Cybersecurity and Information Security: Force Structure Modernizations in the Chinese People's Liberation Army

Miranda Bass

Since 2012, the Chinese government under Chairman Xi Jinping has taken steps to assume the role of a global power, including a sweeping modernizing of its military, the People's Liberation Army (PLA), in order to transform it into a force capable of projecting power. Notably, in 2015, the PLA formed the Strategic Support Force as a separate service, concentrating all of its satellite and network operations forces, including cyber operations forces, into a single, high-profile organization. This policy choice to reorganize the PLA force structure reflects and reinforces the new preeminence of information operations in China's national security, the majority of which takes place in cyberspace.

Keywords: China, military, cyber, force structure, modernization, information operations, national security

Introduction

All militaries need to evolve commensurately with developments in military technology and the strategic and political goals of their society. The Chinese People's Liberation Army (PLA) was born as the military wing of the Chinese Communist Party (CCP). It has remained an army of the party ever since and has not transitioned into a national military. It began its first efforts at modernization under Chairman Deng Xiaoping in 1979 with the whole-of-society Reform and Opening movement and following a painful loss in the

First Lieutenant Miranda Bass, US Army is an MA candidate at Tel Aviv University.

Sino-Vietnamese War. As China has assumed a powerful global role over the past twenty years, the PLA has sought to expand beyond being a low-capacity, internally focused conscript army to becoming a formidable regional force. Both the goals of advancing global status and military modernization, nested therein, have accelerated under Chairman Xi Jinping since he took office in 2012. An integral part of the orientation and capabilities of a military is its force structure, which also evolves with modernization efforts. Force structure is a fundamental aspect of the composition of a military and a challenging area in which to introduce new systems due to bureaucratic resistance. Thus, any developments in this area are the result of long-term, high-level commitment and dedicated effort. Beginning in the early 2000s and particularly over the last five years, the PLA and Chinese government as a whole have taken major steps to codify and institute comprehensive cyber policy, culminating in a gargantuan modernization of its military force structure in 2015, including a total reorganization of PLA forces involved in cyber operations. The main thrust of this reorganization was the formation of the Strategic Support Force (SSF) 解放军战略支援部队 *jiefangjun zhanlue zhiyuanbudui* on December 31, 2015. This paper will detail the changes within the PLA and explain how the establishment of the SSF was a sound decision for China's goals in cyberspace and information management.

Cyberspace, Cyberattacks, and Cyber Defense

Cyberspace is a notoriously difficult term to pin down due to its manifold use in contemporary discourse. While the popular notion of a link between cyberspace and electronics is true, it is not the whole story. From a security perspective, a useful definition of cyberspace comes from its components, three layers resting one on top of the other: physical, syntactic, and semantic.[1] Every layer is necessary for cyberspace to exist as a whole and without one, the whole system would disappear, albeit perhaps only temporarily. The physical layer of cyberspace consists of the medium's tangible infrastructure, including wires and boxes filled with electronics that physically sit in various sites around the world. From a security perspective, the salience of the physical layer is the potential for an adversary to attack these boxes and cripple the ability of people and machines to operate in cyberspace.

1 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), 39.

The syntactic layer is unseen, occupied by the machines and protocols that facilitate all exchanges and operations in cyberspace. This layer is the domain of machine interaction, including routing and switching. Most hacking, which is a cyberspace interaction in which one party completes an action for its own benefit through the perversion of existing pathways to the detriment of other parties, takes place at the syntactic level. The semantic layer contains the vast majority of the data and interfaces that the typical user commonly conceives of as cyberspace in that it exists separately, although often adjacently, to the natural world. Unlike the syntactic layer, the semantic layer appears mostly in natural human language.

With a working definition of cyberspace, it is possible to turn to hacking, the twisting of the medium's intended pathways for human ends. The typical goal of hacking is to steal data, usually from another user or system's machine.[2] In security terms, these cyber activities are known as computer network exploitation (CNE) and can happen between any type of actor. A state may, and they often do, steal data from another state, organization, or individual to advance its national goals; corporations steal intellectual property from each other; and individuals steal data from any entity to commit identity theft, for ideological motivations, or for any other potential goal a person might have. It is worth having a basic understanding of the general outline of CNE in order to discuss its ramifications in government and military force structure. Stealing data is non-rivalrous, meaning that its theft does not impede its free use unlike stealing an object like rocket launchers, and anyone or anything monitoring the system hosting the data may not realize that theft has even taken place.[3] CNE begins with the exploiting party obtaining unauthorized access of the target system, receiving the privileges, the level of access, of a user or administrator in that system. The exploiter then attempts to pilfer the desired data while evading detection to enable the highest chance of success. Due to the non-rivalrous nature of CNE, this outcome is entirely possible.

Fundamentally, CNE is espionage, which states traditionally have not considered an act of war prior to the rise of cyberspace. CNE does not deprive the user of full use of the machine; the user suffers no harm apart from losing information; and the law of war does not recognize espionage as *casus belli*, a cause sufficient to initiate a war.[4] A cyberattack often looks similar to CNE

2 Libicki, *Cyberdeterrence*, 14.
3 Libicki, *Cyberdeterrence*, 15.
4 Libicki, *Cyberdeterrence*, 23–24.

in its early stages, due to the realities of operating in cyberspace, but it has a different goal. A cyberattack is the deliberate disruption or corruption by an attacker, usually a state, of a target system of interest to another state. Similarly to CNE, after the attacking party gains the required privileges, it then proceeds by either disrupting the system so that it does not function properly, causing drastic, obvious, and immediate effects, or corrupting the system in subtle, even unnoticeable ways that may linger or reoccur.[5]

Commensurately to cyberattacks, cyber defense came into existence, albeit of a less thrilling character, as is often relegated to defense in security generally. The goal of cyber defenders is to render their system as impervious as possible to unwanted infiltration of any kind, be it CNE or a cyberattack. System managers can go to great lengths to ensure that a system has a high degree of security, but this outcome is ultimately not ideal for the system's users. The classic problem of security in cyberspace is the tradeoff between security and accessibility. Networked systems exist in order to facilitate user operation and interaction with other machines and the internet. This necessary openness, combined with the original conception and design of the internet as a borderless space largely without security measures, has created a situation in which cyber defenders are at a disadvantage.

States are by no means the only perpetrators of cyberattacks or pursuers of cyber defense, but states that invest heavily in this area are undoubtedly the most sophisticated type of actor due to their size, resources, and goals. National cybersecurity capabilities, encompassing the ability to attack, defend, and conduct espionage, vary widely between states based on the priority that the government has placed on developing this new tool. Although the wealthiest states have bolted ahead in their relative capabilities as with other technological innovations, cyber operations merit a paradigm different from the last major historic innovation in military technology, that of nuclear technology. In contrast to nuclear technological development, which was prohibitively expensive for the vast majority of states and certainly for non-state actors, cyber capabilities are radically accessible to any actor, including private individuals. Due to their immense resources and comparably complex targets, states have the most sophisticated capabilities, but the field is no longer restricted to the wealthiest states; even the poorest states can have

5 Libicki, *Cyberdeterrence*, 15–16.

an outsized effect, like North Korea. Critically, non-state actors can act independently and effectively as well.

Cyberspace is not merely the technological; rather, it is the tool of its users, meaning that any threat comes not from the machines but from the people who design and operate them.[6] Even today cyberspace is still reminiscent of the American West of old, a place vast, unmapped, culturally and legally ambiguous, terse, difficult to navigate, and largely up for grabs.[7] This environment is fertile ground for the innovation about how the world ought to be shaped, which actors and category of actors should be powerful, how communication ought to look, what truth is, and what liberty means. Despite or in conjunction with these possibilities, cyberspace still remains a reflection of the broader, non-cyber world and its power arrangements. Its main contribution to the structure and distribution of power is a lowered barrier to entry for an actor to achieve global relevance, which is no small innovation. In addition to lowered barriers to entry, actors in cyberspace enjoy the near-total irrelevance of spatial distance, net-speeds approaching lightspeed, and a higher degree of difficulty in definitively attributing a particular act to a specific actor. Another less intuitive distinction of cyberspace is that it is nearly impossible to know who will witness a given event, where and when they might see it, or how they might interpret it.[8]

Categories of Cyber Power in National Security

There are several types of cyber power in a national security conception.[9] The broadest is productive cyber power, the construction of discourse in cyberspace, which includes both reinforcing existing discourse and inventing and disseminating something new. Cyberspace uniquely facilitates discourse and its amplification with minimal barriers. Structural cyber power is the maintaining of existing power structures and enabling or constraining actors within these structures. Structural cyber power tends toward the anarchic, in particular enabling eye-catching vitriol and resentment of disaffection to flourish and propagate. Institutional cyber power is the control of cyberspace through institutions such as the Internet Corporation for Assigned Names

6 David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power* (London: International Institute for Strategic Studies, 2011), 13.
7 Betz and Stevens, *Cyberspace and the State,* 14.
8 Betz and Stevens, *Cyberspace and the State,* 40.
9 All of the following types of cyber power are derived from Betz and Stevens, *Cyberspace and the State,* 45–50.

and Numbers (ICANN), an American non-profit responsible for coordinating databases of names and numerical addresses on the internet. This type of cyber power also extends to informal institutions, namely, norms, which construct and are constructed by actors' behavior in cyberspace. The narrowest form is compulsory cyber power, which includes CNE and attacking to control a machine or network's behavior, preventing an actor from operating in cyberspace and similar operations of coercion.

All these types of cyber power are relevant to the military, which is a key body in a country's national cybersecurity policy and operations, although certainly not the only one. The link to the military of compulsory cyber power is self-evident, as it is often the military that executes such operations. The link to structural cyber power is relevant both in that structural cyber power broadens the threat possibilities, from primarily state actors or only the most highly organized and capable non-state actors to networked individual nodes acting with lowered barriers to entry. In short, cyberspace weakens the constraints of existing power structures with respect to which actors have access to impactful global interactions. Institutional cyber power is relevant to military power in that the norms of military operations in cyberspace are still being written. Thus, a military that seeks to create the rules of the game in its own interests, which is the case in every state that has the capability or aspiration for international influence, seeks to expand its own internal structural cyber power as well as that of its state in general. Productive cyber power is more unique in that it links the military realm of war with its political dimension by enabling an actor to mold discourse to its strategic advantage. Although this activity originates in the political realm, not the military, military organizations can still undertake operations in this line of effort and are indelibly shaped by them.

The traditional Clausewitzian definition of the object of war is the overthrow of one's enemy, rendering the adversary powerless. Based on this understanding, cyber power is a force multiplier, but not a substitute for physical force.[10] However, according to a soft power understanding of war using the model of Joseph Nye, the object of the conflict is persuasion, and cyber power could be strategically decisive in this framework; nonetheless, this definition is not quite as helpful. Cyber power is an increasingly critical complement to other more kinetic capabilities, but it certainly does not negate

10 Betz and Stevens, *Cyberspace and the State*, 86.

these capabilities or change the objective nature of war. What it does do, crucially, is give a weapon to the historically weak, militarily and politically. Over the last several centuries, the West has maintained its military and political power through a virtuous cycle of economic and political expansion. Since decolonization, however, its military power has achieved less effective and decisive results through kinetic action and weapons. To address this, Western states have changed tactics to utilize the allure of ideas, based on Nye's soft power mold, which has been successful.[11] Because of this reality, actors opposed to Western hegemony, particularly, illiberal regimes, now perceive the free internet and all of its discourse and information to be a knife at their throats.[12] Thus, it is a national security imperative for regimes in which authoritarianism and illiberal politics are the order of the day to control the flow of ideas. No major political entity has more thoroughly understood this imperative and acted accordingly than the CCP, in large part because the party developed from a totalitarian system amidst the throes of the twentieth century and has adhered to ideological purity including Marxist discourse control since its inception.

The question of how exactly the CCP has gone about controlling the internet, cyberspace, and information in general is beyond the scope of this paper. For these purposes, however, the CCP describes the potential of the internet as an engine of economic development, a vehicle for more easily creating and disseminating culture, a platform for social governance both by enhancing individual rights and facilitating government control, and a territory that demands national sovereignty just as land, sea, sky, and space do.[13] Beside the benefits, the party identifies the primary threat of cyber penetration to be challenges to Chinese political security, which is foundational to national development and the happiness of the people, by instigating social unrest. Cyberattacks threaten economic security and so-called harmful information threatens the security of traditional culture.[14] What follows is the structure of the PLA's cyber and information operations forces and, crucially, the military modernization project of 2015, how the

11 Betz and Stevens, *Cyberspace and the State*, 132.
12 Betz and Stevens, *Cyberspace and the State*, 132.
13 Office of the Central Cyberspace Affairs Commission, "Guo jia wang luo kong jian an quan zhan lue," *Zhongguo Wangxinwang*, December 27, 2016 (accessed December 10, 2019), http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.
14 Office of the Central Cyberspace Affairs Commission, "Guo jia wang luo kong jian an quan zhan lue."

modernization has reshaped those same forces, and why the change in force structure supports the party's military goals.

Before discussing technical military organization, it is necessary to understand the Chinese conception of cybersecurity, which, like so much Chinese thought, is different from the common Western understanding. The Western idea of cybersecurity in China is called network security 网络安全 *wangluo anquan*. This idea fits under the umbrella of the broader idea in China of information security 信息安全 *xinxi anquan*, which is more about content management; that is, censorship and control of information dissemination is the object of the semantic layer of cyberspace rather than network security or integrity *per se*.[15] A former chair of the organization that produced China's first cybersecurity policy document argued that information security was "necessary for social stability and socialist cultural and ideological development."[16] These words are not empty rhetoric. They are foundational to the CCP's national security concept and, in particular, its cybersecurity concept.

Informationization in the PLA

"Informationization" is the most accurate translation of the Chinese term 信息化 *xinxihua*, a guiding principle of the PLA's modernization and transformation from an internally oriented farmer's army into a power projector. To the extent that there is any civil society in China at all, it exists on the internet.[17] This poses a potentially critical threat to stability in China, which, according to the CCP, is based on the total absence of any discernable dissent or dissatisfaction with party rule. Chinese cyber policy began to emerge in the early 2000s from the State Information Leading Group (SILG) and State Council Information Office, two early organizations that worked on information security. The seminal policy piece is a SILG opinion from 2003 referred to as Document 27, which established China's national

15 Jon R. Lindsay, "Introduction—China and Cybersecurity: Controversy and Context," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 11.

16 Qu Weizhi, *China's Path to Informationization*, cited in Jon R. Lindsay, "Introduction—China and Cybersecurity: Controversy and Context," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 11.

17 Weizhi, *China's Path to Informationization*, 1.

cybersecurity policy for the first time in exclusively defensive terms.[18] In the following decade, a dense bureaucratic tangle of offices and institutions was responsible for disparate aspects of the creation and management of Chinese cybersecurity policy. Progress during this period was halting, as government attention was diverted to other priorities: first, planning for the 2008 Beijing Olympics and then the global financial crisis. In 2012, however, Chairman Xi took office and the CCP began to move toward increased social control and a less open society and to aspire to become a top global power. Upon taking office, Chairman Xi immediately began to reorganize government offices according to new policy priorities, and in 2014 the SILG became the Cybersecurity and Informatization Leading Group (CILG), which Chairman Xi personally led and continues to lead along with the other highest-ranking party leaders in the country. These staffing decisions raised the issue of military informationization to the highest level of importance in policy. PLA military doctrine is weighted heavily toward the offensive on the operational level, including preemptive strikes, and has a defensive orientation at the strategic-political level.[19] Functionally, this doctrine means that since the PLA cyber forces are engaged in operations short of outright war, they are highly active and aggressive. Cyber operations-specific doctrine emphasizes striking first in an armed conflict with cyberattacks to paralyze the adversary's command and logistics systems.[20]

Pre-Modernization Force Structure

By the first half of this decade, the PLA had developed a large complement of cyber-engaged and cyber-adjacent forces. The PLA General Staff Department (GSD), subordinate only to the supreme command authority (the Central Military Commission), was responsible for day-to-day joint operations, intelligence, strategic planning, operational requirements, training, mobilization, military diplomacy, and the security of senior leaders, making

18 Weizhi, *China's Path to Informationization*, 8.

19 Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 141.

20 Lindsay, "Introduction," 18.

it the cutting-edge driver of the PLA's future.[21] The GSD contained the 2nd, 3rd, and 4th Departments, notated as 2/PLA, 3/PLA, and 4/PLA, respectively.[22] 2/PLA was China's human intelligence (HUMINT) organization, conducting foreign intelligence collection from human sources. Their overt operations were conducted by a global network of defense attachés, selected for their analytical capabilities and language skills, and typically lacking conventional military experience.[23]

3/PLA was China's signals intelligence (SIGINT) organization which had its origins in pre-internet traditional SIGINT but by the twenty-first century was dealing with all forms of SIGINT. Its mission and operations consisted primarily of cyber reconnaissance and CNE.[24] 4/PLA was far more secretive and conducted more disruptive activities in the fields of electromagnetic warfare, information operations and warfare, and computer network attacks (CNA).[25] The PLA has three categories of cyber military operations, which it terms computer network warfare 计算机网络战 *jisuanji wangluo zhan*: computer network reconnaissance, which is CNE; computer network strike, CNA; and computer network defense (CND).[26] Within computer network warfare, doctrine articulates offensive operations as destroying adversary network systems, information, and degrading adversary operational effectiveness. Defense operations include protecting Chinese network systems, information, and the conduct of operations, essentially the converse of their offensive operations.[27]

3/PLA is of particular interest due to its high-profile cyber operations. It was the largest employer of top-tier linguists in the country in 2014 and engaged in advance computing, encryption, and decryption.[28] Its headquarters were

21 Mark Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 164.

22 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure."

23 Nigel Inkster, "The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 33.

24 Inkster, "The Chinese Intelligence Agencies."

25 Inkster, "The Chinese Intelligence Agencies."

26 Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," 143.

27 Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," 139.

28 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 164.

located in the Haidian district of Beijing, close to many of the highest-level government offices. 3/PLA command oversaw a headquarters unit, political department, logistics department, Science and Technology (S&T) Intelligence Bureau, S&T Equipment Bureau, and the 56th Research Institute, the PLA's oldest and largest computer science R&D institution.[29] Also under 3/PLA was the secretive Beijing North Computer Center (BNCC), responsible for cyber reconnaissance architecture design, technology development, systems engineering, and acquisition. BNCC was one of the first PLA organizations responsible for cyber operations in their twentieth-century infancy and contained ten subordinate divisions responsible for computer network operations (CNO), which include the full spectrum of CNE, CNA, and CND.[30] 3/PLA operational personnel and linguists received their training at specialized PLA universities.[31] Other cyber operations assets, termed Technical Reconnaissance Bureaus (TRBs), existed outside of 3/PLA. The three PLA services (PLA Air Force, Navy, and Second Artillery or Strategic Rocket Force) each had their own TRBs, as did each of the seven military regional commands. The PLA Air Force had three regional TRBs that monitored the activity of neighboring air forces, conducted airborne SIGINT missions, and conducted CNO that directly supported air force operations. The PLA Navy had two TRBs, one each for the northern and southern seas, and were likely occupied with ship-based SIGINT collection. 2nd Artillery also had its own TRB. The TRB serving each military regional command supported the command's operations. A detailed account of 3/PLA's operational bureaus and their activities follows addressing exactly in which operations the PLA cyber operational forces were and continue to be engaged.

3/PLA had direct authority over twelve operational bureaus, eight headquartered in Beijing, two in Shanghai, one in Qingdao, and one in Wuhan. These TRBs existed and operated independently of those under the services and military regional commands. 3/PLA also had a dedicated Hong Kong and Macao office.[32] The unit commander had a corps-level grade, and

29 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 166–167.

30 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 168.

31 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 169.

32 This and all bureau information is taken from Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 170–172.

the bureau directors and their equally powerful political commissars had division-level grades, overseeing between six and fourteen offices. First Bureau, headquartered in Haidian with 3/PLA headquarters, was one of the foremost national authorities on CNO and information security. Second Bureau, primarily in Shanghai, targeted the United States and Canada in pursuit of political, economic, and military intelligence while also maintaining professional affiliations and research relationships with numerous academic institutions in the area. Third Bureau, headquartered in Beijing, had at least thirteen geographically dispersed subordinate units, indicating that the Third Bureau was likely occupied with collecting from line-of-sight radio, direction finding, and emission control and security. Fourth Bureau was headquartered in Qingdao, a port city, and focused on Japan and the Korean Peninsula, with offices up and down the coast. Fifth Bureau was also headquartered in Beijing, with offices in Heilongjiang, one of the northernmost provinces of China, and had a Russia mission. Sixth Bureau was headquartered in Wuhan, in central China, and had offices spread across the whole region, indicating a Taiwan and South Asia mission. Seventh Bureau was also headquartered in Haidian and employed some English translators. It participated in CNO, but its mission was unclear. Eighth Bureau was adjacent to 3/PLA headquarters and focused on Europe and perhaps the Middle East and Latin America as well. Ninth Bureau was the most opaque, headquartered just outside Beijing, and was responsible for computing, analysis of strategic intelligence, database management, and audiovisual technology. Tenth Bureau was headquartered in Beijing and had a Central Asia or Russia mission, perhaps specifically in the fields of telemetry, missile tracking, and nuclear testing. Eleventh Bureau was also headquartered in Beijing and had a Russia mission. Twelfth Bureau was headquartered in Shanghai and had a satellite mission, focused on space-based SIGINT.

3/PLA had the lead role in CNE and CND, but the lead CNA organization was likely the more secretive 4/PLA, which held the formal name of the Electronic Countermeasures and Radar Department. 4/PLA was responsible for radar joint operational requirements development and electronic countermeasures (ECM), including satellite jamming and counter-stealth radar systems.[33] The organization included at least four bureaus, an advisory group, and the 54th

33 Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," 174.

Research Institute. The ECM Bureau planned, programmed, and budgeted for ECM systems; the Technical Equipment Bureau was occupied by acquisition; and personnel assigned to 4/PLA received specialized training in a dedicated PLA university. There were at least two known operational ECM brigades, and they were likely responsible for electronic reconnaissance satellite ground receiving stations that supported joint targeting as well as satellite jamming.

Post-Modernization Force Structure

All of these organizations were transformed, however, with a decision that took effect on January 1, 2016. Instead of the numerous, more dispersed organizations operating underneath the GSD, all cyber and information operations assets were placed under the Strategic Support Force (SSF) as part of a general force-structure overhaul. The seven military regional commands were reorganized into five theater commands, and the new theaters were awarded the command authority that formerly belonged to the individual services in order to better facilitate joint operations like most expeditionary militaries.[34] This force structure reorganization removed TRBs that had been directly subordinate to the services and military regions and placed them under the authority of the SSF. The SSF is the PLA's fully integrated joint information warfare force, providing the PLA with strategic information using primarily network-based and space-based capabilities, and these are its two primary departments.[35] These capabilities include communications, navigation and positioning, intelligence, surveillance and reconnaissance, and protecting PLA information infrastructure.[36] The SSF conducts information operations in space and cyberspace, electronic warfare, and psychological operations. Thus, by nature it is not a dedicated cyber operations force, but, rather, a dedicated information operations force that operates primarily in cyberspace as well as other mediums, commensurate with the Chinese understanding of information security and cyberspace. The GSD and other

34 Xinhua News, "Xin shi dai de zhong guo guo fang," *Xinhuanet*, July 24, 2019 (accessed December 10, 2019), http://www.xinhuanet.com/politics/2019-07/24/c_1124792450.htm.

35 Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019," *Jamestown Foundation China Brief*, May 29, 2019 (accessed October 9, 2019), https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

36 Ni and Gill, "The People's Liberation Army Strategic Support Force."

organizations housing forces that had similar mission sets were all disbanded at the end of 2015.

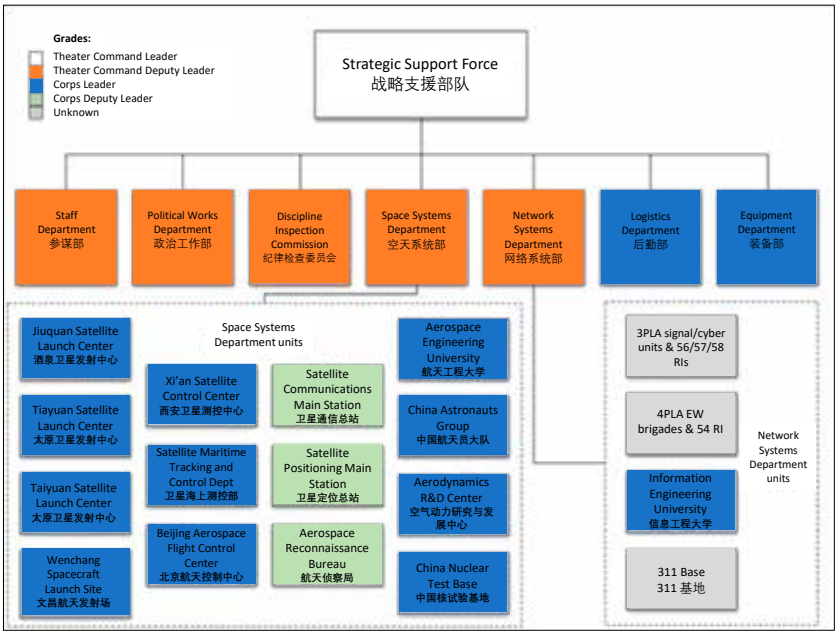

Figure 1. The Strategic Support Source

Source: Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019," *Jamestown Foundation China Brief*, May 29, 2019 (accessed October 9, 2019), https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

In addition to the two operational Space Systems and Network Systems Departments (SSD and NSD respectively), the SSF also has a staff department responsible for operations, planning, training, project management and oversight, and personnel management.[37] The political works department is an integral part of any PLA body. In this army, being of the party and not the nation as a whole, every organization must maintain integrity of political thought and mission in line with party ideology. The SSD handles nearly every aspect of the country's space operations and the NSD subsumed the former 3/PLA and 4/PLA network missions, including SIGINT, cyber espionage, CNO, electronic warfare, and psychological operations. Thus, the new force does not conduct significantly different operations from what 3/

37 Ni and Gill, "The People's Liberation Army Strategic Support Force."

PLA and 4/PLA have been doing for years, but it has been raised to the level of a full-fledged PLA service, comparable to the 2nd Artillery, indicating the elevation of the status of information operations to the highest level.

Chinese language sources reinforce with exactingly particular rhetoric in official discourse that the SSF is a new type of war-fighting power 新型作战力量 *xinxing zuozhan liliang*, which means that the CCP considers the SSF and information operations to be a veritable domain for national security.[38] Official sources report that SSF information operations and the creation of such a force are representative of Military Modernization with Chinese Characteristics 中国特色强军 *zhongguo tese qiangjun*, a phrase that echoes the decades-old refrain of Socialism with Chinese Characteristics 中国特色社会主义 *zhongguo tese shuhuizhuyi*, which was and continues to be a guiding principle for national Reform and Opening 改革开放 *gaige kaifang*. Official sources describe the SSF as helping to achieve the Chinese Dream and the dream of military modernization, and that all officers and soldiers must adapt to the new policies.[39] The entire structure of the PLA, not just the creation of the SSF, is undergoing modernization in order to improve national security, while the SSF, in particular, is a new war-fighting power in national defense.[40]

Conclusion

The restructuring of cyber forces inside the PLA is part of the modernization project of the entire military that began in 2015. China's defense white paper of 2019 identifies its two goals for 2020 to be mechanization, which is the physical modernization of tactical equipment, and informationization construction, which refers to institutions within the PLA that manage information security and, nested therein, cyber security.[41] By 2035, the PLA's stated goal is to fully complete military modernization and to operate in

38 Liu Shangjing ed., "Guo fang bu zin wen fa xin ren jiu shen hua guo fang he jun dui gai ge you guan wen ti jie shou mei ti zhuan fang," Ministry of National Defense of the People's Republic of China, January 1, 2016 (accessed October 9, 2019), http://www.mod.gov.cn/info/2016-01/01/content_4637926.htm.

39 Xinhua News, "Lu jun ling dao ji gou huo jian jun zhan lve zhi yuan bu dui cheng li da hui zai jing ju xing xi jin ping xiang zhong guo ren min jie fang jun lu jun huo jian jun zhan lve zhi yuan bu dui zhi xu jun qi bing zhi xun ci," *Xinhuanet*, January 1, 2016 (accessed October 9, 2019), http://www.xinhuanet.com//politics/2016-01/01/c_1117646667.htm.

40 Xinhua News, "Lu jun ling dao."

41 Xinhua News, "Lu jun ling dao."

the same league as the world's leading militaries. This larger goal includes modernization of military theory, organizational forms or force structure, weapons, and equipment.[42] Standing up the SSF is the fruition of the goal of informationization construction, and it will likely remain the primary force structure for PLA cyber operations forces in the coming decade. As stated in their white paper, more force structure changes may occur before 2035 in order to complete the modernization project. With the SSF as the new organizational form for cyber operations forces, however, future modernizations are unlikely to dramatically alter this force structure; rather, major force structure changes are more likely to alter the precise chain of command under which the SSF falls and not the organization itself.

The sweeping 2016 force structure reorganization creating the SSF may have produced few changes on an operational level for the former 3/PLA and 4/PLA mission sets beside elevating their status. Nonetheless, it represents and reflects a change of the highest order in military strategy and priorities in which information operations have become a new domain of warfare that is absolutely critical to the continued domestic peace that the CCP requires in order to maintain its authority and legitimacy as the only game in town that can keep such a populous and physically vast country tranquil and prosperous. To this end, the CCP under Chairman Xi's highly centralized and effective leadership took cyber operations from bureaucratic confusion and backwaters, and formed it anew under the umbrella of information operations, so that the mission most directly supported the CCP goals of ideological unity and intolerance of dissent as ways to realizing national security. The force structure reorganization was a reflection of and an effective enhancement for new cybersecurity and information security policy, as the Chinese understand that the two come hand in hand.

42 Xinhua News, "Xin shi dai de zhong guo guo fang."