The Strategic Support Force and the Future of Chinese Information Operations

Elsa B. Kania
John K. Costello

The establishment of the Strategic Support Force (战略支援部队, SSF) in December 2015 was a critical milestone in the history of the Chinese People's Liberation Army (PLA), against the backdrop of its historic reform agenda.[1] The SSF's creation reflects an innovation in force structure that could allow the PLA to operationalize its unique strategic and doctrinal concepts for information operations. Despite limited transparency, it is nonetheless possible to glean critical details about the SSF's composition and key missions, based on a range of open sources.[2] It is clear that the SSF has been designed as a force optimized for dominance in space, cyberspace, and the electromagnetic domain, which are considered critical "strategic commanding heights" for the PLA.[3] Under its Space Systems Department (航天系统部), the SSF has seemingly consolidated control over a critical mass of the PLA's space-based and space-related assets. Through these capabilities, the SSF has taken responsibility for strategic-level information support (信息支援) for the PLA in its entirety, enhancing its capability to engage in integrated joint operations and remote operations.[4] Concurrently, the SSF has integrated the PLA's capabilities for cyber, electronic, and psychological warfare into a single force within its Network Systems Department (网络系统部), which could enable it to take advantage of key synergies among operations in these domains. However, beyond the SSF, the PLA also appears to be building up network-electronic operations (网电作战) capabilities within its national Joint Staff Department headquarters and within new regional theater commands (战区), reflecting the emergence of a multi-level force structure specializing in information operations. Thus, the SSF reflects the PLA's uniquely integrated approach to force structure and operations in these vital new domains. This realization of this paradigm through the SSF will enhance the PLA's capabilities to fight and win future "informatized" (信息化) wars.

Elsa B. Kania is an adjunct fellow with the Technology and National Security Program at the Center for a New American Security, where she focuses on Chinese defense innovation in emerging technologies, particularly artificial intelligence. Her research interests include Chinese military modernization, information warfare, and defense science and technology. She is an independent analyst, consultant, and co-founder of the China Cyber and Intelligence Studies Institute (CCISI), which seeks to become the premier venue for analysis and insights on China's use of cyber and intelligence capabilities as instruments of national power.

The Impetus for Reforms

The creation of the SSF reflects the PLA's attempts to resolve prior issues and build up its military cyber forces to ensure their combat capability. Although critical elements of Chinese thinking on information operations had crystallized by the late 1990s—and have remained remarkably consistent since—the PLA has lagged in its efforts to construct forces capable of realizing the intended missions and strategic objectives.[5] Instead, China's military cyber force often ended up being turned to purposes of political and commercial cyber espionage, whether in furtherance of formal missions or, in some cases, seemingly for profit and/or at the behest of local state-owned enterprises. Even when those activities were sanctioned by the appropriate command authorities, the scope and scale may not have been fully known to higher-level PLA leadership, while the risks of apprehension appear to have been largely dismissed, due to the perception that attribution would be futile.

However, this calculus has since changed. In February 2013, Mandiant released the APT1 report, which exposed Unit 61398 of the PLA,[6] and then, in May 2014, the US government charged five 3PLA officers with computer hacking and economic espionage.[7] Although this intended 'naming and shaming' has not resulted in a complete cessation of such activities, their exposure does appear to have had, to at least a limited extent, a deterrent effect and resulted in discernible changes in PLA behavior, including an initial reduction in the frequency of its cyber espionage activities. In September 2015, Presidents Obama and Xi agreed, "neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage."[8]

John Costello is a Senior Analyst for Cyber and East Asia at Flashpoint. John is a co-founder and the executive director of the China Cyber and Intelligence Studies Institute. He is a Cybersecurity Fellow for New America and former Congressional Innovation Fellow for majority staff in the U.S. House of Representatives Committee on Oversight and Government Reform. John is also a US Navy veteran, former NSA Analyst, and is fluent in Mandarin Chinese.

Subsequently, there was a notable decrease in Chinese Advanced Persistent Threat (APT) activity, as documented by FireEye, among others.[9]

At this point, it appears that there has been a notable change in the pattern of Chinese cyber operations. There have been several incidents of cyber-enabled intellectual property theft by Chinese APT groups, although some have seemingly reflected notional adherence to the agreement by targeting companies specializing in defense technology, telecommunications, and software services that could be utilized for both legitimate defense and commercial purposes. Concurrently, the activities of non-military cyber actors, especially a number of contractors linked to the Ministry of State Security (MSS), have become more prominent, while military cyber forces appear to have been redirected away from such activities. For instance, in November 2017, three Chinese hackers working for Boyusec, which is known to act on behalf of MSS,[10] were charged by the US government with hacking several corporations for commercial advantage,[11] in apparent violation of the Obama-Xi agreement. It remains to be seen whether the tenuous norm against commercial cyber espionage will take hold.[12] In the meantime, the MSS appears to have taken the lead, emerging as a major player and full-spectrum intelligence agency, while the focus of PLA cyber operations seems to have shifted away from commercial towards combat-oriented activities.

China's government has also actively sought to build up a cyber defense at the national level, mainly in response to a series of incidents—including the discovery of Stuxnet, the Arab Spring, and the Snowden—each of which revealed unique threats and vulnerabilities that China faces in the cyber domain. The resulting concerns over

pervasive information insecurity have resulted in the development of a more robust framework to enhance national security and resilience. Consequently, China has undertaken a complete overhaul of legal and regulatory regime overseeing information security, spearheaded by the Cyberspace Administration of China (CAC), founded in 2014. The key component of this information security push is the National Cybersecurity Law (NCL), which was made law in November 2016 and implemented in June 2017. The law has acted as a central organizing principle and enforcement mechanism under which agencies have implemented new regulatory regimes over content management, device management, cybersecurity information sharing, encryption, and supply-chain security.[13]

Concurrently, the PLA's historic reform agenda has sought to transform it into a "world-class" military capable of "fighting and winning wars," which requires the advancement of offensive cyber capabilities that would be integral in early stages of a conflict. As constituted, PLA cyber forces were deemed inadequate relative to superior US cyber capabilities. The separation of cyber espionage and offensive cyber forces between 3PLA and 4PLA seemingly prevented their realization as a coherent, integrated fighting force for this new domain. On the surface, the creation of the SSF could be seen as a response and parallel to the US establishment of U.S. Cyber Command (USCYBERCOM).[14] However, a deeper analysis reveals that a more apt counterpart may be USCYBERCOM's parent organization, U.S. Strategic Command (USSTRATCOM), which, like the Strategic Support Force, is responsible for space, cyber operations, and strategic C4ISR support to "combatant commands", regional joint-force areas of responsibility that act has direct analogs to the Chinese military's new theater commands. The SSF is nevertheless a uniquely divergent entity in force structure that distinguishes itself from both USSTRATCOM and USCYBERCOM in several key respects. The most obvious is that China's Strategic Support Force is a military service rather than joint force command and lacks a nuclear mission, USSTRATCOM's original *raison d'etre.* For cyber operations, the differences are deeper and more qualitative. The SSF's cyber corps approach the cyber domain in a much more comprehensive way, reflecting a highly integrated approach to information operations that actualizes critical concepts from PLA strategic and doctrinal approaches.

Overview of Force Structure

The SSF is a unique product of the PLA's reforms, which seek to enhance its capabilities to engage in joint operations.[15] In its design, the SSF is intended to be optimized for future warfare, in which the PLA anticipates such "strategic frontiers" (战略边疆) as space, cyberspace, and the electromagnetic domain will be vital to victory.[16][17] According to its commander, Lieutenant General Gao Jin (高津), the SSF will "protect the high frontiers and new frontiers of national security," while seeking to "seize the strategic commanding heights of future military competition."[18] Despite its relative novelty, the SSF itself is constructed from prior organizational components, reflecting a modular approach to reorganization through which existing institutions have been restructured under new organizations to align with new paradigms.

The SSF is largely composed of operational units and organizations from the PLA's former four "general departments", the General Staff Department (GSD), General Armaments Department (GAD), and General Political Department (GPD) units responsible for space, cyber, electronic, and psychological warfare. In its function and structure, the SSF appears to act in a similar status to that of the nuclear-armed PLA Rocket Force's (PLARF) predecessor, the Second Artillery Corps, which similarly consolidated strategic capabilities under direct national control. This environment has served the strategic missiles mission well; in a few decades, China has fielded an impressive array of both nuclear and conventional missiles that now form the bedrock of its nuclear and conventional deterrence posture. Military leadership may be trying to replicate the success of that model in space and cyber domains, responding to shifts in modern warfare by extending concepts of conventional deterrence into these domains. [19]

The SSF appears to be designed around the operational imperative of "peacetime-wartime integration," which is also a major impetus for the overall reform agenda. [20] Under its prior organizational structure, the PLA would have confronted the challenge of transitioning from a peacetime posture to a wartime posture just prior or immediately after the outbreak of war. For strategic-level information operations, such a shift would have demanded unprecedented coordination across entrenched divisions between national-level departments, services, and military region to form an information operations group (信息作战群) in conflict. The SSF has seemingly streamlined this process through organizing these units into operational groups as standard practice, optimized as a wartime structure. This concept of peacetime-wartime integration is particularly critical for the SSF's Network Systems Department and cyber mission. At a basic level, cyber operations require a persistent cycle of cyber reconnaissance, capabilities development, and deployment to ensure cyber effects can be leveraged in a conflict. Given the functional integration of these peacetime and wartime activities—and the close relationship between reconnaissance and attack—in cyber operations, the integration of China's military cyber offense and espionage capabilities has become a functional necessity. [21] This force structure is consistent with the PLA's recognition of the reality of blurred boundaries between peace and warfare in these domains, which is reflected in its notion of "military struggle" (军事斗争) in cyberspace, as confrontation occurring across a spectrum, of which the highest form is warfare.

Concurrently, the SSF is intended to actualize a shift from a discipline-centric to a domain-centric structure that enhances the PLA's capabilities in critical strategic frontiers. Previously, space, cyber, and electronic warfare units were organized according to the type of mission—the disciplines of reconnaissance, attack, or defense—rather than their warfighting domain. This is best seen in the cyber mission, for which espionage was handled by the Third Department of the former GSD (3PLA), while the offensive elements were handled by the Fourth Department (4PLA), and the former Informatization Department

(信息化部) undertook certain elements of defense. Under the SSF, the idea of "integrated reconnaissance, offense, and defense" (侦攻防一体化) may serve as an organizing concept, which could involve the integration of disciplines together to enhance full-spectrum war-fighting capabilities.[22] This new organizational structure could also enable levels of unified research and development, planning, force construction, and operations that would have been infeasible under the previous structure.

Concurrently, the SSF will confront the reality of rapid, disruptive technological changes, often driven by research and development in the private sector. These dynamics render the SSF's tasking to pursue civil-military integration (or "military-civil fusion," 军民融合) as an integral aspect of its mission. This will involve taking advantage of dual-use technological advances and leveraging civilian talent. Indeed, cyberspace has been highlighted as a priority domain for China's national military-civil fusion strategy, with a particular focus on personnel training and issues of human capital.[23] For instance, the SSF has established partnerships with over nine units and enterprises, such as the University of Science and Technology of China and the China Electronics Technology Group (CETC), to focus on "fostering high-end talent," including through education, training, cooperation, and exchanges.[24]

Similarly, authoritative PLA texts, such as the 2013 AMS SMS, have argued, "since the boundaries between peacetime and wartime are ambiguous, and military and civilian attacks are hard to distinguish, persist in the integration of peace and war [and] in the military-civil fusion; in peacetime, civilians hide the military, [while] in wartime, the military and the people, hands joined, attack together..."[25] As prominent PLA strategist Ye Zheng (叶征) highlighted, "The strategic game in cyberspace is not limited by space and time, does not differentiate between peacetime and wartime, [and] does not have a front line and home-front..."[26] Indeed, the SSF is designed to achieve dominance in a domain in which traditional boundaries are blurred and in which the private sector is integrally involved.

The SSF's Leadership, Structure, and Missions

Established in December 2015, the SSF is commanded by Lieutenant General Gao Jin (高津). Gao Jin served with the former Second Artillery Force and was the president of the Academy of Military Science, which advises the Central Military Commission on strategy and doctrine.[27][28] From an operational perspective, the SSF's headquarters for its space and cyber mission forces are the Space Systems Department (航天系统部) and Network Systems Department (网络系统部) respectively, which command combat forces likely referred to as the "Space Corps" (天军) and "Cyber Corps" (网军). Through the consolidation of the PLA's strategic-level capabilities for these domains, the Space Systems Department and Network Systems Department will respectively pursue missions of strategic information support and strategic-level information operations.

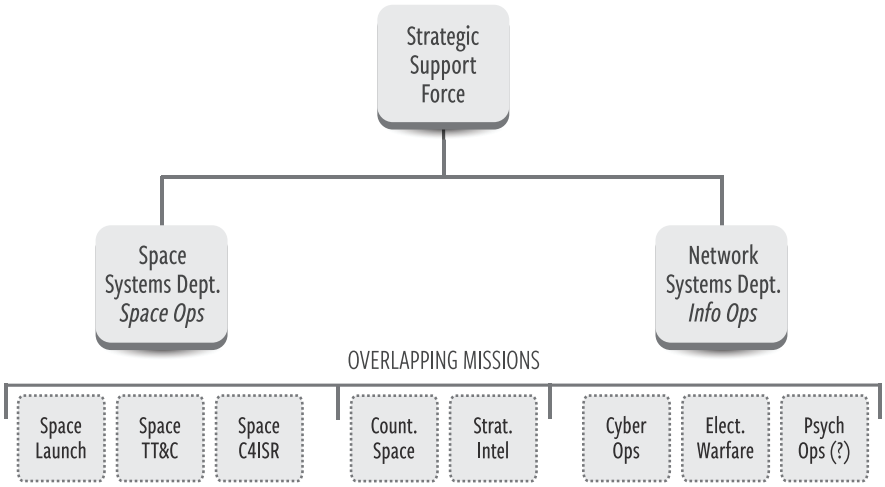

Figure 1. The basic missions of the SSF's two main components: Space and Cyber Corps.

The SSF's Network Systems Department (网络系统部), likely under the command of Major General Zheng Junjie (郑俊杰), appears to integrate a critical mass of the PLA's strategic-level cyber, electronic, and psychological warfare capabilities. The former 3PLA, which was responsible for technical reconnaissance and cyber espionage, appears to be the central component around which the Network Systems Department is organized.[29] As the PLA's premiere cyber espionage organization, the 3PLA's preeminence in this domain makes them a natural fit as the primary "tent-pole" for the SSF's cyber force. Although cyber espionage constitutes one of its central missions, the 3PLA has also been responsible for traditional signals and communications intelligence. Not only the former 3PLA's Technical Reconnaissance Bureaus but also the two electronic warfare brigades from the former 4PLA have been integrated into the Network Systems Department.[30]

Of note, the Network Systems Department also appears to have taken over essential research agendas that could support capability development. It is noteworthy that the GSD 56th, 57th, and 58th Research Institutes, all formerly under the 3PLA, have all been transferred to the Network Systems Department.[31] These research institutes previously reported directly to 3PLA headquarters and were tasked with military research, development, testing, and acquisition (RDT&A) in support of 3PLA's mission.[32][33] Also, the 54th Research Institute, which was formerly subordinate to the 4PLA and focused on electronic and network countermeasures, has moved to the SSF.[34]

Although the name "Network Systems Department" might imply that the department solely incorporates cyber/network warfare capabilities, it appears that China's view of cyberspace is changing, and this organizational structure reflects such a conceptual evolution. The PLA seems to be starting to redefine what "cyberspace" means, expanding the definition to include all aspects of information warfare, such that the concept is

effectively synonymous with the information domain.[35] This would more closely comport with how China's civil authorities view cybersecurity as closely linked to the notion of information security, which includes concerns over content and reflects ideological concerns. In an operational context, this means that China has a more integrated approach to information domain across the "stack," from physical assets, through electronics, to digital networks, all the way to information exchanges and media content. This integrated approach may allow for better planning, acquisition, and operations while enabling the creation of a more flexible cadre of personnel tailored towards new paradigms of information operations.

Although the SSF has consolidated a critical mass of capabilities, the PLA's information operations forces appear to have a more complex, multi-level structure. The SSF does not appear to have incorporated and consolidated the entirety of PLA's cyber espionage and technical reconnaissance capabilities. Under the PLA's previous structure, each service and military region (MR) maintained its own Technical Reconnaissance Bureau (TRB), responsible for signals intelligence and cyber espionage. At this point, it is unclear to what extent the SSF will incorporate these other service or military region TRBs, though there are preliminary indications that a number of them have been transferred into the SSF. On the other hand, the cyber defense mission associated with the former GSD Informatization Department's Information Assurance Base (信息保障基地) and its subordinate Network Security and Defense Center (网络安防中心), remains under the new Joint Staff Department's Information and Communications Bureau (信息通信局).[36] Although, the SSF could incorporate or develop a defensive mission to complement its reconnaissance and offensive capabilities, it appears that the Cyberspace Administration of China, along with the Ministry of Public Security, take primary responsibility for supporting cyber defense at the national level, including the protection of critical infrastructure, and regulatory and law enforcement responsibility, respectively, over compliance with cybersecurity laws and provisions.

Surprisingly, the former GSD Fourth Department (4PLA), also known as the Electronic Countermeasure and Radar Department (电子对抗与雷达部), has *not* been transferred in its entirety to the SSF. While its subordinate electronic warfare brigades have been incorporated into the SSF, its headquarters appears to have been shifted under the CMC Joint Staff Department as the Network-Electronic Bureau (网络电子局 or 网电局) and the Network-Electronic Countermeasures *Dadui* (网电对抗大队), with Wang Xiaoming (王晓明) as the head.[37] The former 4PLA was previously responsible for the entirety of the strategic-level, or national level, and a considerable element of campaign-level electronic warfare for the PLA. Also of note, there appear to be network-electronic countermeasures (网电对抗) units not only at the CMC level but even under the new theater commands (战区),[38] but the parameters of their missions and potential coordination with the SSF remain to be seen.

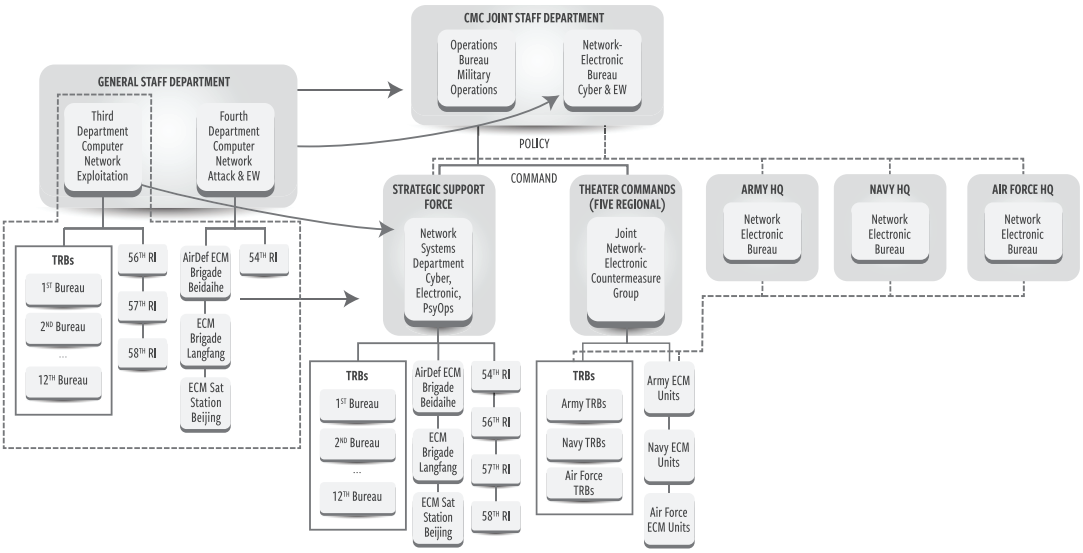

Figure 2. A notional chart depicting the shift in responsibilities for electronic warfare and cyber warfare under the new "network-electronic" paradigm.

At this point, given this complex force structure, there are some unresolved questions regarding command. It appears that the SSF, not unlike the former Second Artillery Force, and now Rocket Force, falls under the direct authority of the CMC rather than being commanded by theater commands. However, the new theater commands and subordinate service elements may possess or construct their own cyber or network-electronic operations capabilities. According to one notional schematic by an SSF scholar, theater command joint operations command departments, through their joint operations cyberspace operations command centers, will exercise command over cyberspace operations forces under each of the services; the CMC Joint Operations Command, through a CMC Joint Command Cyberspace Operations Command Center, commands over the SSF itself, which commands cyberspace strategic reconnaissance, assault, defense, and support forces and capabilities; and in addition, the Cyberspace Administration of China, has authority over military-local cyberspace coordination centers, which could support defensive operations.[39] Although this is not necessarily fully consistent with official command structure, the key elements of it reflect a three-tiered approach to China's cyber capabilities. At present, the construction of more robust cyber or network-electronic combat forces within theater commands likely remains a work in progress. In addition, there do not yet appear to be functional mechanisms for coordination among cyber operations forces at different levels.

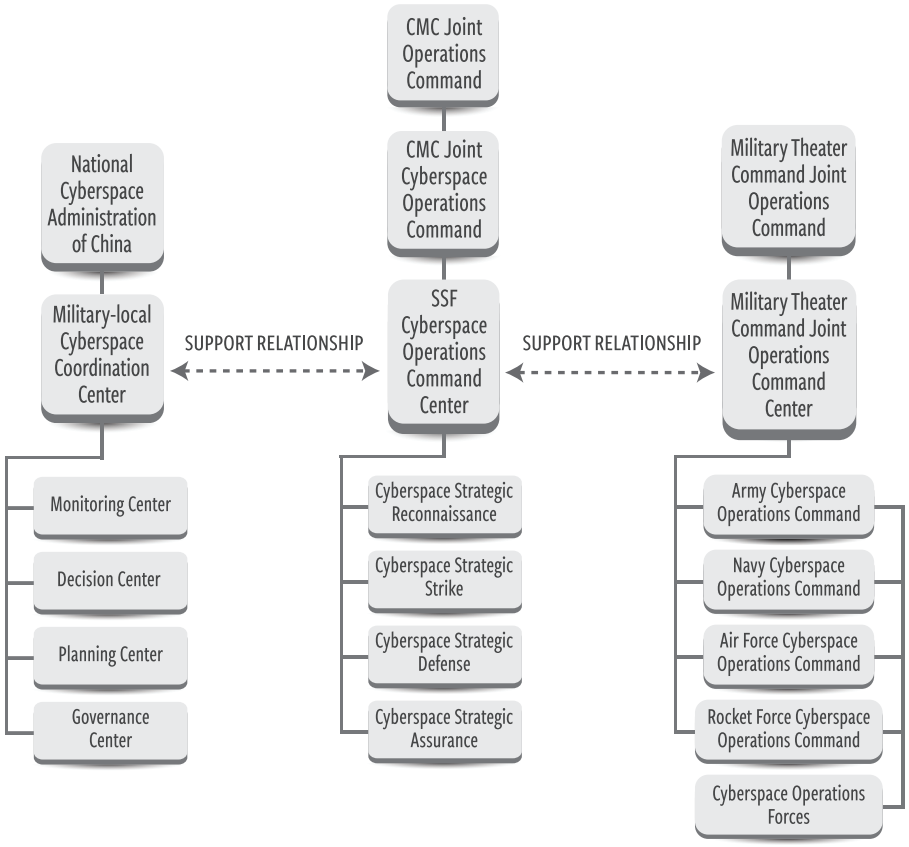

Figure 3. Notional Cyberspace Operational Command System Structure

In addition, PLA information operations forces might be differentiated among strategic information operations forces, which include satellite information attack and defense forces, "new concept" electronic assault forces, and Internet assault forces; campaign information operations forces, which include conventional electronic warfare forces, anti-radiation assault forces, and battlefield cyber warfare forces; and tactical information operation forces, which include satellite information attack and defense forces, and battlefield cyber warfare forces, according to a relatively authoritative PLA textbook.[40]

The PLA's force structure for network-electronic operations capabilities must be contextualized by the concept of the information operations group (信息作战), a joint-force wartime construct that was displayed during the August 2017 military parade that marked the 90th anniversary of the PLA's establishment.[41] In the parade, the information operations group included an information support formation (信息支援方队), electronic reconnaissance formation (电子侦察方队), electronic countermeasures formation (电子对抗方队), and unmanned aerial vehicles (UAV) formation (无人机方队).[42] The informa-

tion operations group would bring together the disparate elements responsible for cyber, electronic, and psychological warfare into an operational command at strategic, campaign, and tactical levels. Before reforms, the national-level or strategic information operations group would have drawn units from the General Staff Department, General Political Department, and the General Armaments Department. The SSF reflects an attempt to knock down prior silos between these units and incorporating them into a cohesive force in peacetime, both to smooth over the transition to wartime, and to construct a more effective war-fighting force.

The information operations group as displayed in this parade resolves a few remaining questions on the relationship between the SSF and China's wartime structure for information operations. First and foremost, the parade formally identifies the SSF's role as the primary fighting force for information operations and "information support" (信息支援), which involves support for intelligence, surveillance, and reconnaissance in space, cyberspace, and the electromagnetic spectrum. Similar to the relationship between the other services and their corresponding operations groups, the SSF serves as the central component of the information operations group. Secondly, while the SSF is the primary fighting force for information operations, it is not the only one. Beyond the SSF, there are units from former military regions and within services that will fall under the new joint theater commands (战区) and focus on campaign-level operations. For instance, in the parade, the electronic countermeasures (ECM) formation came from the PLA, specifically from an air defense brigade and an Army Division ECM detachment (分队).[43] According to relatively authoritative literature on this concept, in a conflict scenario, each service's and branch's information countermeasures forces would combine with the information combat group (信息战斗群).[44] What is still unclear are the composition of different-echelon information operations groups, and whether tactical or campaign-level groups could have a national mission or how they would coordinate or de-conflict their respective missions.

Remaining Challenges

Thus far, in the course of PLA reforms, the Central Military Commission has focused on making broad strokes and affecting change in larger, leading organizations first, in what has been characterized as "above the neck" (脖子以上) reforms.[45] Such an approach minimizes the disruptiveness of these reforms and helps to generate buy-in from leadership on deeper cuts that will undoubtedly take place in the future. These initial steps seek to create a foundation upon which future reforms can be built. For the SSF, this has meant that the old siloed nature of space, cyber, and electronic warfare have been broken and reorganized into new verticals through the Space Systems Department and the Network Systems Department.

Such high-level changes alone, however, will not be enough to enable more profound reform. Although the SSF's force structure reflects significant progress towards a domain-

centric approach to war-fighting in the space, cyber, and electromagnetic domains, with the integration of disciplines of reconnaissance and offense, some incongruences remain at lower levels. At present, elements of the former General Staff Department's cyber, space, and electronic warfare capabilities likely remain integrated within units responsible for other missions. To follow through fully on the conceptual framework associated with the creation of the SSF, deeper, more painful cuts will need to happen to break apart and recombine existing units.

The PLA is currently engaging in "below the neck" (脖子以下) reforms, likely to be implemented over the remaining three year period through 2020 within which the reforms are intended to take place. This current stage of the process will presumably entail undertaking deeper, more difficult changes than previous changes have presaged. For the SSF, this process will test whether the PLA can fully implement the concepts and guiding paradigms that will enable better war-fighting or institutional barriers and vested interests will win the day. At this point, it remains to be seen how the SSF will make these deeper changes to restructure or otherwise integrate disparate organizational components. According to one article, in the SSF's current "grassroots construction" process, "cross-unit forces transfer and handover are progressing smoothly; new adjustment and formation of units are being completed and delimited according to plan; the system of systems architecture and contours of new-type combat forces is starting to appear..." [46] It appears that deeper changes are occurring within the SSF, with the restructuring and reorganization of units, and their transfer to different locations. The SSF's future trajectory will be a critical bellwether of the PLA's capability to implement historical organizational reforms. Indeed, its ability to function as a cohesive force would require deeper, structural changes to ensure the integration and coordination of capabilities that were previously stove-piped, perhaps in the face of considerable bureaucratic resistance.

The Future of Chinese Information Operations

The SSF will undoubtedly take on a central role as the information warfare component of China's military strategy, acting as the 'tip of the spear' in its strategic planning and posture. In their entirety, the PLA's military reforms seek to synthesize military preparations into an "integrated peacetime and wartime" military footing. [47] The use of "strategic presets" is intended to place China's military into an advantageous position at the outset of war, enabling it to launch a preemptive attack or quickly respond to aggression, contributing towards a first strike (先发制人) that is consistent with the perceived offense dominance of the domain. [48] This allows China to offset its disadvantages in technology and equipment through preparation and planning, particularly against a "powerful adversary" (强敌) with technological superiority, generally a byword for the US in PLA strategic literature. In practice, these strategic presets require careful selection of targets so that the first salvo of hard-kill and soft-kill measures can completely cripple

an enemy's operational 'system of systems,' or the ability to use information technology to conduct operations.

Within the context of a joint campaign, PLA information operations forces would be directed to obtain information superiority (信息优势), since to seize and preserve information dominance (制信息权) is considered an important prerequisite and foundation for joint operations.[49] In furtherance of the PLA's "system of systems" operational concept, information operations are recognized as critical means of striking "vital point targets" (要害目标) in an adversary's systems, while ensuring the continued functioning of one's systems.[50] From the PLA's perspective, achieving such information dominance is necessary for air and sea dominance.[51] *The Science of Military Strategy (SMS),* an influential PLA textbook, calls for the coordinated employment of space, cyber, and electronic warfare means as strategic weapons to achieve these ends, to "paralyze enemy operational system of systems" and "sabotage the enemy's war command system of systems."[52] This includes launching space and cyberattacks against political, economic, and civilian targets as a deterrent. Thus, the SSF would be an integral aspect of the PLA's approach to any future informatized war and integrated strategic deterrence.

In its entirety, this emerging force structure for PLA information operations has seemingly been designed with concepts that have consistently occurred in authoritative PLA literature but could not previously be operationalized due to prior organizational divisions. Traditionally, there has a separation between cyber and electronic warfare and between reconnaissance and offensive capabilities, respectively stove-piped within 3PLA and 4PLA. The partial integration of these capabilities within the Network Systems Department could thus appreciably increase the efficacy of Chinese information operations. In particular, the PLA's concept of integrated network-electronic warfare (网电一体战, INEW), which dates back to the early 2000s, is now reflected in organizational realities, enabled by the potential integration of the relevant capabilities, and focus on the construction of new network-electronic countermeasures forces. In early writings, Major General Dai Qingmin (戴青民), former head of 4PLA, who formulated the concept of INEW, anticipated future information operations involving "the destruction and control of the enemy's information infrastructure and strategic life blood, selecting key enemy targets, and launching effective network-electronic attacks."[53] He argued that this integration of cyber and electronic warfare would be superior to the US military's approach at the time of network-centric warfare.[54]

Through its integration of space, cyber, and electronic warfare capabilities, the SSF may be uniquely able to take advantage of cross-domain synergies resulting from the inherent interrelatedness and technological convergence of operations in these domains.[55] Potentially, the Network Systems Department could thus enable the SSF to develop the capability to 'bridge the air gap' and deliver cyberattacks via electronic warfare against isolated

US battlefield networks.[56] Concurrently, the SSF's apparent responsibility for psychological warfare could enable the PLA to exploit the impactful nexus of cyber and psychological warfare capabilities, learning from the success of Russia's efforts. At this point, it is too early to evaluate whether the integrated approach to these domains and the associated disciplines that the SSF represents will be realized in practice, given the likely organizational frictions and resistance associated with such massive reforms. However, the Strategic Support Force, and the military reforms more generally, represent a new era of Chinese information operations, in which long-dormant organizational and operational concepts have found new footing in a new military order.

NOTES

1. This piece is informed by and draws upon the authors' prior writings on the SSF, which include the following: John Costello, "The Strategic Support Force: China's Information Warfare Service," *China Brief,* February 8, 2016, https://jamestown.org/program/the-strategic-support-force-chinas-information-warfare-service/. John Costello, "The Strategic Support Force: Update and Overview," *China Brief,* December 21, 2016, https://jamestown.org/program/strategic-support-force-update-overview/. Elsa Kania, "China's Strategic Support Force: A Force for Innovation?" *The Diplomat,* February 18, 2017, http://thediplomat.com/2017/02/chinas-strategic-support-force-a-force-for-innovation/. Elsa Kania, "PLA Strategic Support Force: The 'Information Umbrella' for China's Military," *The Diplomat,* April 1, 2017, http://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/.

2. The authors relied upon a range of Chinese language open sources available online for this analysis. These included but were not limited to official reporting in PLA media, the publications of SSF affiliates, social media postings, and procurement notices. The authors' knowledge of Military Unit Cover Designations (MUCDs) and the names of relevant individuals were also integral to this analytical effort. Further details about sources and methods are available upon request.

3. For an expansive discussion of this concept, see: Zhou Bisong [周碧松], *Strategic Frontiers* [战略边疆], National Defense University Press [国防大学出版社], 2016.

4. Kevin McCauley, "System of Systems Operations: Enabling Joint Operations," Jamestown Foundation, February 28, 2017, https://jamestown.org/product/pla-system-systems-operations-enabling-joint-operations-kevin-mccauley/. Joel Wunthrow, "A Brave New World for Chinese Joint Operations," *Journal of Strategic Studies,* Volume 40, 2017, http://www.tandfonline.com/doi/abs/10.1080/01402390.2016.1276012?journalCode=fjss20.

5. James C Mulvenon, "The PLA and Information Warfare," *In The People's Liberation Army in the Information Age,* Vol. 145, Rand Corporation, 1999.

6. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-aptl-report.pdf.

7. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," Department of Justice: Office of Public Affairs, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

8. "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," September 25, 2015, The White House Office of the Press Secretary, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

9. FireEye iSight Intelligence, "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," June 20, 2016, https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html.

10. Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3," May 17, 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3/.

11. "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," Department of Justice Office of Public Affairs, November 27, 2017, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

12. Jack Goldsmith and Robert D. Williams, "The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage," Lawfare, November 30, 2017, https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage.

13. Paul Triolo, Samm Sacks, Graham Webster, and Rogier Creemers, "China's Cybersecurity Law One Year on", DigiChina, November 30, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/.

14. Xiao Tianliang [肖天亮] (ed.), *The Science of Military Strategy* [战略学], National Defense University Press [国防大学出版社], 2015.

15. For a more detailed analysis of these reforms, see: Joel Wuthnow and Phillip C. Saunders, "Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications," China Strategic Perspectives: NDU Press, March 2017, http://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/ChinaPerspectives-10.pdf?ver=2017-03-21-152018-430.

16. Strategic Frontiers [战略边疆], China Strategic Support, August 15, 2016, http://zlzy.81.cn/tb/2016-08/15/content_7231775.htm.

NOTES

17. Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部] (eds.), *The Science of Military Strategy* [战略学].

18. "All Military Actual Combat Military Training Forum Delegates Deliver a Speech" [全军实战化军事训练座谈会代表发言摘登], *PLA Daily,* August 7, 2016, http://military.people.com.cn/n1/2016/0807/c1011-28616977.html.

19. Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部] (ed). *The Science of Military Strategy* [战略学], Military Science Press, 2013.

20. Liu Wei (刘伟) (ed.), *Theater Command Joint Operations Command* (战区联合作战指挥), National Defense University Press (国防大学出版社), 2016.

21. Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部], eds. *The Science of Military Strategy* [战略学]. Military Science Press [军事科学出版社], 2013.

22. Xiao Tianliang [肖天亮] (eds.), The Science of Military Strategy [战略学], National Defense University Press [国防大学出版社], 2015, 388.

23."Reshape Cyberspace Military-Civil Fusion Talent Cultivation" [重塑网络空间军民融合人才培养], People's Daily Online, September 15, 2017, http://media.people.com.cn/n1/2017/0915/c414363-29538892.html.

24. "The SSF and 9 Local Units Cooperate to Cultivate High-Level Talent for New-Type Forces" [战略支援部队与地方9个单位合作培养新型作战力量高端人才], Xinhua, July 12, 2017, http://news.xinhuanet.com/politics/2017-07/12/c_1121308932.htm.

25. Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部], eds., *The Science of Military Strategy* [战略学]. Military Science Press [军事科学出版社], 2013.

26. Ye Zheng [叶征]. A Discussion of the Innate Characteristics, the Composition of Forces, and the Included Forms" [论网络空间战略博戏的本质特征, 力量构成与内容形势], China Information Security [中国信息安全], August 2014.

27. Gao Jin's role as commander of the SSF is noteworthy in two respects: First, he is a career Second Artillery officer, so his new role muddies the waters a bit in understanding whether the SSF will be a force composed of Army personnel but treated administratively separate from the Army—not unlike the former PLASAF-PLA Army relationship—or will be composed of personnel from various services and treated administratively separate from all forces. Secondly and more important to this discussion, before his new post as SSF commander, Gao Jin was head of the highly-influential Academy of Military Sciences (AMS) which besides being the PLA's think-tank (along with the National Defense University), is responsible for putting out *The Science of Military Strategy,* a wide-reaching consensus text that captures and guides PLA strategic thinking at the national level. The most recent edition published in 2013 was released under his tenure as commandant of AMS, and many of the ideas from that edition have found their way into the 2015 defense white paper and have informed the reform agenda. His new role could thus be seen as CMC-level endorsement of the views on China's strategic thought contained in *The Science of Military Strategy.*

28. See, for instance: "Gao Jin Becomes Strategic Support Force Commander" [高津任战略支援部队司令员], Sina, January 1, 2016, http://news.sina.com.cn/c/sz/2016-01-01/doc-ifxneept3519173.shtml.

29. There is a growing number of public records that link former 3PLA units and facilities—including former Technical Reconnaissance Bureaus and the 3PLA headquarters itself—to the SSF.

30. The sources are available upon request.

31. Several open sources all indicate their transfer to the SSF.

32. See, for instance, Mark Stokes, Russell Hsiao, and Jenny Lin, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049, November 11, 2011, https://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.

33. The 56th Research Institute focuses on research and development of advanced computing technologies, including supercomputers. The 57th Research Institute seems to engage the development of communications intercept and signal processing systems, and it has also focused on satellite communications technology. The 58th RI focuses on cryptography and information security.

NOTES

34. Several open sources indicate this transfer, including: "How Can the Strategic Support Force Forge New Quality Weapons" [战略支援部队如何锻造新质利器], *PLA Daily,* March 11, 2016, http://www.chinanews.com/mil/2016/03-11/7792939.shtml.

35. Wang Jinsong (王劲松), Wang Nanxing (王南星), and Ha Junxian (哈军贤), "Research on Cyberspace Operations Command" [网络空间作战指挥研究], Journey of the Academy of Armored Force Engineering [装甲兵工程学院学报], October 2016.

36. "After a Year of Military Reform, Reviewing "New Institution Time" in the Military Newspaper's Published Articles" [军改一周年 军报刊文回眸"新体制时间"之变], *PLA Daily,* December 2, 2016, http://military.people.com.cn/n1/2016/1202/c1011-28919716.html.

37. The relevant sources are available upon request.

38. The relevant sources are available upon request.

39. Wang Jinsong (王劲松), Wang Nanxing (王南星), and Ha Junxian (哈军贤), "Research on Cyberspace Operations Command" [网络空间作战指挥研究], *Journal of the Academy of Armored Force Engineering* [装甲兵工程学院学报], October 2016.

40. *Lectures on the Command of Joint Campaigns* [联合战役指挥教程], Military Science Press, 2013, 218-222.

41. Dennis J. Blasko, Elsa B. Kania, and John K. Costello, "The PLA at 90: On the Road to Becoming a World-Class Military?," *China Brief,* August 10, 2017.

42. Ibid. For a full listing of formations in the parade see: *PLA Daily,* August 1, http://www.81.cn/jfjbmap/content/2017-08/01/content_183726.htm and related official media coverage.

43. "The Electronic Countermeasures Formation" (电子对抗方队), Xinhua, July 30, 2017, http://news.xinhuanet.com/politics/2017-07/30/c_1121402312.htm.

44. *Science of Joint Tactics* [联合战术学], Military Science Press, 2013, 120.

45. "'Below the Neck' Reforms Begin" ["脖子以下"改革展开], China Military Online, December 19, 2016, http://www.81.cn/jmywyl/2016-12/19/content_7413070_2.htm.

46. "Exposition on Strategic Support Force Grassroots Construction" [战略支援部队基层建设工作述评], September 24, 2017, http://military.workercn.cn/268/201709/24/170924102952875.shtml.

47. Liu Wei (刘伟) (ed.), *Theater Command Joint Operations Command* (战区联合作战指挥), National Defense University Press (国防大学出版社), 2016.

48. Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部] (ed.), *The Science of Military Strategy* [战略学], 320.

49. *Lectures on the Command of Joint Campaigns* [联合战役指挥教程], Military Science Press, 2013, 218-222.

50. Ibid.

51. Ibid, 165.

52. Ibid, 164.

53. Dai Qingmin, "On Seizing Information Supremacy," Zhongguo Junshi Kexue, April 20, 2003. qtd. in Larry M. Wortzel, "The Chinese People's Liberation Army and Information Warfare," Strategic Studies Institute, March 2014.

54. Dai Qingmin [戴清民]. A New Perspective on Warfare [战争新视点], Liberation Army Press [解放军出版社], 2008.

55. John Costello, "Bridging the Air Gap: The Coming Third Offset," February 17, 2015, War on the Rocks, https://warontherocks.com/2015/02/bridging-the-air-gap-the-coming-third-offset/.

56. Ibid.