The Role of PLASSF and China's Grand Strategy

Ying Yu Lin[1](林穎佑)

Adjunct Assistant Professor, Institute of Strategic and International Affairs National Chung Cheng University

1. Introduction

The People's Liberation Army (PLA) Strategic Support Force (PLASSF) is a new service formed in China's military reforms in 2016. It has a unique status in that it is directly subordinate to the Central Military Commission (CMC), not to any theater command. It is comprised of many special units assigned to major military organizations before the reforms. Notable examples included the space systems branch of the former CMC General Armament Department (GAD), cyber warfare units of the former CMC General Staff Department (GSD) Third and Fourth Departments, and command, control, communication, computer, intelligence, reconnaissance and

[1] Dr. Ying Yu Lin is Adjunct Assistant Professor at Institute of Strategy and International Affairs National Chung Cheng University in Chiayi Taiwan. He received Ph. D in Graduate Institute of International Affairs and Strategic Studies, Tamkang University. His research interest includes PLA study, Cyber security, Sea power. He can be reached via Email:singfredrb@hotmail.com.

reconnaissance (C4ISR) units of the former GSD Informatization Department. Compared with other services, including the army, navy, air force and rocket force, the SSF has quite limited resources. Other services have troops to deploy and weapons to showcase. Their troops have to travel a certain distance to reach training bases. The difference between the SSF and other services can be observed from open-source information. The SSF does not have troops that it could deploy. Its function is to provide combat units with intelligence that can help them conduct military operations. It is basically a support force. The SSF mainly operates in virtual space, which inevitably adds to the difficulty of collecting information and doing research on the service. [2]

According to relevant information, the SSF is composed of the space systems, network systems and electronic/electromagnetic systems departments, all of which are corps-grade components.[3] It also has a political commissar

---

[2] John Costello ,"China's Strategic Support Force: A Force for a New Era",Feb.15.2018
〈https://www.uscc.gov/sites/default/files/Costello_Written%20Testimony.pdf〉

[3] Ying Yu Lin, "The Implications of China's Military Reforms"(Mar.03.2016),***The Diplomat***, http://thediplomat.com/2016/03/the-implications-of-chinas-military-reforms .

system and discipline inspection and staff units. These components used to be units of different organizations. Whether there was any conflict between them and their former organizations and how they handed over their missions during the transition are subjects that have aroused the interest of scholars in the field of PLA studies over the past few years.

As stated in some media interviews, the SSF focuses its efforts on providing support to missions related to "military operations." Therefore, intelligence gathering, which used to be handled by the GSD or GAD, is now a task of the SSF because it falls into the category of military operations. On the contrary, missions not directly related to military operations or intelligence with no direct relevance to first-line troops are not likely to become a responsibility of the SSF. Therefore, whether the former GSD Second Department (Intelligence Department) has been incorporated into the SSP is a topic much discussed by scholars in the field. There is no definite answer since not much information can be available in this regard. After all, information about intelligence organizations is always kept secret by all countries.[4] However, given that the

[4] Joe McReynold, "Chinese Thinking on Cyber Deterrence", paper presented at the conference of " The PLA Prepares for Military Struggle in the Information Age: Changing Threats, Doctrine, and Combat Capabilities" (Taipei: CAPS-NDU-RAND 2013 International Conference on PLA Affairs, November 14-15,2013).

SSF is tasked with the job of "providing support to military operations," the former GSD Third and Fourth Departments should no doubt have been incorporated into the SSF. Space bases and astronauts subordinate to the former GAD must have been put under the control of the SSF as well. However, intelligence functions of the former GSD Second Department were considered to have been transferred only partially to the SSF. They included remote sensing and image analysis. But the most important functions, such as intelligence analysis and operations behind enemy lines, should be under the control of the CMC Joint Staff Department (JSD) Intelligence Bureau. The JSD is the successor to the GSD. [5]

2. Observation on training exercises and joint operations maneuvers involving SSF

Besides the Taiyuan base, the SSF has another base to execute missions related to electronic warfare, also an important task for the service. The base should be the "Luoyang Electronic Equipment Testing Center," also known as PLA No. 33 Testing and Training Base, in Luoyang, Henan Province. In the "Exercise Quenching Luoyang-2018A" in May 2018, a unit from the SSF served as the blue army, playing a part in electronic and electromagnetic attacks and

[5] U.S. Department of Defense, ***Annual Report To Congress :Military and Security Developments Involving the Peoples Republic of China 2017*** (Washington DC: US DoD, May.2017).pp.34-35.

counter-attacks initiated by the PLA Army (PLAA).[6] It shows that electronic warfare forces subordinate to the former GSD Fourth Department have been incorporated into the SSF, tasked with the same missions as before. However, video footages that have been made public show that part of the equipment used by those electronic warfare forces is sourced from the private sector. Whether it means that the PLA has problems getting sufficient supply has yet to be found out. On Oct. 14, 2018, the Central Theater Command and SSF jointly launched a training exercise in an area south of the banks of the Yellow River. The exercise revolved around the themes of reconnaissance and counter-reconnaissance, tracking and counter-tracking, deception and counter-deception, and countermeasures and counter-countermeasures. It was meant to train participating troops in a complex electro-magnetic environment, where their battlefield adaptability, survivability and support capability were put to the test, and the possibility of a cross-service joint realistic combat training mechanism was explored. [7] The

[6] "Exercise Quenching Luoyang-2018A: red and blue armies compete with each other for dominance in electro-magnetic space." Xinhuanet. May 16, 2018. Retrieved from http://big5.xinhuanet.com/gate/big5/www.xinhuanet.com/video/2018-05/16/c_129873557.htm

[7] "A brigade of Central Theater Command competes in an exercise with a SSF unit." China News Net. Oct. 14, 2018. Retrieved from

exercise should have taken place at the No. 33 Testing and Training Base. From the example above, we could infer that the SSF might have established an electronic warfare blue army at the base, similar to the specialized blue army specific to the Zhurihe training base. The base is an important electronic warfare training center.

In terms of joint operations, many training exercises, as described in media reports, involved requests by field forces for support from the SSF. It could be a main point of discussion for scholars in their studies on links between the command chain and integrated joint operations mechanism. For example, an exercise held by the PLA Rocket Force (PLARF) in February 2018 revealed the relationship between the PLARF and SSF. Media reports described the exercise as involving the following changes: transformation from single-service training into cross-service joint training, enhancement of coordination with other services in the deployment of ballistic missiles and air arms, joint air defense and joint support, and transformation from being "capable of intercepting missiles" to being "capable of fighting a battle." Media reports also mentioned phrases like "target room of a rocket force base," "highly efficient operation of a combat information support platform," and "locating the target and taking steps according to plan to activate a rapid operating system, select a tracking and positioning satellite and

http://www.chinanews.com/mil/2018/10-14/8649401.shtml

submit a report to a SSF unit asking for supply." After the rapid operating system calculates ballistic missile information, the battlefield situation room's operating system quickly verifies the information. With authorization from the base leadership, the information will then be transmitted to a ballistic missile brigade.[8]

A theater command joint operations command center should have no place for the SSF and first-line troops still have to go through a theater command to ask for support from the SSF. For example, after a landslide happened in Tibet on Oct. 13, 2018, the Western Theater Command Joint Operations Command Center responded to requests from local authorities for support. It subsequently looked into feasible solutions. The requests were for the SSF to take more satellite photos of a barrier lake formed in the wake of the landslide. The Western Theater Command Air Force also dispatched unmanned aerial vehicles (UAVs) to affected areas. The Tibetan Military Region quickly got itself ready for disaster relief missions.[9]

---

[8] "From being 'capable of intercepting missiles' to being 'capable of fighting a battle.'" China Youth Daily. Feb. 22, 2018. Retrieved from http://www.chinanews.com/mil/2018/10-14/8649401.shtml

[9] "Western Theater Command deploys troops to assist disaster relief missions around a barrier lake along Yalu Zangbu River." China Military Online. Oct. 18, 2018. Retrieved from http://www.81.cn/lj/2018-10/18/content_9316785.htm

This shows that the SSF is directly subordinate to the CMC and that theater commands ask for support from the SSF only when they need relevant intelligence. It is not clear for the moment whether the SSF takes the initiative to provide battlefield intelligence to theater command joint operations command centers in peacetime or whether the information is provided first to the CMC Joint Operations Command Center and then passed down to theater command joint operations command centers while the top leadership is planning theater campaign actions.

3. The impact of China's Cyber Security Law

On November 7, 2016, the Standing Committee of China's National People's Congress (NPC) voted to pass the Cyber Security Law, which is set to take effect from June 1, 2017. This legislation has several characteristics: providers of network products and services are not allowed to sell user data to third parties; online scams are subject to severe crackdowns by law enforcers; a network real-name registration system is to be clearly defined and enforced; the critical information infrastructure is to be put under protection; organizations or individuals outside mainland China are to be severely punished for attacking or damaging the critical information infrastructure within China; a network communication control is to be launched in the event of a major network security incident. The first few characteristics underscore China's strong intention to put Internet activities under its control, which becomes an

urgent need especially after online crimes in China contribute to the formation of an Internet dark industry chain in recent years -- a fairly large size of underground economy. [10]China suffers a tarnished reputation as a result. As China is on course to become an information powerhouse, online crimes will surely put it under great stress. All these concerns might have been the main reason behind China's determination to restore order on the Internet.

It is a double-edged weapon, however. As the Chinese government strengthens its control of the Internet, it represents that it will keep a closer watch on cyberspace. China initially took the Internet as part of the media, which it considered to be an ideological state apparatus. Newspapers, radio broadcasts, and television stations have been put under government control for this reason. Due to the fact that the Internet has some characteristics not so self-evident in traditional media (such as anonymity and fast transmission speed), the Chinese government uses technical control to manage information exchange between people within mainland China and foreigners outside the mainland. [11] The Internet real-name

[10] Jack Wagner, "China's Cybersecurity Law: What You Need to Kno w"June.01.2017, ***The Diplomat***, <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-nee d-to-know/> .

[11] IT Advisory KPMG China ,"Overview of China's Cybersecurity

registration system has thus become a necessity. But as the saying goes, “as virtue rises one foot, vice rises ten.” A huge business profit has grown out of criminal activities derived from the Internet real-name system. Because of the system, fake accounts and thefts of personal information become an increasingly valuable business. It is necessary to take these problems into consideration in the enforcement of the Internet real-name system.

In respect to Internet security, China’s Cyber Security Law stipulates that information companies should provide relevant data to state security agencies for the maintenance of national security and the prevention of criminal activities. Under the name of national security, the Chinese government is justified in enforcing Internet control as what it says is part of anti-terror efforts or fight against criminal activities. Even the U.S. has the Patriot Act to collect information within its territory. In the re-authorized provisions of the act, the U.S. government is authorized to have access to the digital information of any person ranging from bank to library records. It arouses concerns over possible infringement on personal privacy and human rights. The controversial provisions, after having been reauthorized by two presidents, became invalid in

---

Lawa”,Feb.2017

〈 https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf〉

2016. But chances for China to give up its control of the Internet are pretty low. In 2010, Google Inc. withdrew from the Chinese market because of its refusal to allow Chinese authorities to censor its digital data. Now that China has made such censorship become a legal requirement, it remains to be seen whether foreign businesses will choose to stay in or withdraw from the booming electronic commerce market in China.

As far as Beijing is concerned, cyberspace is a main domain for national development. Such intention can be seen in the National Information Development Strategy Outline released in June 2016. But as the Internet development is maturing, Beijing starts to strengthen its control, especially in respect to incidents that might concern national security or the reputation of the government.

4. China's efforts to gain international discourse right

Also noteworthy are China's efforts to enhance its "information discourse right" via hosting various kinds of international conferences related to the Internet and information industry. A most representative example is the 2016 World Internet Conference held in Wuzhen, China's eastern Zhejiang province. There are other examples like electronic commerce conferences,

The outline calls for informatization to penetrate into modernization and increasing the speed of releasing the huge

potential of informatization. It serves as a guide for China's informatization development over the next decade, providing a direction for China's information industry in the future. It draws up three phases of development for China. In the first phase, the core technologies of China's information industry are to partially reach the levels of advanced countries by 2020. The next phase is for China to establish by 2025 mobile telecommunication networks that are at the forefront of technology in the world and to overturn the condition of having to rely on foreign countries for core technologies. China is to help develop domestic companies with strong international competitiveness. In the third phase, China's informatization development is to lay foundation for a prosperous democratic civilization and the development of a modern socialist state. In the development of fifth-generation (5G) mobile telecommunications, China has even taken the lead to formulate communication protocols. It establishes China's status in the information industry, which represents China's growing grasp of future technologies that are equivalent to the core technologies mentioned in the National Information Development Strategy Outline.

5. Silent Invasion: China's Cyber Business Influence[12]

[12] Clive Hamilton, Alex Joske, *Silent Invasion：China's Influence in Australia* (AU: Hardie Grant 2018).

In order to gain an advantageous position ahead of other countries, China adopts a carrot and stick approach to carry out its strategy for Internet control while focusing its efforts on software and hardware development at the same time. China could use its strong economic power to achieve the goal, such as increasing the market share of its products and companies via consumer information products manufactured at cheap labor costs (such as mobile phones, wireless monitors, and routers) and the acquisition of foreign companies (such as Lenovo). In respect to software, the large market share of communication applications like QQ and WeChat leaves foreigners who want to communicate or trade with Chinese people with no choice but to use these applications. Chinese-made software and hardware might have been implanted with malware during production. After the passage of the Cyber Security Law, China has a better reason to ask information product manufacturers to plant snoopware on their products in the name of national security. Out of national security concerns, quite a few countries prohibit the use of electronic products made in China. Despite that, after a comparison of the cost-performance (CP) ratios of various products on the market, many foreign consumers still choose to buy Chinese ones. Meanwhile, foreign companies trying to set foot in the Chinese market find it necessary to compromise with the Chinese government over the issue. The potential profit that can be gained from the Chinese market is sizable,

after all. As meeting with the leaders of major U.S.-based information companies in Seattle during his visit to the U.S. in 2015, Chinese President Xi Jinping might be sending such message to them.

6. Using commercial means to achieve political goals

Hardware development is the basis for a nation's computer network strength, also a cradle for hackers. But the discussion of information hardware now is not just about the informatization of a nation but also about the market share of its commercialized hardware. For example, U.S.-made consumer electronic products used to monopolize world markets. They were the number one choice in the world with assured quality. Now electronic products made in China at low labor costs are sweeping through the entire world at fast speeds. Besides mobile phones, routers and Internet equipment made in China have entered U.S. and European markets through a low pricing strategy. With its capital advantages, China increases its share of overseas markets through corporate acquisitions, acquiring at the same time more advanced information technology. For example, the personal computer (PC) business of U.S. computer giant IBM was bought by Lenovo, a Chinese company, in 2005 and has since been branded as Lenovo on world markets. Most recently, Chinese mobile phones have found their way into U.S. and European

markets through a low pricing strategy.[13]

But is it possible that these products contain drive-by downloads in firmware or pre-planted backdoors? Or are their built-in systems inflected with malware that sends user information to hackers? These concerns are the main reasons for the U.S. to restrict the use of peripheral equipment provided by Chinese telecommunications service providers like Huawei Technologies Co. and ZTE Corporation. Although Chinese-made mobile phones have pricing advantages, test reports show that they are likely to leak user information. Despite the security concerns over Chinese-made mobile phones, quite many consumers still choose to buy them because of their cost-performance (CP) ratio. This leaves some room for possible malicious attacks in the future.

Software development is also an area where nations vie with each other bitterly. Especially after the popularization of cloud applications and mobile devices, mobile phone security has become a focus of attention for every nation. In an attempt to prevent information leakage, China forbids the use of iPhones among high-ranking officials. The ban makes much more sense after Edward Joseph Snowden, a former contractor

[13] Robert Bebber " China's Cyber-Economic Warfare Threatens U.S." *Proceedings.* July.2017 〈https://www.usni.org/magazines/proceedings/2017/july/chinas-cyber-economic-warfare-threatens-us〉.

of the U.S. national security system, disclosed classified information about the U.S.' global surveillance programs, notably the Prism Program. It forced China to develop its own system so as not be subject to the influence of other nations.

In order to enforce Internet censorship and surveillance, China has blocked many IOS communications apps, a move which, combined with China's commercial advantages and the preferences of vast majorities of Chinese consumers, leaves foreign visitors with no other choice but to adopt Chinese communications apps, such as QQ in earlier years and the most popular WeChat now. But according to information security reports, all these apps contain vulnerabilities. Now that China has taken steps to combine wireless communications with mobile payment services, it means that every electronic transaction is likely to be monitored by the Chinese government.

The software competition also involves a wrestling for the control of networking platforms. It started with Google's withdrawal from the Chinese market in 2010 because of China's Internet surveillance. Other famous platforms like the social networking giant Facebook and video-sharing website YouTube have also been blocked because of China's Internet control policy. Different from other countries, China has a huge domestic market that has been growing dramatically in recent years. Along with China's rapid economic growth comes a drastic rise in the number of netizens. China's

domestic market is big enough to sustain the development of its own systems and websites.

Besides software systems, networking platforms are also a main fighting domain for on-line public opinion warfare. It is the reason why many Internet service providers and social networks were denied entry to the Chinese market. A variety of means are available for the control of the Internet. They include the Great Firewall under the control of China's propaganda system, the Golden Shield Project of China's public security system, and the Green Dam Project of the Ministry of Industry and Information. Of course, many Chinese Internet users can jump over these firewalls to have access to the outside world. But information circulating on the Internet is still under China's control. Many opposing opinions, once posted on the Internet, will be quickly removed or blocked. The websites where such opinions appear are characterized by crowd-gathering capabilities and links to search engines for any kind of information. It is only too natural for China to prevent such websites from circulating opinions unfavorable to it.

The competition in cyberspace, initially focused on software and hardware aspects, has shifted in recent years to the securing of discourse power. Discourse power in the information field depended in the past on the setting up of communication protocols and system specifications to facilitate the standardization of products and communication methods.

Generally speaking, the development was connected with the U.S., the birthplace of the Internet, one way or another. In recent years, however, China has reaping benefits from its economic growth, vast Internet users, and booming e-commerce.

That Chinese President Xi Jinping started his 2015 state visit to the U.S. on the West Coast sends the same message. While in Seattle, Xi met with the leaders of major U.S. high-tech corporations in the U.S.-China Internet Industry Forum organized by the Chinese side and co-organized by Microsoft. All the major players in the field were present at the forum to discuss the possible cooperation on the Internet and the prospective development of the information industry in China. The two areas are where U.S. information technology companies are highly interested in cultivating. Will U.S. companies make some compromises to China for the sake of seeking more cooperation with it and accompanying business interests? Is China still capable of maintaining Internet control while opening its market to foreign investors? All these issues will be the focus of attention in the Sino-U.S. information competition in the future.

Out of business concerns, U.S. companies' stance has taken a turn. First of all, Google, after having withdrawn from the Chinese market in 2010 because of China's Internet control, is coming back. During Google's absence from the Chinese market for a period of five years, Internet users in

China increased a lot, making China become the world's largest e-commerce market as represented by the mushrooming of third-party payment services like Taobao, Alipay, and WeChat Pay. Google has consequently missed huge business opportunities. In 2015, Google announced that it has worked with Chinese partners to return to China and launch the China version of its Google Play app. The move was aimed at sharing a piece of the big pie in China. Considering that Apple's iOS encryption is more complicated, the Chinese government intentionally limits the functions of iOS apps. This gives an edge to telecommunications operators using the Android operating system, also a chance for Google to return.

In May 2015, the U.S. Commerce Department, ascertaining Huawei's participation in activities that potentially undermine U.S. national security or foreign policy interests, decided to add the world's largest telecommunications equipment manufacturer to its "Entity List," banning companies in the U.S. from selling technologies or products to Huawei. The move is expected to disrupt Huawei's supply chain, very much like what the U.S. previously did to ZTE, another Chinese telecommunications giant. It means that the U.S. will not only stop importing Huawei products but also ban companies in the U.S. from exporting products to Huawei. It is considered by many analysts to have something to do with the on-going trade war between China and the U.S. As a matter of fact, the U.S. Congress started to question as early as in 2011

whether Huawei products would pose a threat to U.S. national security. Quite a few think-tanks and cyber security study groups then conducted researches into Huawei products, including handsets, routers, security monitoring equipment and other information items, to find that they were all capable of sending back data to servers in China. Seen from the perspective of China's national strategy, Huawei starts by gaining a foothold in the markets of certain specific countries by offering products at relatively low prices. After expanding its market shares in those countries, Huawei goes on to promote the specifications of its products so that those countries will have no choice but to cooperate with China in the building of their information infrastructure. Such kind of "Cyber debt trap," together with the employment of the tactic of using "economic leverage to gain political submission," is now seen more and more frequently in China's foreign diplomacy strategy.

7. Threats from digital products

In the realm of Cyber security, a country should acquire basic defensive and offensive hacking capabilities. A new front for Cyber warfare is the market share of a country's information products. The development of information products lays the foundation for a country to build its networking capability. However, current discussions about information products focus not just on technical aspects. They are more about market shares of commercialized products. For

example, consumer electronics products made by the U.S. used to be the top choices around the world, monopolizing the world market. Now Chinese electronics products made at low costs are quickly sweeping through global markets. In addition to mobile phones of Chinese brands, routers and network equipment made in China have also gained entry into global markets because of their relatively low costs. With the advantage of huge capital, China increases the overseas market shares of its products by mergers and acquisitions, even acquiring information technology in some cases. An earlier example is Lenovo's purchase of the personal computer (PC) business of IBM, formerly a PC giant in the world. The Lenovo brand is now present in markets around the world. Is it possible for these information products to have bugged firmware, be planted with backdoors or embedded with systems containing malware that automatically sends back user information to unknown servers. All these concerns cause the U.S. government to restrict use of network peripherals made by Chinese telecommunications companies.

Malware not only enables theft of data but also facilitates collection of user information. In this age of Internet of Things, all home appliances that can be connected to the Internet may become backdoors for intrusion by hackers or sensors for monitoring. For instance, the camera on a digital television may be used to watch the television owner's every move at home, while a robot vacuum cleaner could map the house of its

owner and record cleaning routes. These are real happenings. To keep watch on democratic activists or dissidents, China adopted early on the Golden Shield Project to monitor netizens, using in combination the Great Firewall to block all websites deemed “politically incorrect” by Beijing. With the progress in big data collection and artificial intelligence (AI) in recent years, China has established a facial recognition system to enforce social monitoring. For example, the Skynet system in a city can virtually monitor every citizen. The system has now been expanded to the countryside, becoming the Xueliang Project launched in 2018. It makes use of various types of cameras to monitor the public. All sorts of monitoring equipment exported by China to other countries may send back to China data of foreign citizens. These are the potential risks in using Chinese products.

Although freedom, convenience and security cannot be obtained at the same time, it depends on the user to make the right choice. However, most users do not have the same awareness. There are even instances of ignorance taken as omniscience in some organizations. It indicates a lack of information security awareness. In the public opinion warfare domain of this information age, all personal information will become part of the big data to be collected for analysis. Hostile countries may make use of both hardware and software to collect a vast amount of personal information about individuals of certain specific countries so that they could know those

countries' ethnic distribution and characteristics, customize misinformation for targeted ethnic groups, and launch digital and public opinion warfare accordingly to divide the opposing forces or incite internal rivalry within them. Such new type of warfare could be taken as a derivative of information threats.

8. Conclusion

Cyber security can't be achieved only by banning products of a certain brand. It also requires the support of relevant laws and government polices. Human factors are especially of vital importance. Many technology companies, for instance, have long forbidden employees to use phone in restricted areas, but leaks of classified information still occur from time to time. Cyber security incidents like a suspension of operations because of malware intrusions also happen. It shows that a mere ban on phones does not solve the problem. The key is in the cyber security awareness in a company or unit and among its members. If members of an organization, from leaders down to all subordinates, still think in terms of buying or banning certain equipment or software without developing a comprehensive cyber security awareness, they are curing only the symptoms, not the disease. New technology may provide a new way of stealing intelligence, but human weaknesses are usually the most vulnerable part. Social engineering involves taking advantage of people's trust to achieve goals by cheating. Therefore, besides enhancements in software and hardware protection, it is also imperative to strengthen cyber security

awareness.

In response, Taiwan should strengthen publicity efforts, provide correct information, and establish channels to clarify rumors and stop misinformation from being disseminated. The government should make public its cyber security policy orientations and relevant cyber security knowledge on a regular basis gain an advantageous position in cyber manage. As cyber security specialist Bruce Schneier as said, “(cyber) security is a process, not a product.”