</td><td colspan="3">Military Intelligence Department</td></tr>
<tr><td colspan="8">12 bureaus under the Third Department of the People's Liberation Army's General Staff Department</td><td>Others</td></tr>
<tr><td>Unit 61398 (the U.S. as the main target)</td><td>Unit 1486 (western countries as the main target)</td><td>Unit 661419 (Japan as the main target)</td><td>Unit 78020 (Southeast Asia as the main target)</td><td>Unit 61726 (Taiwan as the main target)</td><td>Unit 61786 (Russia and Central Asia as the main target)</td><td>Unit 69010 (Central Asia and Southeast as the main target)</td><td>Other units</td><td>(Such as information war force under the headquarters, Base 311)</td><td></td></tr>
</table>

Figure 8-1 Structure of Strategic Support Force and other Cyber Warriors

Source: Compiled by the author.

III. SSF's Cyber Warfare Techniques and Recent Cases

Cyberwarfare might engage in a series of techniques and tactics that works with physical battles. It can be an influential determinant of victory or defeat in modern warfare. Cyberattacks may come at different intensities for different purposes—it may be for intelligence gathering, restricting the target's activity, or creating more advantages by cutting off the opponent's ability to access networks and information

systems. With horizontal integration of the intelligence, electronics, and cyber divisions previously under the General Staff Department, the PLA SSF has mastered different cyberattack techniques and can mix and match these techniques. These capabilities have posed a grave threat to Taiwan's government agencies, key infrastructure, and industry supply chains.

In the military domain, the PLA's threats to Taiwan's cyberspace, electromagnetic spectrum safety, and military C4ISR must not be understated, given its growing digitalization of platforms, equipment, and weapon systems. In the meantime, the SSF is also tasked with information warfare, psychological warfare, and cognitive warfare. Disinformation has recently become a highly emphasized element of cyber defense.[9]

The ways the SSF initiates cyberattacks are not dissimilar to most cybersecurity and information security incidents. The major approach involves identifying possible vulnerabilities by collecting relevant information of the targets and then acquiring important and confidential intelligence according to requirements. It may also be the invasion of the target's system by implanting malware or direct attacks on the software loopholes previously detected to destroy the system. Below are some examples of the techniques:

Phishing: This is a type of social engineering. It is the acquisition of the target's confidential emails by cheating with electronic communications, usually via emails or fake websites.

Ferry: This attack is primarily done by entering the physically isolated networks via mobile devices to steal data or engage in other malicious activities. Ferry is often accompanied by Trojan horses.

Distributed denial-of-service attack (DDoS): The purpose is to disable the target from continuing to provide services. Attackers use a large number of computers (invaded in advance) for simultaneous connection and send a hefty number of

---

[9] Gui-hsiang Wen, "Disinformation Seeks to Tear Taiwan Apart. President: Everybody Stays Alert of Cognitive Warfare," *Central News Agency*, April 16, 2021, https://www.cna.com.tw/news/aipl/202104160089.aspx; Kai-hsiang You, "Ministry of Justice Investigation Bureau's Video Deliberately Distorted. Scholars: PLA ups Its Cognitive Warfare Techniques," *Central News Agency*, April 18, 2021, https://www.cna.com.tw/news/firstnews/202104180076.aspx.

packets to block and paralyze the network to overload the system and make normal functioning impossible.

Great Cannon: Derived from the Great Firewall, this initiates distributed denial-of-service attack (DDoS) mainly by hijacking web traffic.

Advanced persistent threat (APT): This attack is based on prior observation and analysis of the target over a long period in order to stay on top of the target's dynamic information and initiate customized attacks. Attackers often resort to multiple and complicated techniques, including social engineering, by invading and penetrating possible loopholes. APT attacks may be a long, secretive process in multiple stages.

The process of initiating psychological warfare or cognitive warfare is also similar to that of general cyberattacks. The difference is that the former aims to influence the audience's psychological status or change the audience's perception by collecting information with specific disseminating techniques. As far as the SSF is concerned, network, electronic, and psychological warfare are interrelated and can work in conjunction.

Psychological warfare	Target the objective	Lurking and intelligence stealing from the objective	Release disinformation (/ true) information	To influence the target audience
Cyberattacks	Target the objective	Lurking and intelligence stealing from the objective	Various types of cyberattacks	To influence the target audience

Figure 8-2 The Path Diagram of Psychological Warfare and General Cyberattacks

Source: Compiled by the author.

Limited by data source, this paper does not intend to pinpoint the techniques and steps and specify the victims, incidents, and objects targeted by the attacks from the SSF. On the other hand, below we provide a list of cyberattacks that the SSF might have been possibly involved in since 2020 based on relevant information security reports or media coverage. It is worth mentioning that these cyberattacks may not all be operated by the SSF alone. Instead, these may be joint attacks from

mercenary hackers for hire or other state-owned or -sponsored cyber warriors. The final section provides a summary of the advanced persistent attack (APT) groups possibly related to the Strategic Support Force.

The first case in point was the ransomware attacks in May 2020 on CPC Corporation Taiwan and Formosa Plastics. The timing was sensitive because it was close to the presidential inauguration ceremony dated on May 20. After the probe by the Ministry of Justice Investigation Bureau, it was believed to be the work of the Chinese hacker organization APT 41 (also known as Double Dragon; Barium; Winnti; Wick Panda; Wicked Spider). This organization is thought to be highly related to the Strategic Support Force and meant to demonstrate the capability in neutralizing Taiwan's essential services to create panic. It was very much of a show of muscle and warming.[10] In June 2020, Prime Minister of Australia, Scott Morrison, openly said that Australia had been under complicated, large-scale cyberattacks from "national" hackers for months, where both government agencies and private companies were targeted. While Mr. Morrison did not specify the name of the attacking country, most reports believed it was China.[11] In October 2020, the media reported that the Chinese hacker organization RedEcho attacked India's electric grids and caused a blackout in Mumbai. It was when the border row turning to tense between China and India, and there was a standoff between the Chinese and the Indian armies. Further, it was generally believed that the hacker organization was meant to intimidate the Indian government. The reports by information security companies indicate that there are many similarities in the behavior of RedEcho and APT41.[12]

In March 2021, Microsoft exposed the initiation of a zero-day attack by the Chinese hacker organization Hafnium on the loopholes of the Microsoft Exchange Server. In the middle of July, the U.S. and its allies, including the Five Eyes,

---

[10] Qian-ru Weng, "Ministry of Justice Investigation Bureau Discloses the Full Results of the Probe into Ransomware Attach on Formosa Plastics," *iThome*, August 12, 2020, https://www.ithome.com.tw/news/139331.

[11] "Australia Cyberattacks: PM Morrison Warns of 'Sophisticated' State Hack," *BBC NEWS*, June 19, 2020, https://www.bbc.com/news/world-australia-46096768.

[12] "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," *Recorded Future*, February 28, 2021, https://www.recordedfuture.com/redecho-targeting- indian-power-sector/.

European Union (EU), North Atlantic Treaty Organization (NATO), and Japan, condemned the China government's irresponsible and malicious cyber activities around the world. Subsequently, four Chinese hacker suspects were prosecuted. The U.K.'s National Cyber Security Centre said in a statement that the State Council of China is related to the hacker organization Hafnium that attacked the Microsoft Exchange Server. It was also specified that China's Ministry of State Security is behind the two hacker organizations, APT31 and APT40.[13]

Numerous psychological and cognitive warfare cases attempt to sabotage Taiwan's image or its diplomatic relations by manufacturing international incidents. In April 2020, many fake accounts tweeted about the Taiwanese people's apology to Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization. It was later proven to be a plot and a scam by Chinese netizens. In December 2020, there was a fake official document pretending to be a request from the Ministry of Justice Investigation Bureau to the Office of the President for cooperation with the U.S. to drive a democratic revolution in Thailand. This request was then later proven to have come from Mr. Liu, who went to China for training by the Internet Water Army. In September 2021, the information security company TeamT5 was said to have been instructed by the Taiwan government to illegally collect the personal data of the Japanese people and confidential information of important business figures, proven to be online disinformation propaganda from China.[14]

The number of information security incidents in the world broke records again and again during the past year, and it seems that the attacks from China's cyber warriors have become more frequent and aggressive. As the world is caught in the

---

[13] John Hudson and Ellen Nakashima, "U.S., Allies Accuse China of Hacking Microsoft and Condoning Other Cyberattacks," *Washington Post*, July 19, 2021, https://www.washingtonpost.com/national-security/microsoft-hack-china-biden-nato/2021/07/19/a90ac7b4-e827-11eb-84a2-d93bc0b50294_ story.html.

[14] Yen-fen Huang, "China's New Trick in Cognitive Warfare! Targeting Taiwanese Information Security Company and Manufacturing Fake News to Incite Disharmony between Taiwan and Japan Governments," *iThome*, September 23, 2021, https://www.ithome.com.tw/news/146834; Bo-wen Hsiao, "Taiwanese Distributes Fake News from Chinese Cyber Warriors. First Cyber Case in National Security," *Central News Agency*, December 11, 2021, https://www.cna.com.tw/news/firstnews/202012110028.aspx; Bo-wen Hsiao, "Chinese Netizens Pretend to be Taiwanese Apologizing for Attacking Tedros Adhanom Ghebreyesus," *Central News Agency*, April 10, 2020, https://www.cna.com.tw/news/firstnews/202004100033.aspx.

competition between China and the U.S., cyberspace has been already a heated battlefield.[15]

Table 8-1 APT Groups Possibly Associated with the SSF

Name	Target Areas or industries	Target Profiles	Attacks to Taiwan
APT1 (61398)	Government, national defense, NGOs, academics, critical infrastructure, entertainment, high-tech	Multi-disciplinary but mostly focusing on political, economic, and military intelligence	Yes
APT2 (61486)	Government, academics	Focusing on satellite and aviation industries	
APT3	National defense, aviation, space, architecture, manufacturing, high-tech, telecommunication, transportation	Focusing on companies in cutting edge domains	
APT10 (menuPass)	Government, national defense, aviation, space, energy, finance, medicare, pharmaceuticals, high-tech, media, telecommunication	Mainly targeting governments and corporates, particularly Japanese	Yes
APT18	National defense, aviation, space, architecture, engineering, education, medicare, high-tech, telecommunication, biotech	Mostly targeting governments, corporates, and human rights groups	
APT19 (a.k.a. Deep Panda)	Government, national defense, energy, education, finance, telecommunication, manufacturing, high-tech, and medicare	Focusing on governments and national defense domains. Mostly targeting at advisory groups and political dissidents	

[15] Nicole Perlroth, "How China Becomes the Main Cyber Threat to the U.S.," *NY Times Chinese*, July 20, 2021, https://cn.nytimes.com/technology/20210720/china-hacking-us/zh-hant/.

Name	Target Areas or industries	Target Profiles	Attacks to Taiwan
APT26	Government, NGOs, aviation, space, national defense, energy, finance, telecommunication, food & agriculture, medicare and healthcare	Focusing on competitive companies in aviation, national defense, and energy	
APT40	Government, national defense, engineering, manufacturing, shipping, logistics	Focusing on domains related to maritime technologies. Thought to be closely associated with the Chinese navy	
APT41 (a.k.a. Barium, Winnti, Wicked Panda, Wicked Spider Group)	Government, national defense, architecture, education, energy, medical science, high-tech, manufacturing, petrochemicals, retail, telecommunication, transportation, entertainment	Multiple disciplines. Noted rather active when the Anti-ELAB Movement was ongoing in Hong Kong	Yes
Blacktech	Government, architecture, finance, media, medicare & healthcare	Mostly focusing on East Asia	Yes
Tonto Team	Government, national defense, finance, media, information technology	Mostly targeting Korea, Russia, and Japan before 2019. Later targeting Mongolia and Russia	Yes
Mustang Panda	Government, NGOs, aviation	Mostly targeting non-government organizations. Often using the Mongolian language	Yes

Name	Target Areas or industries	Target Profiles	Attacks to Taiwan
RedDelta	Government	Mostly targeting government agencies. Found in 2020 to frequently attack Vatican and Catholicism related organizations	

Source: Compiled from Gulshan Rai, "Cyber DNA of China-Deep," Focused and Militarized, *Vivekananda International Foundation*, March 23, 2021, https://reurl.cc/1oeR7W; Adam Hlavek, "The China Threat, In Brief," *IronNet*, January 10 2021, https://reurl.cc/r1LWAk; "Groups," *MITRE/ ATT & CK*, https://reurl.cc/95V8qn; "Advanced Persistent Threat Groups," *MANDIANT*, https://reurl. cc/EZGdvR; APT list, CYBER INTEL MATRIX, https://reurl. cc/NZqe8Q.

IV. Conclusion

Cyberwarfare is taken by the PLA as a key to victory in information warfare. According to the Taiwanese Ministry of Defense's 2021 China Military Power Report, the PLA is now able to initiate soft kill, hard kill, and electronic attacks on the western region of the First Island Chain, blocking communication and blanking signals. The PLA traditional troops can also work with the cyber warriors to attack the global networks wireline and wireless. These capabilities have been sufficient to neutralize the R.O.C. Armed Force's air defense, command of the sea, and countermeasure capabilities. The SSF is obviously among the key contributors to the PLA's rapid development in terms of its capabilities. Thus, Taiwan's national defense is under serious challenge.[16]

The frequency of cyberattacks and the variety of attack techniques have risen since 2020. There is also an increasing wave of psychological attacks. Further, this paper found many incidents which attempted to damage the image of Taiwan's government and its relationship with its allies. To counter the challenges, Taiwan's

[16] Ching-lyu Yang, "National Security Crisis! Ministry of National Defense'2021 China Military Power Report' Revealed that PLA Has Already Had a Complete Grasp of Taiwan's Military Dynamics," *Newtalk*, September 1, 2021, https://newtalk.tw/news/view/2021-09-01/629400.

government units in national security are urged to respond carefully and embark on in-depth research on the Strategic Support Force.