INSS

INSTITUTE FOR NATIONAL STRATEGIC STUDIES

CHINA STRATEGIC PERSPECTIVES 13

# China's Strategic Support Force: A Force for a New Era

by John Costello and Joe McReynolds




Center for the Study of Chinese Military Affairs
Institute for National Strategic Studies
National Defense University

## Center for the Study of Chinese Military Affairs

The mission of the China Center is to serve as a national focal point and resource center for multidisciplinary research and analytic exchanges on the national goals and strategic posture of the People's Republic of China and the ability of that nation to develop, field, and deploy an effective military instrument in support of its national strategic objectives. The Center keeps officials in the Department of Defense (DOD), other government agencies, and Congress apprised of the results of these efforts. The Center also engages the faculty and students of the National Defense University and other components of the DOD professional military education system in aspects of its work and thereby assists their respective programs of teaching, training, and research. The Center has an active outreach program designed to promote exchanges among American and international analysts of Chinese military affairs.

## China Cyber and Intelligence Studies Institute

CCISI is a nonprofit organization focused on the study of China's use of cyber, intelligence, and information operations as instruments of state power. CCISI seeks to empower policymakers and analysts with a nuanced and informed view of Chinese cyber issues derived from in-depth study of Chinese language sources, strategy, doctrine, and capabilities. John Costello and Joe McReynolds are co-founders and Director Emeritus and Director of Operations, respectively, for CCISI.

**Cover photo:** Uniform patch of the People's Liberation Army Strategic Support Force (DOD)

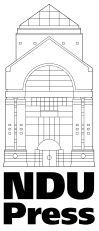
# China's Strategic Support Force

# China's Strategic Support Force: A Force for a New Era

by John Costello and Joe McReynolds

*Center for the Study of Chinese Military Affairs*
*Institute for National Strategic Studies*
*China Strategic Perspectives, No. 13*

Series Editor: Phillip C. Saunders




National Defense University Press
Washington, D.C.
October 2018

First printing, October 2018

For current publications of the Institute for National Strategic Studies, please visit inss.ndu.edu/Publications.aspx.

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

ISBN 978-0-16-094959-3

**Contents**

## Acknowledgments

The authors thank Dr. Joel Wuthnow (National Defense University), Dr. Alex Crowther (NDU), and Frank Miller (Defense Intelligence Agency) for useful comments in the peer-review process, and Dr. Phillip C. Saunders (NDU) for substantive comments, editing, and encouragement. Ian Burns McCaslin assisted in finalizing and formatting the footnotes and helped with the pinyin and Chinese characters in the text and footnotes. Thanks to Jim Chen (NDU), Major Ryan Neely, USA, Major Adam Greer, USAF, and Phil Stockdale (NDU) for their help in proofreading the manuscript. Dr. Jeffrey D. Smotherman and Joanna Seich (NDU Press) designed the published format and prepared the artwork for press.

The paper that became this monograph was originally presented at the 2017 International Conference on People's Liberation Army Affairs, "PLA Reforms, Part Deux," in Taipei, Taiwan, on November 17–18, 2017. The conference series is co-sponsored by Taiwan's Council of Advanced Policy Studies, the Center for Strategic Studies, National Defense University, and the RAND Corporation. Stan Weeks (SAIC) and Yuan-Chou Jing (Center for Strategic Studies) provided useful comments on the earlier draft. This monograph will also be published as a chapter in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms* (NDU Press, forthcoming). The e-book will be available at <http://ndupress.ndu.edu/Publications/Books/Chairman-Xi-Remakes-the-PLA>.

## Executive Summary

In late 2015, the People's Liberation Army (PLA) initiated reforms that have brought dramatic changes to its structure, model of warfighting, and organizational culture, including the creation of a Strategic Support Force (SSF) that centralizes most PLA space, cyber, electronic, and psychological warfare capabilities. The reforms come at an inflection point as the PLA seeks to pivot from land-based territorial defense to extended power projection to protect Chinese interests in the "strategic frontiers" of space, cyberspace, and the far seas. Understanding the new strategic roles of the SSF is essential to understanding how the PLA plans to fight and win informationized wars and how it will conduct information operations.

- The SSF combines assorted space, cyber, electronic, and psychological warfare capabilities from across the PLA services and its former General Departments.

- In addition to expected efficiency gains from this approach, the SSF was created to build new synergies between disparate capabilities that enable specific types of strategic information operations (IO) missions expected to be decisive in future wars.

- Despite a lack of transparency and the fact that the SSF is still in transition, a coherent picture has emerged of how the SSF's components fit together and the strategic roles and missions they are intended to fulfill.

The SSF reports to the Central Military Commission (CMC) and oversees two co-equal, semi-independent branches: the Space Systems Department, which leads a space force responsible for space operations, and the Network Systems Department, which leads a cyber force responsible for information operations.

- The Space Systems Department is largely built around elements of the former General Armament Department and now controls nearly every aspect of PLA space operations, including space launch and support; telemetry, tracking, and control; information support; and space warfare. This appears to resolve previous PLA bureaucratic power struggles over responsibility for space missions.

- The Network Systems Department is built around the former General Staff Department 3rd Department and incorporates all strategic IO units in the PLA, including those

responsible for cyber warfare, electronic warfare, psychological warfare, and technical reconnaissance. This centralization addresses longstanding challenges in operational coordination between the PLA's cyber espionage and cyber attack forces. Below the strategic level, the Network Systems Department shares operational- and tactical-level missions with units under the services and regional theater commands.

- The PLA has thus far pursued a "bricks, not clay" approach to the creation of the SSF. Instead of building the organization from scratch, the PLA has renamed, resubordinated, or moved existing organizations and their component parts and then redefined their command relationships.

The SSF has two primary roles: strategic information support and strategic information operations.

- The SSF's strategic information support role entails centralizing technical intelligence collection and management, providing strategic intelligence support to theater commands, enabling PLA power projection, supporting strategic defense in the space and nuclear domains, and enabling joint operations.

- The SSF's strategic IO role involves the coordinated employment of space, cyber, and electronic warfare to "paralyze the enemy's operational system-of-systems" and "sabotage the enemy's war command system-of-systems" in the initial stages of conflict.

- The SSF improves the PLA's ability to conduct information operations by integrating multiple disciplines of information warfare into a unified force, integrating cyber espionage and offense, unifying information warfare campaign planning and force development, and unifying responsibilities for command and control of information operations.

- The SSF also appears to have incorporated elements of the PLA's psychological and political warfare missions, a result of a subtle yet consequential PLA-wide reorganization of China's political warfare forces. This may portend a more operational role for psychological operations in the future.

The PLA reforms have substantially altered the command context for many of the missions now under the SSF, redefining longstanding organizational relationships and creating new responsibilities across the PLA command bureaucracy.

- The reforms dissolved the four general departments and created an expanded Central Military Commission, including a new Joint Staff Department (JSD) with responsibility for supervising joint operations. The CMC now oversees a dual command structure where services are responsible for force construction and five theater commands are responsible for conventional joint operations in their respective regions. The SSF and Rocket Force fall outside this bifurcated arrangement, maintaining responsibility for both their own force construction and strategic operations.

- The PLA has created a new force-wide structure under the JSD for managing cyber and electronic warfare missions. Along with the creation of the SSF, this framework aims to institutionalize the PLA's longstanding goal of "integrated network and electronic warfare." The exact division of responsibilities between the JSD and SSF remains unclear, including how the PLA will integrate SSF espionage and offense-oriented cyber operations with CMC management of the PLA's cyber defense mission.

- The SSF has been entrusted with technical reconnaissance capabilities supporting operations, but not with intelligence capabilities supporting strategic decisionmaking. In context, this reform gives the PLA more latitude to move away from its army-dominated past and direct intelligence resources toward critical operational needs.

The PLA reforms can be compared to U.S. reforms after the Goldwater-Nichols Department of Defense Reorganization Act of 1986, which were similarly aimed at transforming a peacetime military structure toward one more optimized for joint warfare. The SSF is partly modeled on U.S. Strategic Command (USSTRATCOM), with modifications reflecting China's unique approach and challenges.

- The PLA's decision to construct the SSF as a separate service rather than a joint force construct like USSTRATCOM was ostensibly driven by lessons learned from observing foreign militaries and is intended to avoid redundancies in force development and counterproductive rivalries for funding and resources.

- Unlike U.S. Cyber Command, the SSF's Network Systems Department (the closest comparable organization in the PLA) is responsible for a much broader range of operations, including kinetic, cyberspace, space, electromagnetic, and psychological operations.

- Questions remain about how the SSF will integrate its cyber espionage and attack missions, which have historically been separated. Integration will require developing new strategy and doctrine on the use of force in cyberspace without the benefit of substantive operational experience or robust real-world case studies.

The creation of the SSF heralds a new era for China's strategic posture, both in terms of the PLA's preparations for fighting and winning informationized wars and its shift to projecting power farther from China's shores.

- The SSF embodies the evolution of Chinese military thought about information as a strategic resource in warfare, recognizing both the role it plays in empowering forces and vulnerabilities that result from reliance on information systems.

- The SSF's responsibility for both information support and information operations is prescient, enabling more rapid adaptation as China shifts from reliance on asymmetric capabilities as a weaker power to contending with adversaries on more symmetric terms as a near-peer competitor.

- The consolidation of information operations under the SSF could act as a limiting factor for the development of service space, cyber, and electronic warfare capabilities necessary for tactical warfighting needs.

- It remains an open question how the SSF will manage conflicting or overlapping responsibilities between its space and cyber forces. Force integration at lower organizational and administrative layers is challenging, and deficiencies in integration may impede the SSF's ability to integrate its in-house space and cyber missions as well as its coordination with theater commands and other entities.

- The SSF's ability to execute its envisioned roles will depend in large part on the PLA's ability to address weaknesses in its broader organizational culture, including a historical emphasis on top-down control and distrust of bottom-up decisionmaking.

## Introduction

In late 2015, the People's Liberation Army (PLA) initiated a series of ongoing reforms that have brought dramatic changes to its structure, model of warfighting, and organizational culture. Undoubtedly, among the most important changes has been the creation of a unified Strategic Support Force (SSF) [*zhanlüe zhiyuan budui*, 战略支援部队]. This force combines assorted space, cyber, and electronic warfare (EW) capabilities from across the PLA services and its former general departments.

The few statements that Xi Jinping has made about the role of the Strategic Support Force have been almost comically circumspect, affirming that it is both a "strategic" force and a "supporting" one. Even 2 years after its founding, some aspects of the SSF's organizational structure remain opaque to outside observers. However, despite this lack of transparency, a coherent picture has gradually emerged of how various SSF components fit together and the strategic roles and missions that they are intended to fulfill.

Although the Strategic Support Force is often described as having been designed to streamline the organization of China's information warfare forces and thereby improve their efficiency, such incremental advantages are not the primary reason that the SSF was created. Rather, the SSF's structure is first and foremost intended to create synergies between disparate information warfare capabilities in order to execute specific types of strategic missions that Chinese leaders believe will be decisive in future major wars. The PLA views cyber, electronic, and psychological warfare as interconnected subcomponents of information warfare writ large. Understanding the primary strategic roles of the SSF is essential to understanding how China will practice information operations in a war or crisis.

This paper begins by examining the evolution of China's approach to the space, cyber, and electromagnetic domains over the last three decades. It then provides an analysis of military organizational reforms launched in 2015, contextualizing the SSF's creation against the backdrop of broader changes to PLA structure, command organization, and changing concept of operations before focusing on the organizational dynamics of the SSF itself. The paper then explores each of the SSF's operational components, those responsible for its space, cyber, EW, and psychological operations mission areas. After giving a brief overview of how peacetime-wartime command relationships have shifted in the reforms, the paper then details the new joint force structure of the Central Military Commission (CMC) and evaluates how the responsibilities for intelligence and technical reconnaissance, network and EW, and information support missions have shifted force-wide given the preeminence of the SSF in these missions and the new

CMC and regional theater command structure. Finally, the paper outlines the key operational responsibilities of the SSF in the context of the two primary roles it plays: strategic information support and strategic information operations. The paper then defines China's conceptualization of information warfare as applied to the SSF and notes key points where this concept aligns and diverges from a U.S. approach.

A key observation underpinning the research for this paper is the insight that the PLA, at least in the initial stages of its reforms, has pursued what we call a "bricks, not clay" approach to reorganization. Instead of building whole organizations from scratch, the PLA effected structural changes by renaming, resubordinating, or moving whole, existing organizations and their component parts and then redefining their command relationships within the PLA. While the names, descriptors, designators, and, in some cases, the commanders of these organizations have changed, the addresses, key personnel, phone numbers, and other unique designators have remained consistent throughout the reforms. Through analysis of hundreds of public bid and tender documents, contracts, articles, and research papers, the authors have been able to identify numerous instances where these designators remained the same, while the organizations to which they were tied underwent changes of name or affiliation. From clusters of these instances, it can be inferred which existing organizations have been renamed or shifted in the reorganization, and from that one can determine both the new structure of the SSF and changes in the PLA's larger command context.

Identifying the Military Unit Cover Designators (MUCDs) that have been assigned to the SSF, a block of numbers between 32001 and 32099, was particularly useful in this analysis. These designators are commonly used as a cover mechanism for open-source references to PLA units. Since organizations and units operating within this block are now subordinate to the SSF, one can apply the above methodology to systematically identify SSF units and their command relationships.[1]

This structural analysis informs analysis of the roles and missions of the SSF itself. Based on the assumption that the operational responsibilities of most units and organizations that were shifted to the SSF have not been fundamentally changed by the reforms, one can draw upon the existing body of Chinese military and PLA literature to gain insight into prior organizations that are now components of the SSF. With an understanding of the structure and mission of the SSF, one can then determine its broader roles and responsibilities within the PLA by evaluating this mission set against public comments, strategic literature, an understanding of the intent and impetus for reforms, as well as the broader command and organizational context under which the SFF was being formed.

## The SSF in Historical Context

China's approach to the interrelated space, cyber, and electromagnetic domains—the main functional and warfighting areas for the Strategic Support Force—has undergone considerable evolution over the past three decades. In the 1990s, China identified and absorbed lessons from the 1991 Persian Gulf War, which in its view demonstrated that "the new revolution in military affairs had moved from theoretical exploration into the phase of implementation . . . drawing back the curtain on informationized warfare."[2] The lessons China took from the Gulf War fundamentally changed the way that its military planners viewed the future of warfare as well as an understanding of its own vulnerabilities, prompting a decades-long upheaval in Chinese thinking on the strategic role of information in warfare.[3]

China drew two primary lessons from the Gulf War. First, the war proved that the widespread integration of information technology in warfare could confer overwhelming military superiority. As a result, a country's progress in "informationizing" [*xinxi hua*, 信息化] itself, both in a military context and on a broader societal level, is central to its national security.[4] To this end, the PLA recognized that it would need to study and adopt operational concepts that are informed by the U.S. concept now referred to as "network-centric warfare."[5] The operational use of space-based command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) attracted particular notice, with PLA writers frequently referencing it as a barometer of how informationized warfare had become.[6] Second, the PLA quickly assessed that U.S. use of these technologies created fundamental dependencies that could be exploited in wartime. This line of thinking paved the way for China's unique information warfare strategy, which seeks to "overcome the superior with the inferior" through the application of asymmetric information countermeasures against critical nodes in space, cyberspace, and the electromagnetic domains.[7] After working through a number of doctrinal iterations, by the end of the 1990s the PLA had successfully developed the foundational concepts that have guided China's strategy for and development of its information warfare forces ever since.

Chinese strategists spent the 2000s focused primarily on applying these concepts and lessons, both through force-wide concepts such as integrated network and electronic warfare (INEW) [*wangdian yiti zhan*, 网电一体战] and at the operational level. By the end of the decade, the PLA had successfully fielded a regional constellation of Beidou navigation satellites, space-based surveillance platforms, and dual-use communications and relay satellites. Taken together, they formed the foundation of a nascent Chinese C4ISR system to enable regional surveillance, reconnaissance, and precision strikes.[8] At the same time, China was rapidly developing its ability

to launch offensive information operations. By 2009, PLA EW forces had fielded a basic capability to deny or disrupt U.S. space-based C4ISR and navigation.[9] China's military cyber forces attracted global attention from the mid-2000s onward due to a series of high-profile cyber intrusions that demonstrated both growing sophistication and the rapid progress that Chinese forces had made in the span of a few short years. China also demonstrated a counterspace capability with the development of a direct-ascent antisatellite system, which destroyed an obsolete satellite in a January 2007 test.[10]

The advancement of the technical capabilities of Chinese space, cyber, and EW forces stood in stark contrast with the PLA's stagnant operational structure, which remained virtually unchanged throughout the 2000s. In the years immediately leading up to the PLA's 2015 reorganization, there was a growing realization in scholarly circles that the PLA's structure and organization, not its technological capabilities, had emerged as the foremost roadblock facing modernization efforts.[11] The key organizations responsible for space, cyber, and EW missions were distributed across different parts of the PLA and remained stovepiped in their respective organizations, even as the PLA's strategic literature increasingly called for greater integration of these forces as an operational necessity.[12] It is therefore unsurprising that the PLA saw the current period of major reforms as an opportunity to finally realign its sprawling space, cyber, and EW capabilities into a unified force.

The Strategic Support Force's creation comes at an inflection point for the PLA. China has accelerated the ongoing shift of its military posture from land-based territorial defense to extended power projection, not only in the East and South China seas but also beyond them.[13] As part of this transition, China's leaders have expressed a growing desire to protect their country's interests further afield in the "strategic frontiers" of space, cyberspace, and the far seas.[14] On this point, the relatively authoritative 2013 edition of the *Science of Military Strategy* observed that "preparations and prepositioning in fighting for new strategic spaces is both an important brace-support for a country's use of these international public spaces, and also an important action in contesting new military strategic commanding heights."[15] China's 2015 Military Strategy White Paper similarly describes the three as "critical domains" and echoes their importance to China's national interests.[16] The SSF's design is a logical fit for improving China's access to the space and cyber domains in peacetime and contesting them in wartime. The SSF's "remote operations" in the far seas and beyond are aimed at achieving strategic national objectives through counterintervention and power projection.[17]

Even before the SSF's creation, the idea of forming an organization like it to meet the demands of future warfare had been germinating within the PLA's strategic theory community for

years. As early as 2007, China's strategic literature called for an independent space force to unify myriad elements of Chinese organizations responsible for space operations.[18] Similarly, after the formation of U.S. Cyber Command (USCYBERCOM) in 2009, there were numerous calls for China to establish its own equivalent, with PLA scholars noting the inherent advantages of a unified command.[19] In 2012, the influential PLA information warfare specialist Ye Zheng suggested a conceptual and organizational integration of information warfare disciplines into an integrated network-electronic-psychological warfare force that partially resembles the SSF's cyber force.[20]

However, the closest conceptual forerunner for the Strategic Support Force comes from U.S. Strategic Command (USSTRATCOM). The PLA's decision to incorporate both space and cyber forces into a single service-like entity does not appear to have any clear bellwether in Chinese strategic literature. Due to USSTRATCOM's broad responsibilities for space, cyber, strategic EW, and strategic information support, it was chosen as a model for the SSF.[21] Following USSTRATCOM's example, the SSF is tasked with space and cyber missions, while also providing the theater commands with ISR support for joint operations.

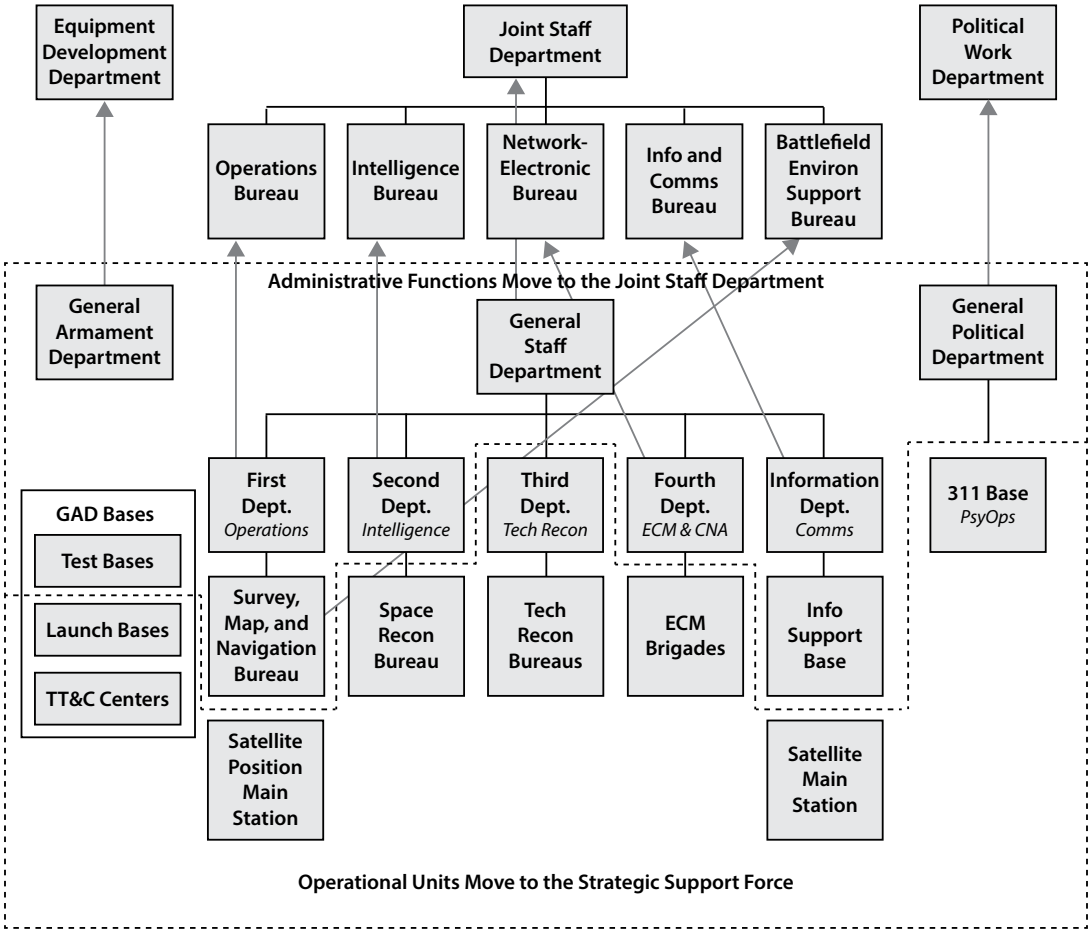
## The SSF and PLA Reform Efforts

The Strategic Support Force was created as part of a broader reorganization that dissolved the PLA's four former general departments, incorporating the bulk of their functions into 15 joint force "functional organs" within an expanded Central Military Commission. The General Staff Department (GSD) became the new CMC Joint Staff Department, the General Political Department (GPD) became the CMC Political Work Department, the General Armament Department (GAD) became the CMC Equipment Development Department, and the General Logistics Department became the CMC Logistics Support Department.[22] These are not exact analogues to their predecessors; some capabilities, tasking, and component parts have been transferred elsewhere within the PLA, particularly in the case of the SSF.

At the outset of the reorganization, the SSF was formed out of these departments' operational units responsible for space, cyber, and EW. This move was aimed in part to alleviate the organizational silos and other roadblocks that previously impeded the effective employment of these elements as a cohesive, coordinated strategic force under the general department system. The SSF's space mission is formed primarily from units under the former GAD and select elements of the GSD responsible for space-based C4ISR. The SSF's information warfare mission comes largely from the former Third and Fourth departments of the GSD, which had respectively held the responsibilities for technical reconnaissance and offensive cyber operations. The elements of the GPD responsible for psychological operations were also incorporated into the

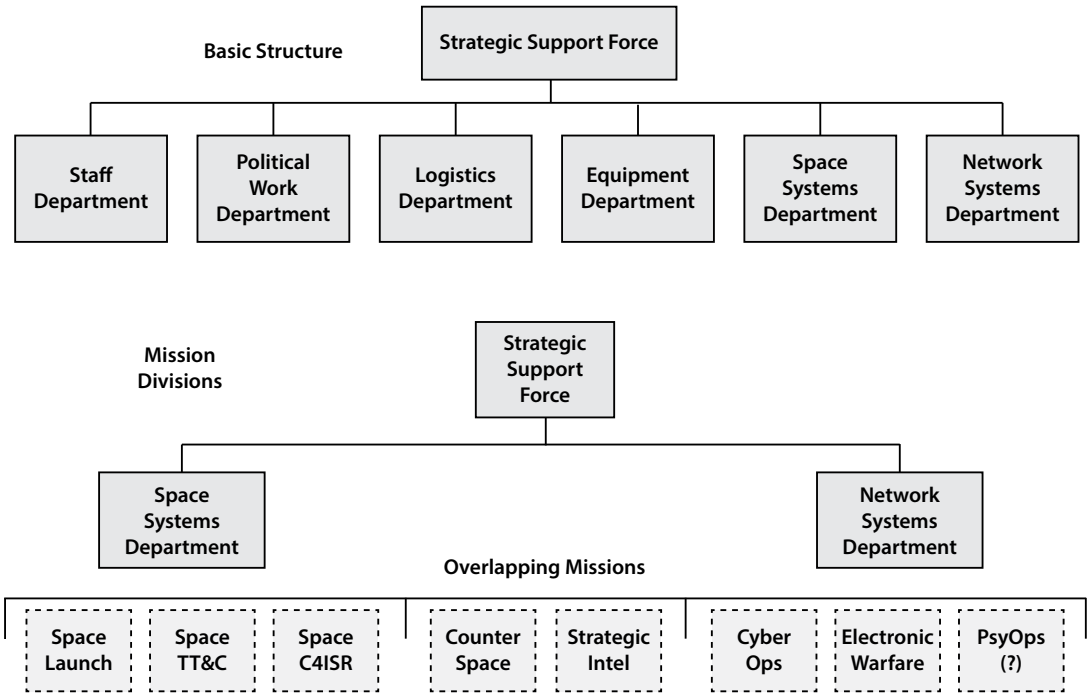
SSF, in keeping with the PLA's aforementioned conceptualization of cyber, electronic, and psychological warfare as interconnected subcomponents of information warfare. The psychological domain constitutes a core element of the PLA's concept of the "Three Warfares" [*sanzhong zhanfa*, 三种战法], a unique Chinese warfighting model that calls for the coordinated use of psychological operations, public opinion warfare, and legal warfare to gain an advantage over an adversary, and thus the SSF is expected to participate in Three Warfares missions. Figure 1 shows the pre-reform locations of the major components that make up the SSF. Figure 2 shows the post-reform structure of the SSF, including headquarters elements such as the Staff Department and Political Work Department (organized as first-level departments), the Space Systems

**Figure 1. Pre-Reform Locations of Major SSF Components**




*Key*: ECM: electronic countermeasures; GAD: General Armament Department; PsyOps: psychological operations; TT&C: telemetry, tracking, and control; GPD: General Political Department.

**Figure 2. Overall Structure of the SSF**




*Key*: PsyOps: psychological operations; TT&C: telemetry, tracking, and control.

Department (responsible for space operations), and the Network Systems Department (responsible for information operations).

When PLA leadership plotted out a multiyear course for reforms through 2020, they opted for a two-stage approach. The first stage largely consists of "above the neck" [*bozi yishang*, 脖子以上] organizational reforms that lay out the overall design of China's armed forces going forward, with "below the neck" [*bozi yixia*, 脖子以下] reforms coming later to reshape PLA institutions and operations on a more granular level. In keeping with this plan, the PLA has so far largely taken a "bricks, not clay" approach to the creation of the Strategic Support Force. That is, existing institutions have been taken in their entirety and placed within the SSF's new organizational superstructure to serve as a core around which other, smaller elements can later be arrayed. This dynamic is visible in the SSF's space and cyber warfare forces, the central components of which are formed from the GAD's space cadre and the former GSD Third Department, respectively. These in turn act as pillars for their respective missions, with lower grade units from the GSD and services being transferred underneath them.

Prior to the PLA's reorganization, space, cyber, and EW units were organized according to mission type—disciplines of reconnaissance, attack, or defense—rather than their warfighting

domain.[23] This is most evident when looking at the PLA's cyber mission. Previously, espionage and technical reconnaissance in the cyber domain were handled by the GSD Third Department, while the targeting and attack missions were handled by the GSD Fourth Department. Separately, the former GSD Informatization Department [*xinxihua bu*, 信息化部] handled key elements of information systems defense.[24] The approach used for the SSF is intended to enable more effective full-spectrum warfighting by treating space, cyberspace, and the electromagnetic spectrum as primary warfighting domains in their own right, rather than as supporting elements of other domains.[25] In recent PLA strategic writings such as the 2015 National Defense University version of the *Science of Military Strategy*, this approach is termed "integrated reconnaissance, attack, and defense" [*zhen gongfang yiti hua*, 侦攻防一体化].[26]

PLA strategic writings reflect a recognition that employing a domain-centric force for information warfare enables levels of unified planning, force construction, and operations that would have been infeasible under the previous structure. This runs counter to the movement of the PLA's conventional armed services toward force construction and away from operations, which have been tasked to the theater commands. The difference is due to the unique requirements of the information domain, where the vulnerabilities and exploits necessary to create "cyber weapons" are discovered, refined, and deployed in a rapid, continuous loop throughout both peacetime and wartime.

Another important principle that appears to have influenced the design of the SSF is the enduring Maoist imperative of peacetime-wartime integration [*pingzhan jiehe*, 平战结合, or *pingzhan yiti*, 平战一体].[27] Under its pre-reform organizational structure, the PLA would have been required to transition to a wartime posture just prior to the outbreak of war (or immediately following it, if China were taken by surprise). For strategic-level information operations, this operational requirement would have demanded unprecedented coordination between GSD, GAD, GPD, and military region units across multiple echelons. The creation of the SSF and the theater commands has simplified this process dramatically by organizing both China's conventional and information warfare units into permanent operational groupings that are designed to transition seamlessly into wartime command structures, though how smoothly that transition will be carried out in practice remains an open question.

## Overview of the SSF as an Organization

To predict the role that the Strategic Support Force will play in wartime, it is first necessary to understand the particulars of the organization itself, as the SSF's structure will have a major impact on how its forces can be effectively employed during a conflict. Established on December

31, 2015, the Strategic Support Force is a theater command leader grade [*zheng zhanqu ji*, 正战区级] independent military force under the direct command of the Central Military Commission.[28] General Gao Jin, who previously served with the former Second Artillery Force [*di er paobing budui*, 第二炮兵部队] and then as president of the Academy of Military Science (AMS), was named as the first SSF commander.[29] General Liu Fulian[30] served as the SSF's first political commissar until March 2017, when he was replaced by General Zheng Weiping.[31] General Gao's previous role as AMS president highlights the central role that AMS and its internal debates play in China's formulation of its military strategic thought—including, it appears, China's plans for the SSF. This prominence is without parallel in the military academic institutions of western countries.[32] See table 1 for a list of SSF leadership.

Administratively, the SSF operates similarly to the former PLA Second Artillery Force, which was also a force [*budui*, 部队[1]] that functioned like a service and consolidated strategic capabilities under the direct command of the CMC.[33] Of its first-level departments, the SSF has a standard four-department administrative structure that includes the SSF Staff Department [*canmou bu*, 参谋部], Equipment Department [*zhuangbei bu*, 装备部], Political Work Department [*zhengzhi gongzuo bu*, 政治工作部], and a Logistics Department [*houqin bu*, 后勤部].[34] Alongside these departments, the force also maintains headquarters for its space and information warfare forces in the Space Systems Department (SSD) [*hangtian xitong bu*, 航天系统部] and Network Systems Department (NSD) [*wangluo xitong bu*, 网络系统部], respectively.[35]

The SSF's operational responsibilities and chain of command were initially uncertain but have become clearer over time. As part of the PLA reforms, the Central Military Commission restructured the principal responsibilities of the military's main components under a new paradigm encapsulated by the official phrase "CMC leads, theaters fight, and services build" [*junwei guanzong, zhanqu zhuzhan, junzhong zhujian*, 军委管总, 战区主战, 军种主建], envisioning a division of labor that would see the new theaters focus on operations, the services on force construction, and the CMC on supervising and managing both. This approach resulted in a new dual-command structure with an administrative chain from the Central Military Commission

[1] The term *dui* [队] is translated a number of ways in Chinese, though usually as "unit" or "team" in a military context. It is used frequently in Chinese military terminology such as in *budui* [部队], "force" or "corps." When used in a unit name, the term is subject to interpretation based on context and does not give a firm indicator of unit grade or echelon on its own. For the purposes of this paper, the term is most often used in the description of joint units where the term is indicated, most often in the term itself (*dui*) and in a related term *dadui*, which connotes a high-level unit under which *dui*'s fall. As there is no clear English equivalent for these terms, this paper utilizes the original Chinese while providing additional context to avoid confusion.

**Table 1. SSF Leadership, Grades, and Former Positions**

| Name | Position | Grade | Rank | Former Position |
|---|---|---|---|---|
| Gao Jin [高津] | Commander | Military Theater Leader Grade | General | Commandant, AMS; former Second Artillery officer |
| Zheng Weiping [郑卫平] | Political Commissar | Military Theater Leader Grade | General | Political Commissar, Eastern Military TC |
| Lu Jiancheng [吕建成] | Deputy Political Commissar and Director, Discipline Inspection Commission | Deputy Military Theater Leader Grade | Lieutenant General | Deputy Political Commissar, Jinan MR |
| Feng Jianhua [冯建华] | Director, Political Work Department | Deputy Military Theater Leader Grade | Major General | Director, GPD Cadre Department |
| Li Shangfu [李尚福]* | Deputy Commander and Chief of Staff | Deputy Military Theater Leader Grade | General | Director, GAD Xichang Satellite Launch Center |
| Sun Bo [孙波] | Deputy Chief of Staff | Corps Leader Grade | Major General | Director, GSD Management Support Department |
| Zhang Minghua [张明华] | Deputy Chief of Staff | Corps Leader Grade | Major General | Deputy Director, GSD Third Department |
| Rao Kaixun [饶开勋] | Deputy Commander | Deputy Military Theater Leader Grade | Lieutenant General | Director, GSD Operations Department |
| Shang Hong [尚宏] | Deputy Commander and Commander, SSD | Deputy Military Theater Leader Grade | Lieutenant General | Chief of Staff, GAD |
| Kang Chunyuan [康春元] | Political Commissar, SSD | Deputy Military Theater Leader Grade | Lieutenant General | Deputy Political Commissar, Lanzhou MR |

**Table 1. SSF Leadership, Grades, and Former Positions, cont.**

| Name | Position | Grade | Rank | Former Position |
|---|---|---|---|---|
| Hao Weizhong [郝卫中] | Deputy Commander, SSD | Corps Leader Grade | Major General | Director, Taiyuan Launch Center |
| Fei Jiabing [费加兵] | Chief of Staff, SSD | Corps Leader Grade | Major General | Director, Maritime Tracking and Control Department |
| Zheng Junjie [郑俊杰] | Deputy Commander and Commander, NSD | Deputy Military Theater Leader Grade | Lieutenant Major General | Director, GSD Third Department; Director, PLA Information Engineering University |
| Chai Shaoliang [柴绍良] | Political Commissar, NSD | Deputy Military Theater Leader Grade | Lieutenant General | Deputy Political Commissar, GAD |

* Li Shangfu is now director of the CMC Equipment Development Department. His replacement as SSF chief of staff has not been identified.

*Key*: AMS: Academy of Military Sciences; GAD: General Armament Department; GPD: General Political Department; GSD: General Staff Department; MR: military region; NSD: Network Systems Department; SSD: Space Systems Department; TC: theater command.

to the services and an operational chain from the CMC to the five joint force theater commands. In theory, this would imply that subordinate SSF elements would be under the operational command of the five theater commands. In practice, however, much like the PLA Rocket Force [*jiefangjun huojian jun*, 解放军火箭军], which serves as the cornerstone of China's nuclear deterrent, the SSF's capabilities have been deemed sufficiently strategic that it reports directly to the Central Military Commission for operations.[36] The theater commands are confirmed to have subordinate command organizations for ground force, navy, and air force elements within their regions, but none have been found for the Strategic Support Force.

## SSF Structure and Components

Organizationally, the Strategic Support Force's operational forces are split into two co-equal, semi-independent branches: the Space Systems Department, which heads up a force responsible

for space operations, and the Network Systems Department, which heads up a force responsible for information operations. Though the force structure of these departments is largely opaque, as the reforms have progressed details have slowly emerged regarding a growing number of personnel transfers, unit consolidations, Military Unit Cover Designator conversions, and in some cases the establishment of entirely new units with no identifiable predecessor. This transitional state complicates any attempt to give a full accounting of structure and command relationships, but some basic inferences can nevertheless be drawn.

First, the SSF appears to have a bifurcated structure, whereby the SSD and NSD act as largely independent, administrative headquarters for their respective forces and the Staff Department serves as an operational headquarters. This arrangement would help explain the apparent administrative oddity of the SSD and NSD having the same grade as the Staff Department, an organization they would normally report to. Such a command structure may better enable the SSD and NSD to independently develop their own officer corps, tailor training to force needs, and prioritize their own capabilities development while allowing the Central Military Commission to integrate their operations in situations where their missions overlap, such as in certain strategic intelligence and counterspace missions.

Second, SSF units have been assigned MUCDs, the numerical codes that the PLA has long used to conceal a unit's true identity in public sources. The SSF's MUCDs fall between 32001 and 32099.[37] Analysis of these designators largely confirms that, as expected, a number of SSF units are beginning to migrate from their old designations to new MUCDs that fall within the SSF's assigned block. However, a select few appear to be newly created or do not align to known units. MUCDs are a useful tool for determining which stage of reorganization the SSF's forces are undergoing, as a new designator is generally a fair indication that their structure, grade, and command relationships have been reviewed, approved, and are likely to remain static throughout the course of the remaining reforms. On the other hand, a unit still using its pre-reform MUCD invites speculation that a new designation awaits after some administrative change or reorganization.

Finally, many SSF forces appear to be organized as "bases," a form of corps leader grade unit that is distinct to the PLA. The space force in particular had already largely been organized as bases prior to the creation of the SSF. Of the former GAD "test bases" [*shiyan jidi*, 实验基地], numbered 20 to 33, the five responsible for space operations have been confirmed to have been transferred to the Strategic Support Force, whereas the remaining bases were transferred to the CMC Equipment Development Department or the services.[38] These bases appear to have retained their previous numerical designations even under the new system. However, a newly

designated unit called the "Strategic Support Force 35th Base" [*zhanlüe zhiyuan budui 35 jidi*, 战略支援部队35基地] now appears to be responsible for some of the space force's space-based survey, mapping, and navigation missions, including the management of military Beidou satellites.[39] The creation or designation of a new SSF base beyond the aforementioned five that are known to exist, with numbering that extends past what was previously the highest numbered PLA base (the 33rd), raises the possibility that there may be more space-related numerical bases in the offing. Additional bases might also be responsible for supporting the space information support and survey, mapping, and navigation missions.

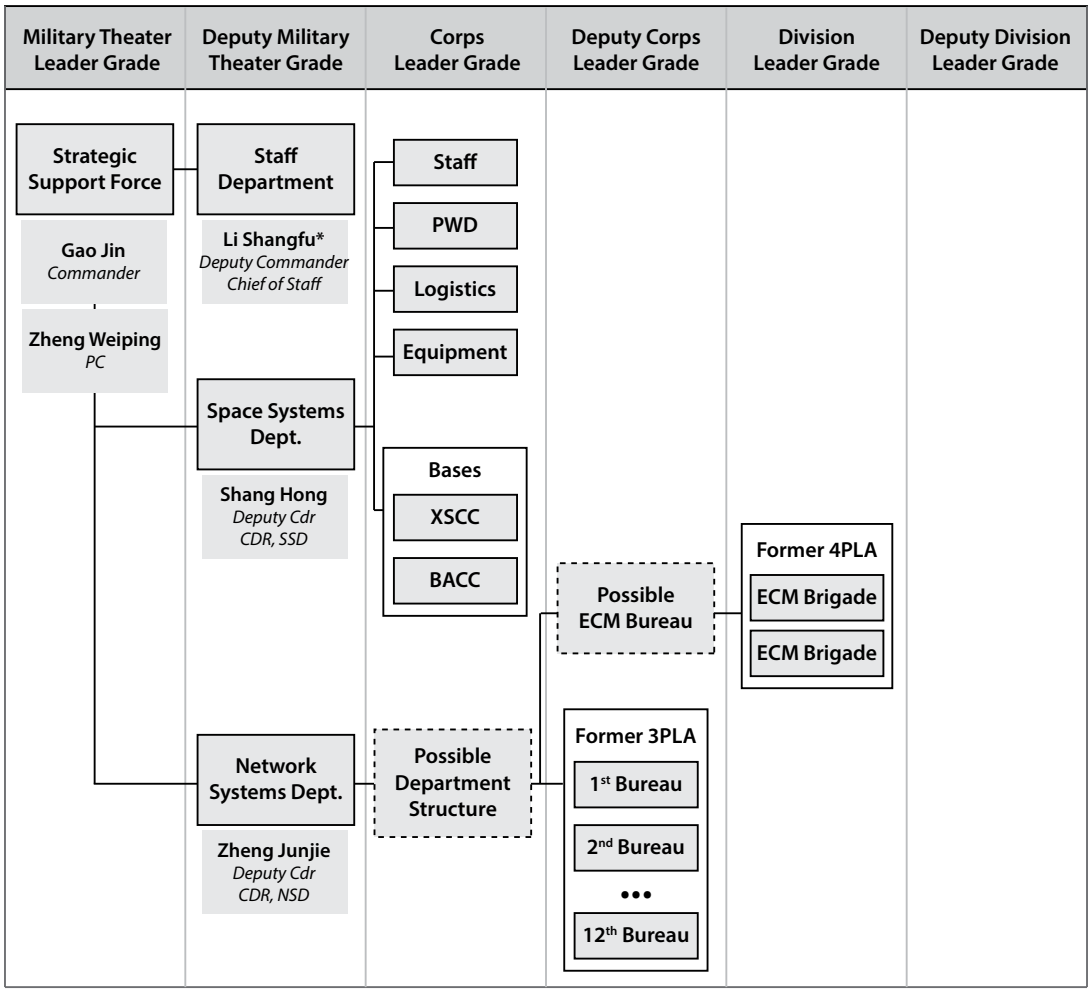
The SSF has also inherited the 311 Base [*311 jidi*, 311基地], also known as China's "Three Warfares Base," from the General Political Department, though its position within the SSF's organizational structure is unclear. The 311 Base is the PLA's sole organization that is publicly known to focus on psychological warfare. Notably, one public record refers to the existence of a "Strategic Support Force Eastern Base" [*zhanlüe zhiyuan budui dongbu jidi*, 战略支援部队东部基地].[40] This invites comparisons to a similar structure used by the newly created Joint Logistics Support Force [*lianhe houqin baozhang budui*, 联合后勤保障部队], which has subordinate bases that align with the five theater commands.[41] These bases could fall directly under the SSF's staff department and serve both space and cyber force personnel or, alternatively, could be a series of bases that fall under the Network Systems Department. The former possibility would help further the SSF mission of supporting the theater commands and may explain the absence of identifiable SSF elements under them—SSF regional bases are still in the process of being created. The latter possibility would answer the question of exactly how the NSD intends to organize the loose and geographically dispersed confederation of cyber, EW, and psychological warfare forces it has inherited.

## A Force in Transition

With reforms scheduled to run from 2015 until 2020, the SSF remains very much a force in transition. Its transitional state complicates efforts to fully understand how it will be permanently organized. There are several peculiarities in the current SSF structure that may either end up as permanent features of its organization (and thus consequential for understanding the SSF's operational concepts), mere transient idiosyncrasies that have been left over from larger structural reforms, or bureaucratic compromises that have yet to be ironed out.

Many of these anomalies relate to the SSF's grade [*jibie*, 级别] structure (see figure 3). The PLA's grade system is separated into 15 grades that correspond to 10 ranks, defining both an organization's and an officer's place in PLA hierarchy. Ranks are occasionally used for ease of

**Figure 3. SSF Grade Structure**




* Li Shangfu is now director of the CMC Equipment Development Department. His replacement as SSF chief of staff has not been identified.

*Key*: BACC: Beijing Aerospace Command and Control Center; CDR: commander; ECM: electronic countermeasure; NSD: Network Systems Department; PC: political commissar; PWD: Political Work Department; SSD: Space Systems Department; XSCC: Xian Satellite Monitor and Control Center.

coordination with foreign militaries, since most other militaries consider ranks to be paramount, but are often not referenced in the PLA's daily practice.

Traditionally in the PLA, an organization's grade, not its commander's rank, has been the determining factor for its authority, shaping which organizations it may answer to, coordinate with, or command. The grade system also defines the potential career paths for officers, providing sequential rungs upon which billets are based.[42] For many officers in the PLA, organi-

zational mergers or streamlining reforms ultimately mean a reduction in billets, which means increased competition over fewer pathways for promotion.[43] For organizations, these changes mean a redefinition of command and coordination authorities, altering relationships within the PLA's command ecosystem. When reorganizing the PLA, planners must be conscious of both officer career paths and organizational responsibilities, balancing the need for structural change against bureaucratic and operational pressures.

Since the SSF is a massive merger between elements of the former GAD and elements of the GSD, these considerations have almost certainly played an important role in decisions about its structure. For instance, one would ordinarily expect that the SSF's Space Systems Department would mirror its Network Systems Department counterpart and have bureaus [*ju*, 局] under its headquarters. This would align with the PLA's overall organizational paradigm wherein "departments contain bureaus, which in turn contain offices" [*bu-ju-chu*, 部-局-处]. Instead the SSD has another layer of departments [*bu*, 部] where bureaus might be expected.[44] This nonstandard structure could either be temporary until the departments can be converted into bureaus, or it could be an indicator that the NSD will defy convention and maintain second-level departments instead of bureaus. Additionally, both the heads of the SSD and NSD are dual-hatted as deputy commanders of the SSF, giving them a deputy theater command leader [*fu zhanqu ji*, 副战区级] grade. The merger and demotion of former GAD elements appears to have created a bureaucratic bottleneck in promotions for much of the space mission's leadership, as many of the senior leaders there, such as the heads of the space launch bases, had already attained corps leader or deputy theater command leader grade. This may help explain the prevalence of former GAD officers in the SSF's leadership, as it was necessary to provide them with billets that accorded with their established grades.

The most consequential and enduring mystery in this regard is that the SSD and NSD appear to be the same grade as the SSF Staff Department, limiting the latter's ability to command and direct their operations. This arrangement may be the result of bureaucratic necessity. Since many of the former GAD launch bases were corps leader grade organizations, the Space Systems Department would need to be at least a deputy theater command leader grade to command them, requiring a grade increase that made it the equal of the Staff Department. Alternatively, it may indicate that SSF structure is in a transitional state, with further changes to come that will move the headquarters as well as the space and cyber forces into a more permanent organizational framework.

### The SSD and China's Space Forces

As noted, the Strategic Support Force's space mission falls under the Space Systems Department, a deputy theater command leader grade organization that has been described as the headquarters of China's military space forces [*junshi hangtian budui*, 军事航天部队], also known informally as its "space force" [*tian jun*, 天军].[45] The initial leadership of this department consists of Major General Shang Hong, who has led it since its inception, Political Commissar Kang Chunyuan, Deputy Commander Hao Weizhong, and Chief of Staff Fei Jiabing.[46] With the exception of Kang, who formerly served as the Lanzhou Military Region deputy political commissar, all are from the former GAD and veterans of China's military space programs.[47]

This reorganization of China's myriad space capabilities into a coherent, unified space force is a response to organizational challenges that arose from space forces being dispersed throughout the military. Previously, the PLA was tasked with executing space missions using assets spread across the GAD and GSD.[48] The SSD has now subsumed nearly every aspect of PLA space operations that were formerly controlled by the GAD and GSD, including space launch and support; space telemetry, tracking, and control; space information support; space attack; and space defense (see table 2). The office overseeing China's manned space missions has stayed with the CMC Equipment Development Department, perhaps in an attempt to avoid the appearance of militarizing China's manned space mission.[49]

Although the bulk of the SSD's operational units and administrative functions are drawn from the former GAD's space cadre, some operational units and missions are drawn from the former GSD. The components brought over from the GSD are primarily related to space-based C4ISR assets, which in the PLA are categorized as "space-based information support" [*tian ji xinxi zhiyuan*, 天基信息支援].[50] For example, although the military intelligence–focused former GSD Second Department [*zongcan er bu*, 总参二部, or *zongcan qingbao bu*, 总参情报部] remains in existence as the new Joint Intelligence Bureau [*lian can qingbao ju*, 联参情报局] under the CMC Joint Staff Department, its former Aerospace Reconnaissance Bureau [*hangtian zhencha ju*, 航天侦察局], responsible for space-based remote sensing and the Yaogan [遥感] series of optical and electronic intelligence satellites, has been separated and transferred over to the SSD.[51] The former GSD Satellite Main Station, which is responsible for satellite uplink, downlink, and managing space-based communication satellites, has also been transferred to the SSD, even as its parent organization, the former GSD Informatization Department's Information Support Base [*xinxi baozhang jidi*, 信息保障基地], has been reorganized under the CMC Joint Staff Department as the Information and Communications Bureau (JSD-ICB) [*lian can xinxi tongxin*

**Table 2. SSF Space Corps Units**

**Space Launch and Support**

| Name | Assessed Grade | Function and Description |
|---|---|---|
| Jiuquan Satellite Launch Center [中国酒泉卫星发射中心]; 20th Testing and Training Base [第20试验训练基地] | Corps Leader Grade | Oldest and largest launch site and the only one that conducts human spaceflight launches. |
| Taiyuan Satellite Launch Center [中国太原卫星发射中心]; 25th Testing and Training Base [第25试验训练基地] | Corps Leader Grade | Launches satellites into sun-synchronous and low-Earth orbits. |
| Xichang Satellite Launch Center [中国西昌卫星发射中心]; 27th Testing and Training Base [第27试验训练基地] | Corps Leader Grade | Launches satellites into geosynchronous orbit. Maintains mobile tracking stations that supply data to other facilities. |
| Wenchang Aerospace Launch Site [文昌航天发射场] | Corps Leader Grade | Completed in 2014. Built to use the new heavy-lift Long March 5 and launch heavier payloads into orbit. |

**Telemetry, Tracking, and Control (TTC)**

| Name | Assessed Grade | Function and Description |
|---|---|---|
| Beijing Aerospace Flight Control Center [北京航天飞行控制中心] | Corps Leader Grade | Responsible for command and control of China's manned spaceflight program. |
| Xi'an Satellite Control Center [中国西安卫星测控中心]; 26th Testing and Training Base [第26试验训练基地] | Corps Leader Grade | Core hub for China's TTC network. Maintains a nation-wide retinue of fixed and mobile TT&C stations. |
| China Satellite Maritime Tracking and Control Department [中国卫星海上测控部]; 23rd Test and Training Base [第23试验训练基地] | Corps Leader Grade | Provides maritime TT&C for China's space launches and intercontinental ballistic missile tests. Maintains a small fleet of *Yuanwang* [远望] tracking ships. |

*ju*, 联参信息通信局] Information Support Base.[52] Finally, the GSD Satellite Positioning Main Station [*weixing dingwei zongzhan*, 卫星定位总站], responsible for managing the PLA's use of China's Beidou navigation satellite constellation, has moved over to the SSD as well.[53] Its parent unit, the operations-focused former GSD First Department's Survey, Mapping, and Navigation

**Table 2. SSF Space Corps Units, cont.**

| | Name | Assessed Grade | Function and Description |
|---|---|---|---|
| Space-Based C4ISR | Aerospace Reconnaissance Bureau [航天侦察局] | Deputy Corps Leader Grade | Responsible for space-based ISR. |
| | Satellite Communications Main Station [卫星通信总站] | Deputy Corps Leader Grade | Responsible for space-based communications and data relay. |
| | Satellite Positioning Main Station [卫星定位总站] | Deputy Corps Leader Grade | Responsible for military use of Beidou navigation system. |

Bureau [*cehui daohang ju*, 测绘导航局], has become the Joint Staff Department Battlefield Environment Support Bureau [*zhanchang huanjing baozhang ju,* 战场环境保障局].

It is currently unclear what responsibilities, if any, the SSF's space force has for antisatellite research, development, testing, and operations, nor is it known whether the SSF has a role in the related discipline of ballistic missile defense (BMD). Both missions could presumably fall under the categories of space attack and defense, respectively, which would place them under the SSF's remit. Alternatively, these missions may be assigned to the PLA Rocket Force, which already has a role in missile operations, or the PLA Air Force (PLAAF), which has already demonstrated a limited capability in both antisatellite missiles and BMD. In August 2017, the DN-3 antisatellite missile was launched from the SSF's Jiuquan Satellite Launch Center, which may indicate that the SSF has responsibility for testing or fielding these systems.[54] The current locations of many of China's offensive space capabilities, including its more experimental co-orbital attack capabilities such as the Shiyan-7 [实验-7, or SY-7] "robotic arm" satellite, remain unknown.[55]

The creation of the SSD nevertheless appears to have resolved at least some of the previous bureaucratic power struggles over space missions between the former GAD, PLAAF, and Second Artillery Force. Although the GAD had long held preeminence in space launch, support, and telemetry, tracking, and control, the capabilities necessary for contesting "space dominance" [*zhikong quan*, 制空权] by holding adversary assets at risk of denial or disruption were split among the three organizations.[56] From the mid-2000s onward, PLAAF leadership forcefully argued that its core responsibility for air defense operations should be extended into space, proposing the strategic operational concept of "integrated air and space operations" [*kongtian yiti zuozhan*, 空天一体作战] as a way toward this coupling.[57] The former PLA Second Artillery Force also promoted itself at various points as the best equipped to carry out the military's space mission set. Its arsenal of short-, medium-, and long-range ballistic missiles, as well as its inherent status as a strategic service, gave it a strong hand in arguing that its existing capabilities

"could be adapted for a space intercept role by reprogramming missile guidance and fusing."[58] At least for the moment, the creation of an independent force with responsibility for PLA space missions provides a definitive conclusion to this long-running three-way dispute, perhaps reflecting a bureaucratic compromise.

There is also a broader question as to whether the SSF's primacy in space and space-based C4ISR will preclude other services from independently developing, operating, or maintaining their own space infrastructure for operations. The PLA's services have been known to defend aggressively against one another's efforts to challenge their primacy in their respective primary domains of operation.[59] It remains to be seen if the PLA's reorganization and the CMC's new functional joint model will relieve pressure on these service rivalries, or if they will intensify as a result of new competition over funding and development of "new-type" capabilities. It is possible that the SSF's space mission may represent a bureaucratic "solution" to the previous fight for space primacy between the PLAAF and Rocket Force.

## The NSD and China's Cyber Forces

The Strategic Support Force's cyber mission has been given to the Network Systems Department, a deputy theater command leader grade organization that acts as the headquarters for the SSF's cyber operations force, sometimes referred to as a "cyber force" [*wang jun*, 网军] or "cyberspace force" [*wangluo kongjian zuozhan budui*, 网络空间作战部队].[60] Despite its name, the NSD and its subordinate forces are responsible for information warfare more broadly, with a mission set that includes cyber warfare, EW, and potentially psychological warfare. Lieutenant General Zheng Junjie was named the NSD's first commander and Lieutenant General Chai Shaoliang as its political commissar.[61] Zheng was the director of the former GSD Third Department (3PLA) [*zongcan san bu*, 总参三部] and commandant of PLA Information Engineering University.[62] Chai previously served as deputy political commissar of the GAD and, before that, of the former Chengdu Military Region [成都军区].[63]

The NSD appears to represent a renaming, reorganization, and grade promotion of the 3PLA. Much as the institutions of the former GSD provided the partial foundation for the creation of the Space Systems Department, they also form the organizational core of the NSD. The Network Systems Department maintains the former 3PLA headquarters, location, and internal bureau-centric structure. In at least one instance, the NSD has been referred to as the "SSF Third Department" [*zhanlüe zhiyuan budui di san bu*, 战略支援部队第三部], mirroring its former appellation.[64]

**Table 3. Former Third Department Units Now Likely under SSF**

| Name of Unit | Notes |
|---|---|
| ***Operational or Administrative Organs*** | |
| 3PLA Headquarters | Now the Network Systems Department (NSD) |
| First Bureau (Beijing) | Assessed to be transferred to NSD |
| Second Bureau (Shanghai) | Assessed to be transferred to NSD |
| Third Bureau (Beijing) | Assessed to be transferred to NSD |
| Fourth Bureau (Qingdao) | Assessed to be transferred to NSD |
| Fifth Bureau (Beijing) | Assessed to be transferred to NSD |
| Sixth Bureau (Wuhan) | Assessed to be transferred to NSD |
| Seventh Bureau (Beijing) | Transferred to NSD |
| Eighth Bureau (Beijing) | Assessed to be transferred to NSD |
| Ninth Bureau (Beijing) | Assessed to be transferred to NSD |
| Tenth Bureau (Beijing) | Assessed to be transferred to NSD |
| Eleventh Bureau (Beijing) | Assessed to be transferred to NSD |
| Twelfth Bureau (Shanghai) | Assessed to be transferred to NSD or Space Systems Department |
| Beijing North Computing Center (Beijing) | Transferred to NSD |
| ***Research Institutes*** | |
| 56th Research Institute | Transferred to NSD |
| 57th Research Institute | Transferred to NSD |
| 58th Research Institute | Transferred to NSD |
| ***Academic Institutions*** | |
| Foreign Language Institute | Now PLA IEU Luoyang Campus |
| Information Engineering University (IEU) | Transferred to NSD |

The bulk of China's strategic cyber espionage forces were previously contained within the technical reconnaissance-focused GSD Third Department, which has been moved en masse into the NSD (see table 3). The Third Department's cyber missions were largely handled by its 12 technical reconnaissance bureaus [*jishu zhengcha ju*, 技术侦察局], which were responsible for both cyber espionage and signals intelligence.[65] While only three of the former bureaus can be fully confirmed to have moved into the NSD, this most likely reflects incomplete public data rather than an incomplete transition. The former GSD's 56th, 57th, and 58th Research Institutes, which previously provided research, development, and weaponization support to the technical reconnaissance mission, have also moved to the NSD.[66] Former military academic institutions,

such as the PLA Information Engineering University [*xinxi gongcheng daxue*, 信息工程大学] and Luoyang Foreign Language Institute [*luoyang waiyu xueyuan*, 洛阳外语学院], have also moved to the NSD and in some cases have been consolidated.[67]

The centralization of China's strategic cyber forces is a key feature of the Network Systems Department. The NSD appears designed to address the operational coordination challenges that previously arose from the structure of the former GSD. Traditionally, computer network attack was handled by the GSD Fourth Department (4PLA), while the PLA counter-network defense mission has been handled by the GSD Informatization Department. It now appears that the former 4PLA's computer network attack forces have been transferred to the SSF to integrate with the cyber espionage elements of the former Third Department (see table 4).[68] However, it is noteworthy that the NSD does not appear to have integrated the PLA's counter-network defense mission, which remains with the JSD-ICB Information Support Base under its Network Security Defense Center [*wangluo anquan fangyu zhongxin*, 网络安全防御中心].[69]

### The SSF and EW

Compared with the space and cyber missions, China's strategic electronic warfare mission has historically been far less divided and compartmentalized, having been concentrated almost entirely within the former GSD Fourth Department. The former 4PLA, which was also responsible for radar and computer network attack, has now been split by the reorganization along administrative and operational lines, with various elements either abolished, reorganized, or transferred to the Joint Staff Department and Strategic Support Force. At the top level, the former 4PLA headquarters has been moved to the Joint Staff Department, where it has been reconstituted as the new joint force Network-Electronic Bureau (JSD-NEB) [*wangluo dianzi ju, wang dian ju*, 网络电子局, 网电局].[70] In its new form, it likely oversees management of the cyber and EW missions across the entire Chinese military, including the SSF, theater commands, and services. The 4PLA's military academy, the PLA Electrical Engineering Institute [*dianzi gongcheng xueyuan*, 电子工程学院], has been subsumed by the National University of Defense Technology (NUDT) [*guofang keji daxue*, 国防科技大学] to become the NUDT Electronic Countermeasure Institute [*dianzi duikang xueyuan*, 电子对抗学院].[71] Meanwhile, 4PLA's GSD 54th Research Institute, responsible for research and development of operational electronic and network countermeasures, has moved over to the Strategic Support Force, likely under the Network Systems Department.[72]

At a lower, operational level, at least some of the 4PLA's EW units have been reassigned to the SSF, with Chinese media reports mentioning unidentified "electronic countermeasure

brigades" under the new force and public documents revealing former 4PLA units now operating under an SSF MUCD designation.[73] Prior to the reforms, the 4PLA maintained a number of electronic countermeasure brigades, detachments, and stations nationwide, none of which has been visibly accounted for in the PLA's new structure.[74] Nevertheless, the reassignment of the GSD 54th Research Institute is a vital clue that EW now falls under the aegis of the NSD, and the former 4PLA's monopoly on strategic electronic warfare makes it a near certainty that some or all of these units have been assigned to the SSF (see table 4).

Integrating the cyber warfare and EW elements of the former 3PLA and 4PLA is a crucial step toward fully realizing a long-held PLA theory of how best to fight information warfare known as integrated network and electronic warfare, which envisions the close coordination of cyber and electronic warfare forces in both capabilities development and operational use. According to this school of thought, the integration of information technology on the battlefield has created a combined "network and electromagnetic space" [*wangdian kongjian*, 网电空间] such that cyber and EW forces "cannot be mutually exclusive, with each [force] fighting [its] own battles."[75] On a more concrete level, integrated network and electronic warfare was conceived by former 4PLA head Dai Qingmin in the early 2000s and represented 4PLA's side of a bureaucratic turf war between 3PLA and 4PLA as to the proper division of missions between the two organizations.[76]

With the adoption of INEW as mainstream PLA thinking, 4PLA took on both the GSD's offensive cyber and electronic countermeasures missions in a partial realization of the concept, but its broader implementation remained largely incomplete.[77] Responsibilities for the cyber and electromagnetic domains remained divided at the strategic level, with the Fourth Department responsible for both network and electronic countermeasures (offense) and the Third Department responsible for cyber espionage and traditional radio-frequency signals intelligence (reconnaissance and espionage). The Strategic Support Force's merging of the two departments' operational responsibilities could bring the concept full circle, creating a unified force for warfighting in the network and electromagnetic space.

The status of this integration is unclear. For now, at least, the integration appears to be notional and largely the result of renaming and functionally realigning rather than at the deeper level of combining of personnel, systems, and culture. That said, the reforms are still incomplete and the next stage is intended to focus on below-the-neck reforms and integration, under which this would presumably fall. Still, it is unclear how foreign observers would measure or understand the progress in these actions, as they produce fewer appearances than larger scale changes. In any case, if successful in achieving deeper integration, this force will be fully empowered to

**Table 4. Former Fourth Department Units Now Likely under SSF**

| Name of Unit | Notes |
|---|---|
| ***Operational and Administrative Units*** | |
| 4PLA Headquarters | Transferred to Joint Staff Department as a new Network-Electronic Bureau |
| Electronic Countermeasure Brigade (ECM) (Langfang) | Assessed to be transferred to Network Systems Department (NSD) |
| Langfang ECM Brigade Detachment (Yingtan) | Assessed to be transferred to NSD |
| Electronic Countermeasure Brigade (Beidaihe) | Transferred to NSD |
| Beidaihe ECM Brigade Detachment (Nicheng) | Transferred to NSD |
| Electronic Countermeasure Center | Potentially merged with Joint Network-Electronic Countermeasure *dadui* |
| Satellite Main Station (Beijing) | Assessed to be transferred to NSD or Space Systems Department (SSD) |
| Regional Satellite Station (Hainan) | Assessed to be transferred to NSD or SSD |
| ***Research Institutes*** | |
| 54th Research Institute | Transferred to NSD |
| ***Academic Institutions*** | |
| Electrical Engineering Institute | Now National University of Defense Technology Electronic Countermeasures Institute |

conduct both espionage and offense operations, a recognition of the ways in which the two disciplines often reinforce and depend on one another on the modern battlefield.

The JSD-NEB now seems to be pushing the INEW concept force-wide as the main successor of the 4PLA, likely overseeing force development and warfighting efforts in the Strategic Support Force, other services, and theater commands. Initially, it seemed plausible that the former 4PLA might move to the SSF to form something along the lines of a hypothetical "Electronic Systems Department" that would stand alongside the SSD and NSD.[78] The fact that 4PLA headquarters has instead been integrated in the Joint Staff Department as the Network-Electronic Bureau makes it more likely that strategic electronic warfare units have been merged with the NSD to better align with the combined network and electronic countermeasures concept that the JSD-NEB is establishing throughout the entire PLA.[79] The "network-electronic" grouping has

also been spotted in other post-reform PLA organizations, such as the national joint force Network-Electronic Countermeasures *dadui* [大队] and a Theater Command Network-Electronic Countermeasure *dui* [队].[80] It is not clear if the NSD has inherited any management institutions from the former 4PLA, or if it will create new bureaus specifically for the purpose of leading the new operational EW units under its command.

### The SSF and the Three Warfares

The Strategic Support Force also appears to have incorporated elements of the military's psychological and political warfare missions, a result of a subtle yet consequential reorganization of China's political warfare forces. Before the reforms, the former General Political Department had primary responsibility for carrying out military political warfare. This mission was encapsulated in a concept developed in the early 2000s known as the Three Warfares, a unique Chinese political warfare model that calls for the coordinated use of psychological warfare [*xinli zhan*, 心理战], public opinion warfare [*yulun zhan*, 舆论战], and legal warfare [*falü zhan*, 法律战] to establish "discursive power" [*huayu quan*, 话语权] over an adversary—that is, the power to control perceptions and shape narratives that advance Chinese interests and undermine those of an opponent.[81] The former General Political Department separated responsibilities for these missions at strategic and operational levels, with the former Liaison Department [*lianluo bu*, 联络部] responsible for the broader mission of political warfare and the 311 Base responsible for more operational aspects of political warfare and psychological operations against Taiwan.[82] While the 311 Base was under the command of the General Political Department in peacetime, in a conflict scenario, the base, a deputy corps leader grade organization, and its six subordinate regiments, would form the core of China's psychological warfare forces in information operations campaigns.[83]

The reforms shook up this arrangement, incorporating the General Political Department into the Central Military Commission as the new CMC Political Work Department and reassigning the 311 Base to the Strategic Support Force.[84] Although the base is unaccounted for in known portions of the SSF's structure, it could potentially fall under the SSF's Political Work Department or, perhaps more likely, the Network Systems Department. The latter possibility would see the NSD in command of the full spectrum of information operations—not only cyber but also electronic and psychological warfare. The move itself appears to remove organizational impediments to coordination across the information operations disciplines, integrating them in peacetime to ease their transition into a wartime structure. PLA scholars have stressed the importance of both psychological and political operations in shaping the

strategic situation ahead of conflict.[85] Integrating the 311 Base's operational forces with the SSF's space, cyber, and electronic missions empowers psychological operations forces with cross-domain intelligence and helps maximize the impact of information operations on an adversary's psychology.

What is unclear is what responsibilities the CMC Political Work Department will have for political warfare and, therefore, psychological operations. The former GPD Liaison Department, which previously served as the PLA's political warfare command center, is unaccounted for in the PLA's structure; it has most likely remained with the CMC Political Work Department in some form. The PLA's inherent status as a party army (not a national one) imposes on its psychological operations forces an additional imperative to ensure ideological loyalty and push party ideals as part of its operational strategy. It is possible that the 311 Base's move signals a "decoupling" of sorts between political and psychological warfare, which have traditionally sat uncomfortably at the intersection of the General Political Department's political command and the GSD's operational command.[86] Both the PLA's revised 2010 Political Work Guidelines and the 2013 edition of the *Science of Military Strategy* indicate the need for psychological operations to more closely align with traditional, nonpolitical, military information warfare forces, and the reorganization may be a direct reflection of this imperative.[87]

## Joint Command and the SSF

The reforms have also substantially altered the command context for many of the missions now under the Strategic Support Force, redefining longstanding organizational relationships and creating new responsibilities across the PLA command bureaucracy. The CMC's new Joint Staff Department may have responsibility for relaying CMC operational decisions to the SSF.[88] Understanding how each of the different components of this organization interface with the SSF is crucial to understanding PLA command and control during a wartime or crisis scenario.

The JSD was based on the former GSD, which had effectively been triple-hatted in the past—serving as a notional joint command headquarters, ground force headquarters, and as administrative headquarters for strategic missions and units. The reforms split these responsibilities apart, forming a new ground force headquarters, establishing the Strategic Support Force from pre-existing space, cyber, and EW forces, and elevating both the GSD and many, but not all, of its subordinate organs to the Central Military Commission as the Joint Staff Department. JSD bureaus oversee various aspects of military command, including operations, intelligence, cyber and electronic warfare, communications, and battlefield environment support. However, the precise manner in which the JSD commands the SSF remains unclear.

### Operational Command in Peacetime and Wartime

In peacetime, the SSF appears to fall under the command of either the CMC's Joint Staff Department Operations Bureau [*liancan zuozhan ju*, 联参作战局] or its Joint Operations Command Center [*liancan zuozhan zhihui zhongxin*, 联参作战指挥中心], which are both responsible for central command and control of both the services and theater commands. Official media state that the center acts as a "strategic command" over services and theater commands.[89] In the previous Joint Staff Department Operations Bureau incarnation as the GSD First Department, it had a set of subordinate bureaus responsible for different types of operations, including both service bureaus, such as the Air Force Operations Bureau [*kongjun zuozhan ju*, 空军作战局] and Navy Operations Bureau [*haijun zuozhan ju*, 海军作战局], as well as functional bureaus such as the Special Operations Bureau [*tezhong zuozhan ju*, 特种作战局] and Information Operations Bureau [*xinxi zuozhan ju*, 信息作战局].[90] Some of these subordinate bureaus appear to have survived and been reorganized as offices [*chu*, 处], though only two have been definitively confirmed to exist: the Overseas Operations Office [*haiwai xingdong chu*, 海外行动处][91] and the Air Traffic Control Office [*kongguan chu*, 空管处].[92]

Since responsibilities for operations have shifted from the services to theater commands, it is not clear whether the former service-centric operations bureaus will ultimately survive or be replaced by geographic bureaus that directly align with theater commands. In any case, there is no clear subordinate office that would appear to be tasked with directing SSF operations. Given the SSF's mission, the chief candidate would be along the lines of a hypothetical "information operations office," a successor organization to the information operations bureau under the Operations Department before the reforms. However, an office that has clear authority over the SSF has yet to be identified.

Prior to the recent reforms, the PLA's plans for a wartime campaign entailed shifting into "operations groups" [*zuozhan jiqun*, 作战集群], temporary entities at the strategic, theater, and tactical levels that would act as joint force commands and direct operations for a particular domain, region, or type of wartime activity.[93] If this basic structure persists, the SSF will likely constitute the core component of an information operations group (IOG) [*xinxi zuozhan jiqun*, 信息作战集群], a joint force wartime construct dedicated to waging information warfare.[94] In his authoritative 2013 work *Lectures on the Science of Information Operations*, Major General Ye Zheng stated that in wartime the PLA would stand up an IOG commanding all aspects of information warfare activity.[95] Its missions would be organized as a series of subordinate elements, referred to as "groups" [*qun*, 群], for mission sets including cyber warfare, EW, psychological warfare, air

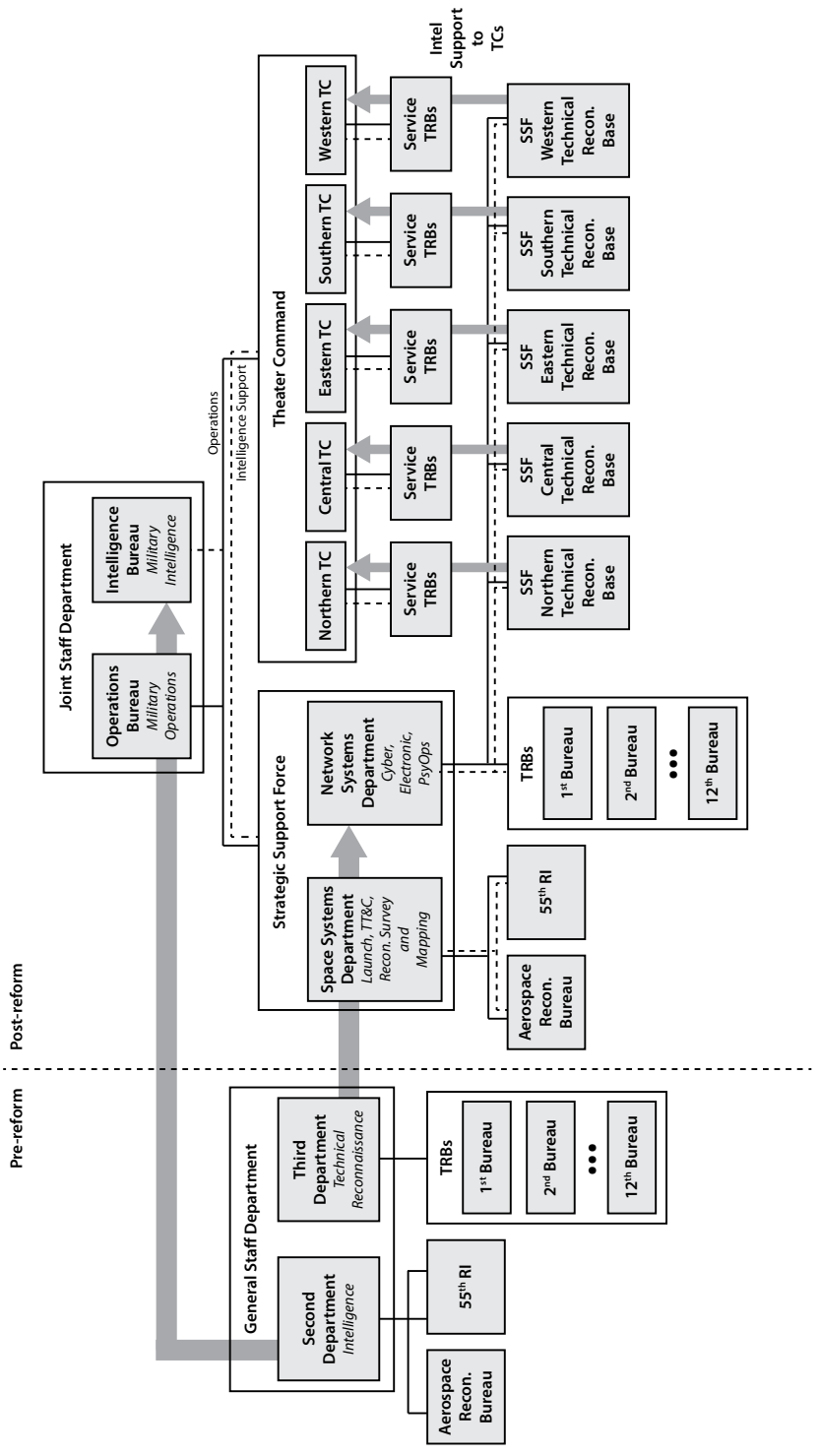
defense electronic countermeasures, and information support.[96] As operations groups are further differentiated at the strategic, theater, and tactical levels of warfighting, it is plausible that any IOGs would be similarly tiered with national-level, campaign, and/or theater-level iterations.[97]

The IOG structure used by the PLA prior to the recent reforms is in many ways the predecessor to the new joint command structure in that it similarly established joint command mechanisms overseeing individual service components at the national and theater levels. The creation of the theater commands may have obviated the need to shift the PLA into a wartime structure for regional campaigns, but the need may still be present at the national level. The Joint Operations Command Center likely facilitates command and control for national strategic missions, but it remains unclear how the organization arranges operational groupings across the services for these purposes. As of now, no joint force construct has been identified under the Joint Operations Command Center that would serve as a standing IOG. Instead, the Strategic Support Force appears to serve both operational and administrative roles. This would mean that the SSF is not a direct analog to a wartime IOG, but rather a force that is optimized for seamless transitioning to a more operational footing. However, an IOG may still be necessary to integrate information operations capabilities from the various services at the national level.

### Intelligence and Technical Reconnaissance

The reforms also substantially reorganized the intelligence responsibilities of the former GSD, creating a new Joint Staff Department Intelligence Bureau out of the former GSD Second Department as well as separating out and centralizing the strategic-level technical collection organizations under the Strategic Support Force (see figure 4).[98] At the national level, this change institutionalizes the PLA's long-standing distinction between "intelligence" [*qingbao*, 情报], which encompasses all-source analysis supporting command decisionmaking, and "technical reconnaissance" [*jishu zhencha*, 技术侦察], which refers to technical intelligence collection directly supporting military operations.[99] The structure appears to maintain the prior arrangement of intelligence flow, whereby "all military intelligence flowed upward through the GSD."[100] The new Joint Staff Department Intelligence Bureau serves the GSD's former role, incorporating intelligence from the theater commands, each of which in turn has its own bureaus responsible for operational and tactical intelligence analysis.[101] Theoretically, the establishment of a separate ground force headquarters and the incorporation of the Intelligence Bureau into the joint staff gives it more latitude to move away from its army-dominated past and direct intelligence resources to critical missions based on operational needs.[102] However, it remains unclear what exact responsibilities the bureau will have beyond the traditional focus on all-source analysis

**Figure 4. PLA's Military Intelligence System in Transition (Notional)**




*Key*: PsyOps: psychological operations; RI: reconnaissance and intelligence; TC: theater command; TRB: technical reconnaissance bureau; TT&C: telemetry, tracking, and control.

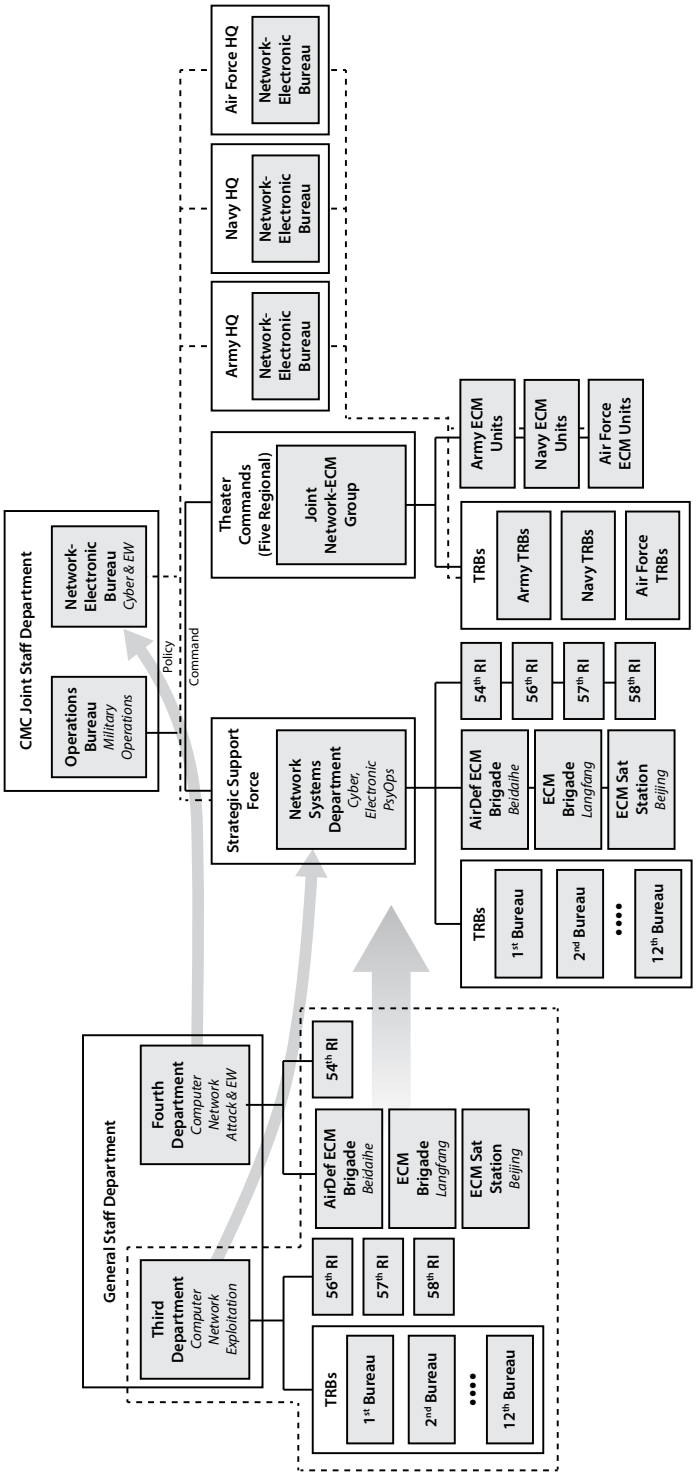
and human intelligence and whether, in light of its elevated role, it will take on more bureaucratic responsibilities for managing intelligence demands and balancing collections requirements among different competing interests within the PLA.

### Network and Electronic Warfare

The Joint Staff Department's Network-Electronic Bureau creates a new force-wide structure for the management of the cyber and electronic warfare missions in the Strategic Support Force, theater commands, and other services. The creation of the JSD-NEB suggests that the PLA is maintaining a dual-echelon structure for cyber and EW, with the SSF's cyber force assuming responsibilities for strategic national-level operations that previously rested with former GSD units, while the services and theater commands continue to be responsible for cyber and EW operations at the operational and tactical levels (see figure 5). The precise responsibilities of the JSD-NEB are unclear, but likely include oversight and integration functions such as issuing operational guidance, deconflicting areas of responsibility, and establishing rules of engagement. In one of the few public mentions of the organization tied to a specific sphere of interest, JSD-NEB Chief Major General Wang Xiaoming and Deputy Bureau Chief Senior Colonel Lin Shishan held a symposium with international law experts at the Wuhan School of Law, discussing international law in cyberspace and "Tallinn 2.0," a study on applicability of international law to cyber operations performed by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.[103]

The reforms have also established a national joint Network-Electronic Countermeasure dadui.[104] This organization appears to have corresponding lower echelon elements in the theater commands, called Network-Electronic Countermeasure dui, which are likely made up of regional service branch and theater command cyber and EW elements.[105] These organizations mirror the former force-wide network of electronic countermeasure centers (ECM centers) [dianzi duikang zhongxin, 电子对抗中心], which were composed of a national center collocated with the former 4PLA and lower echelon elements in the former military regions.[106] Based on the ECM center's public research, its mission appears to have focused on electronic support measures, electronic intelligence, and targeting in the electromagnetic domain.[107] The similarities suggest the former ground force ECM centers were most likely reorganized into joint force Network-Electronic Countermeasure dadui and dui, expanding the scope of their mission to include network reconnaissance and targeting. These organizations suggest that the SSF does not, as some initially thought, have a monopoly of force in cyberspace, but rather continues to share the mission with other components in the PLA.

**Figure 5. Network-Electronic Units in Transition**




*Key:* CMC: Central Military Commission; ECM: electronic countermeasure; EW: electronic warfare; HQ: headquarters; PsyOps: psychological operations; RI: reconnaissance and intelligence; TC: theater command; TRB: technical reconnaissance bureau; TT&C: telemetry, tracking, and control.

### Information and Communications

The new Joint Staff Department's Information and Communications Bureau, reorganized from the former GSD Informatization Department, has inherited responsibilities for force-wide management of information systems, communications, and support for high-level warfighting command and control. The JSD-ICB includes the PLA's Information Support Base [*xinxi baozhang jidi*, 信息保障基地], which has similarly moved over to the JSD.[108] However, the Strategic Support Force's control of critical ground-based satellite communication infrastructure and primacy in operating space-based data relays may indicate it is a primary organization responsible for routing and supporting information flows through outer space, which would imply an overlap with what we understand to be the JSD-ICB's responsibilities. It remains unclear if the SSF will inherit regional communications ground stations for downlink and uplink or whether those will be operated directly by the Central Military Commission, by other services, or by the theater commands. It is worth noting that the Information Support Base appears to have maintained at least some of its subordinate communications regiments through the reforms, raising questions as to whether it might contain a joint "information support force" in the same vein as the Joint Logistics Support Force.[109]

## The SSF's Strategic Missions and Roles

The Strategic Support Force demonstrates China's evolving understanding of how information serves as a strategic resource in warfare. The PLA recognizes that harnessing outer space, the cyber domain, and the electromagnetic spectrum—and denying their use to adversaries—are paramount needs if the PLA is to attain superiority in a conflict. These three domains are the primary conduits by which a military force collects, processes, transmits, and receives information. If a force is denied use of these domains, the informationized system-of-systems infrastructure that underpins modern military operations cannot properly function. For the first time in the PLA's history, the creation of the Strategic Support Force largely unifies both responsibility for fielding critical systems in these domains and conducting operations to dominate each domain's battlespaces.

These two missions, frequently summarized as "information support" and "information warfare," align in large part with the composition of the SSF's subordinate space and cyber forces. This unity of organizational design and mission set is likely to substantially improve the PLA's ability to achieve information superiority in a conflict. The reforms come at a time when

the military's mandate from Xi Jinping to modernize and operate further from China's shores has placed growing demands on China's information support and information warfare forces.

### Strategic Information Support

The first commander of the SSF, General Gao Jin, has emphasized the force's role in information support by stating that the SSF provides vital "support for safeguarding and raising up an 'information umbrella' [*xinxi yusan*, 信息雨伞] for the military system, which will be integrated with the actions of our land, sea, and air forces and rocket forces throughout an entire operation, [and] will be the key force for victory in war."[110] General Gao never expands on what he means by an information umbrella, but much can be inferred from a straightforward look at the types of information support the Strategic Support Force is uniquely positioned to provide.

The SSF's space force contains what the 2013 *Science of Military Strategy* refers to as the "strategic brace support" [*zhanlüe zhicheng*, 战略支撑] of space-based intelligence and communications, both of which are functions that AMS strategists envision as the primary role for space forces in the foreseeable future.[111] The terms used by authoritative sources, such as *brace support* and *information umbrella*, all carry connotations of support and extension, in this case by advancing the PLA's ability to conduct and sustain operations both within Chinese territory and in areas abroad that China understands to be vital to its national interests.

While the SSF's role in strategic information support largely derives from the plethora of intelligence and communications assets under its space force, the cyber force also maintains a deep bench of technical collection capabilities that are consequential even beyond offense and espionage operations within the cyber domain. SSF information support missions can be divided into five primary functions it offers across the military:

- centralizing technical intelligence collection and management
- providing strategic intelligence support to theater commands
- enabling PLA power projection
- supporting strategic defense in the space and nuclear domains
- enabling joint operations.

*Centralizing Technical Intelligence Collection and Management*

The Strategic Support Force commands a wide array of national-level technical collection assets received from the former organizations that now make up the bulk of its force. This includes space-based electro-optical imagery intelligence, synthetic aperture radar, electronic intelligence platforms from across the GSD and GAD, electronic support capabilities from the former Fourth Department, and strategic, long-range ground-based collection systems from the former Third Department.[112] Before the reorganization, management of these systems was siloed (with each answering only to its parent general department) and differentiated based on source. While the reorganization places all these collection assets under the same organization, the advantages inherent to centralization depend heavily on how well the technical systems, data, and organizational procedures that underpin those operations can be integrated. From a purely organizational standpoint, control over these sources of intelligence potentially allows the Strategic Support Force to gain the comprehensive perspective necessary to identify gaps in collection, assess emerging needs, and tailor operations and acquisitions to address shortfalls and new challenges. In short, the sheer breadth of what the SSF can see and hear empowers it to play a decisive role in China's comprehensive domain awareness and national defense far beyond that of any single organization that has come before.

*Providing Strategic Intelligence Support to Theater Commands*

While the theater command technical reconnaissance bureaus and theater-subordinate service elements maintain their own collection capabilities, they are largely focused on operational- and tactical-level intelligence, surveillance, and reconnaissance with limited coverage beyond their regional areas of responsibility. Collection is further hindered by the logistical and geographical limitations of the collections platforms themselves. Limited-range drones, surveillance planes, and shore-based radar provide valuable reconnaissance, but do not provide the type of comprehensive domain awareness necessary for actionable early warning.[113] The Strategic Support Force's space-based surveillance capacity can thus significantly extend the range of the theater command commanders' battlefield awareness, filling critical gaps in their intelligence collection.[114]

The SSF's primacy in space-based intelligence collection also places it in a unique position to develop identifiers on foreign military targets. These identifiers, which can be in the form of specific emitter signatures, signal parameters, radar signatures, infrared heat signatures, or even imagery profiles, can help detect, identify, track, and target certain operational platforms and weapons systems. The development of these indicators requires long-term technical collection

on specific platforms and thus are a direct function of opportunities for surveillance, giving space-based technical collection systems a clear advantage over their terrestrial counterparts. The ability to conduct space-based intelligence collection on foreign military assets thus gives the Strategic Support Force a primary role in developing these indicators, feeding them back to intelligence systems and disseminating them to operational and tactical units in the theater commands for joint force early warning, air defense, and area surveillance. In addition, the SSF may also play a similar role for nonkinetic targeting in the cyber and electromagnetic domains, where it is similarly well-positioned to identify spectrum allocation for foreign adversary sensors, communications, and radar systems for jamming and foreign adversary cyber infrastructure for targeting, intrusion, and compromise.

*Enabling PLA Power Projection*

The SSF enables and sustains the PLA's ability to project power in the East and South China seas and into areas beyond the first island chain. The SSF is said to field assets that cover the entirety of the "information chain," including space-based surveillance, satellite relay and communications, and telemetry, tracking, and navigation, all of which are necessary to support these types of remote operations.[115] Long-range precision strike, far seas naval deployments, long-range unmanned aerial vehicle reconnaissance, and strategic air operations all rely to varying degrees on infrastructure over which the SSF now wields exclusive control. Conventional strike, the most critical component of both the PLA's nonnuclear deterrence posture and its "counterintervention" strategy, is a prime example.[116] Despite being conducted primarily by the PLA Rocket Force, the PLA's long-range conventional strike mission depends heavily on the SSF to support operations, from initial detection, identification, and targeting, to guidance and battlefield damage assessment.

The Strategic Support Force's monopoly on space-based information infrastructure similarly places the service in a position to play an indispensable role in enabling the PLA Navy to operate in the far seas. While providing traditional intelligence support on enemy movement, early warning, and maritime surveillance, the SSF will also provide more foundational "battlefield environment support" [*zhanchang huanjing baozhang*, 战场环境保障], a term the PLA uses to describe battlespace-relevant survey, mapping, meteorological, oceanographic, and navigation information.[117] This knowledge-base is a critical factor for command decision-making in ship movement and operational planning. Placing China's growing fleet of maritime surveillance satellites, dual-use oceanographic and hydrological satellites, and expanding constellation of Beidou navigation satellites under the Strategic Support Force puts it in a primary

position to provide this type of information. The expansion of the Beidou constellation also diminishes China's reliance on the U.S.-produced global positioning system. The constellation is expected to have global coverage by 2020, extending navigation assurance for naval deployments worldwide.[118]

*Supporting Strategic Defense in the Space and Nuclear Domains*

Although the SSF's responsibilities for antisatellite missile operations, ballistic missile defense, and space-based kinetic operations are unclear, its monopoly on space surveillance and early warning means it will at a minimum play a critical role in supporting these missions. Space surveillance—the ability to detect, identify, and track objects in space—is a prerequisite capability for both antisatellite and ballistic missile defense.[119] The SSF's space force has inherited three major telemetry, tracking, and control centers in Beijing and Xi'an and a fleet of *Yuan Wang*–class [远望] tracking ships. Each center provides varying degrees of space surveillance capabilities as well as telemetry functions for China's satellites, space launches, and long-range missiles. The military is also known to maintain four large phased-array radars in Huian, Korla, Longgangzhen, and Shuangyashan, possibly under the former GSD Third Department, that are capable of tracking objects in support of either counterspace or BMD operations.[120] The former 4PLA's nonkinetic counter-space mission likely means it also possessed a ground-based space tracking and surveillance apparatus, which it would have used to feed targeting data to its satellite jamming platforms.[121]

*Enabling Joint Operations*

The SSF's role in strategic information support directly enables joint operations by providing a connective substrate that helps to integrate disparate units and systems from the PLA's four services. The SSF's ability to provide the information umbrella of space-based C4ISR, intelligence support, and battlefield environment assessments helps forge a common intelligence picture among joint forces within each theater command, a fundamental requirement for fulfilling the PLA's mission of winning "informationized local wars."[122] According to PLA commentary, the SSF ensures the "centralized management, centralized employment, and centralized development" of support resources and acts as an "important support" for the PLA's joint operation "system of systems."[123] At the time of its establishment, Xi Jinping spoke of the need for the SSF to support system-of-systems integration, technical interoperability, information-sharing, and intelligence-fusion among the services.[124] The deputy director of the SSF's 54th Research Institute,

Lü Yueguang, goes further and states that "information-dominant system-of-systems integration" challenges will become the "fundamental requirement for future joint operations."[125]

### Strategic Information Operations

In addition to its strategic information support role, the SSF is the primary force for information warfare in the Chinese military, responsible for achieving "information dominance" in any conflict. The *Science of Military Strategy* and other authoritative sources call for the coordinated employment of space, cyber, and electronic warfare as strategic weapons to achieve these ends, arguing that the PLA must "paralyze the enemy's operational system of systems" and "sabotage the enemy's war command system of systems" in the initial stages of a conflict while protecting its own.[126] These concepts are not unique to the Chinese military; many modern militaries emphasize the importance of information dominance, underscoring it as a prerequisite to victory on the battlefield.

The SSF's importance in strategic information warfare is best understood in the context of challenges posed by an "information warfare campaign," the conceptual wartime front where the SSF's forces—and an information operations group—would be employed. This campaign is likely to be a complex, multidimensional set of operations that incorporates kinetic, space, cyber, electronic, and psychological actions through all phases of conflict, and with each discipline of information operations having specific strengths at difference phases of a crisis or conflict.[127] Psychological and electronic warfare, for example, are key in the pre-crisis period to raise the political and military risks associated with aggression. EW has the potential to be a key signaling mechanism for the PLA, due to its ability to bridge the gap between cyber operations, which have a high opportunity cost in terms of blown access when used for signaling, and kinetic strikes, which mark a transition to open warfare. Electronic warfare is the workhorse in Chinese information operations and is frequently portrayed as inherently defensive (in the broadest sense of the term), pulling double duty as both a tool of coercion and information denial. China's evolving concept of "cyber-electromagnetic sovereignty" raises the possibility that the PLA will one day declare the right to deny or degrade satellite reconnaissance aimed at its territorial claims and space-based platforms, which could indirectly be understood as holding its assets at risk, complicating U.S. efforts to project power in the region.

If China's strategic objectives cannot be secured without escalating into an overt conflict, the twin disciplines of cyber operations and precision kinetic strike will likely be employed in concert by the PLA in any first strike, though PLA writings on the nature of informationized warfare suggest that such coordination is only possible once conflict is deemed inevitable

and China has verifiably achieved information dominance. Both cyber operations and kinetic strike offer first-mover advantages to an attacker willing to preempt its adversary, although the intended effects may not be durable or reliable during the transition from peacetime to wartime. However, these capabilities are also prone to denial, counterattack, and uncertain effects. In the best case scenario, however, Chinese writings emphasize that the employment of cyber and kinetic strikes can create a self-reinforcing cycle that paralyzes an adversary at the outset of conflict, cementing one's own information dominance and quickly securing the adversary's compliance.[128]

The relative prominence of the information warfare disciplines shifts once again after the threshold of war is breached and protracted conflict ensues, with cyber warfare losing importance compared to electronic warfare and kinetic strike. Electronic warfare will be a key standoff weapon in any conflict that China is likely to fight, offering the potential to significantly diminish the intelligence collection and information processing capacity of an adversary even as enemy units come within range of the growing web of air, submarine, surface, and missile threats that China is extending out along its periphery. Once outright conventional warfare begins, kinetic strike once again becomes dominant, and psychological operations serve as a tool to maintain the populace's resolve, weaken the enemy's will, and shape diplomatic and political narratives in order to better enable the successful conclusion of the conflict on terms favorable to China.

The SSF evolves the PLA's ability to conduct information operations in both peacetime and wartime in a number of ways, namely, integrating these disciplines of information warfare into a unified force, integrating cyber espionage and offense, unifying information warfare campaign planning, and unifying responsibilities for information warfare command and control. This unity of command, planning, and force development enabled by the SSF potentially realizes the PLA objective to conduct the type of complex, coordinated set of operations an information warfare campaign would require.

*Realizing "Integrated Information Warfare"*

The difficult prospect of maintaining readiness in an ever-changing information environment is a key challenge that the SSF's structural changes are intended to surmount, integrating across divisions in a way that can play to the unique realities of warfighting in the information domain. In this regard, the SSF effects a sort of "integrated information warfare," unifying China's myriad and dispersed forces across three key dimensions. First and most importantly, the force merges espionage and offense disciplines across electronic, cyber, and space warfare.

Secondly, the SSF merges all the types of strategic warfighting operations that take place primarily in information domains (as opposed to physical battlespaces) under a single cohesive force. Both changes are necessary preconditions to implement the third and most important dimension: peacetime-wartime integration. By consciously mirroring the wartime IOG construct during peacetime, the PLA is better enabled to conduct intelligence preparation of the battlespace, cohesively plan cross-domain and cross-discipline information operations campaigns, and develop capabilities suited to the evolving realities of conflict.

*Integrated Cyber Espionage and Offense*

The creation of the Strategic Support Force optimizes China's preparation for conducting strategic information operations by reducing the degree of separation between its espionage and offense-focused disciplines, which previously only unified in war under an IOG. This prior arrangement ignored that the two disciplines are heavily intertwined, draw on common resources, and, when left uncoordinated in a conflict, can even run the risk of interfering with each other.

The SSF brings two key advantages in this context. First, integrating espionage and offense for strategic information operations allows both missions to benefit from shared reconnaissance, which is essential for identifying vulnerabilities and weaknesses around which their capabilities can be built and offensive effects can be planned. The set of conditions on which these capabilities rely do not remain static and are especially sensitive to changes in an adversary's defense posture, readiness, prevailing attitudes, and the broader shift from peacetime to wartime footing. Military readiness in such an environment means maintaining a constant operations cycle of "perpetual mobilization," wherein countermeasures and effects are constantly evaluated against a changing security landscape and the adversary's efforts.[129] The SSF's integration of espionage and offense recognizes that reconnaissance and capabilities development overlap enough between the two disciplines that both suffer if they are kept separated.

Second, grouping espionage and offense together enables commanders to balance conflicting objectives and inherent tradeoffs that can occur between the two disciplines. Espionage operations prioritize maintaining access to adversary systems and communications for the intelligence gains they may provide, whereas offensive operations may involve sacrificing those access methods in order to undermine the adversary's systems and limit his operations, even if the cost is losing a prime source of information. These tradeoffs become even more pronounced in cyber domain operations, where offense and espionage are inherently blurred; cyber accesses are notoriously "dual-use," meaning they are equally useful for intelligence or disruption. Readiness, in these cases, demands empowering commanders to continually evaluate both options

against each other and against overall campaign objectives and evolving military need, a difficult proposition if espionage and offense authorities are typically separated.

*Unified Operations Planning*

The SSF's dual responsibilities for "force construction" and information operations empower it with both the perspective and authority to define campaign objectives and operational plans for an information warfare campaign and in turn to develop a force necessary to carry those out. Owing to the complexities of coordinating disparate elements, Chinese military scholars have stressed the importance of unified planning and command in order to "form a complete operational force and carry out integrated planning and strategy."[130] The influential 2013 work *Lectures on the Science of Information Operations* lists three primary requirements for unified planning and command in information warfare campaigns, each of which has been addressed to varying degrees by either the large structural changes in the PLA's reforms or the creation of the Strategic Support Force:[131]

- Integrated planning within larger joint and combined operations. The SSF affords information operations a status typically reserved for more traditional domains by providing a cohesive military service capable of representing constituent forces in joint force planning and operations. Its creation conceptually upgrades the status of information operations within the PLA from an auxiliary component of ground forces to a primary front of warfare alongside land, sea, and air. Fulfilling a similar role to that which other services play for their corresponding wartime operations groups, the SSF likely serves as the primary constituent service of the information operations group, shouldering responsibility for carrying out information warfare within the broader PLA framework of integrated joint operations.

- Coordinated planning across services, echelons, and theaters. The SSF's precise role in coordinating information warfare planning across other service elements and theater commands has yet to be publicly defined. Aside from the PLA Rocket Force, the SSF appears to stand alone among the services in not having any of its elements subordinate to the theater commands, either indicating that lower echelon information warfare planning may largely fall to the theater commands themselves or that these subordinate elements exist but have not yet been discovered. It is similarly unclear which organization holds planning responsibilities for China's non-PLA armed forces, including local militias and the People's Armed Police. Some military theorists indicate the SSF plays both coordinating and supporting

roles in this context.[132] Given its preeminence in information warfare strategy, however, the SSF will nevertheless influence lower echelon planning at a minimum.

- Unified planning across information operations disciplines. The SSF fulfills the core requirement of unified planning and command by incorporating all information disciplines into a single cohesive force. Chinese scholars have long emphasized the inclusion of "hard-kill" measures into information warfare planning, epitomized by Ye Zheng's concept of integrated information and firepower warfare [*xin huo yiti zhan*, 信火一体战], which calls for the coordinated pairing of network and electronic warfare with conventional long-range precision strikes.[133] The SSF's concentration of technical reconnaissance capabilities provides a unique vantage point from which to identify critical nodes in an adversary's system of systems, prioritize targeting for kinetic strikes, and weigh the use of "hard" and "soft" measures against each other in campaign planning and operations.

*Unified Information Warfare Command and Control*

The importance of information operations in gaining unseen information and intelligence advantages in peacetime imputes upon the Strategic Support Force a unique responsibility for achieving "escalation dominance," a condition wherein China maintains the initiative in shaping adversary behavior in a crisis scenario that has not yet become a full-on conflict. This requires substantial intelligence capabilities as well as the development of a diverse set of measures for countering, influencing, or deterring an adversary, not only before the crisis occurs but also as part of a continuous process of evaluation to judge both the merits of intentional escalation and the risks of unintended escalation. This capability to engage in "calibrated escalation" reflects a highly complex mission set that requires the ability to coordinate across multiple dimensions of the military bureaucracy in order to produce a set of options that can be clearly communicated up the chain of command, where they will then be evaluated against other political, economic, and military costs. Having a singular service to produce, account for these options, and unify command and control is a marked improvement from the dispersed and siloed arrangement that existed prior to the PLA's reforms.

## Comparing U.S. and Chinese Approaches to Information Warfare

While U.S. and Chinese information support and information operations concepts generally align, a key point of departure is the manner in which these two missions are understood

to fit into broader whole-of-nation plans to accomplish strategic objectives.[134] The PLA, like the U.S. military, views information support and information operations as key for anticipating adversary action, setting the terms of conflict in peacetime, and achieving battlefield dominance in wartime. The PLA places a strong emphasis on dismantling the adversary's system of systems, with decapitation and paralysis rather than outright destruction being the ultimate objective. This approach is tied to the long-standing Chinese focus on *winning without fighting*, an older Maoist-era phrase that translates today to shaping an adversary's decisionmaking through actions below the threshold of outright war, accomplishing strategic objectives without escalating to open conflict. In the Chinese view, if this approach fails, the military needs to be prepared to rapidly seize the initiative in order to compel an adversary to quickly cease hostilities on Chinese terms if the threshold of open conflict is reached. Strategic information support is a key enabler, providing both the avenues and intelligence necessary for well-timed political and operational decisions and action. China's preparations for conflict and planning for these strategic campaigns are directly tied to its national emphasis on preempting and shaping enemy action.

Chinese information operations theory and force structure have historically been somewhat inconsistent on this point, recognizing that information operations defy the binary dichotomy of peacetime and wartime, while operating a force that was not up to that challenge. The Strategic Support Force comes at a time when there appears to be renewed interest in moving away from Western models of conflict, in which peace and war are distinct stages, and toward a spectrum of omnipresent "struggle," a Maoist-Marxist-Leninist paradigm that sees a broad political front in an enduring clash of political systems and ideologies, with military competition and conflict being merely one part of that whole.[135]

The strategic cultures and objectives of both the United States and China have been on opposite ends of the spectrum in many respects for decades, yet both sides have increasingly come to largely the same conclusion on the need to transcend the peace-war binary. The Chinese military has long recognized that abandoning the peace-versus-war binary better reflects the reality of modern operations but have lacked a military force structure that can properly act on that understanding. The United States has maintained a force structure that, since 1986, has merged the concept of peace and war and organized for readiness, but nevertheless maintained the strategic and political distinction between the two. The key differentiator is in how both sides view competition and conflict: as either a rising crescendo that if left unchecked results in a discrete crisis event, as the United States does, or as a long-term struggle between opposing objectives, as China does. Somewhat ironically, in the current round of reforms, the PLA is seeking to advance a traditional Maoist understanding of struggle and competition by adopting

a more Western model of military structure—albeit one with Chinese characteristics. The Strategic Support Force's primary roles of information support and information warfare, on which military preparation and readiness in large part rests, are key advancements in China's ability to translate both of these paradigms into operational reality.

Although a truly authoritative insider's view of Chinese information warfare has not been made public, the 2013 *Lectures on the Science of Information Operations* by PLA scholar Major General Ye Zheng gives a comprehensive examination of the unique properties, advantages, and limitations of information operations and their use in warfare. Ye identifies four fundamental principles of Chinese thinking on information warfare that inform the SSF's approach to information operations:

- Information operations are offense-oriented. Chinese scholars believe information dominance is the core of the "three dominances" of information, air, and space that, when achieved, ensure victory. As modern warfare requires the practice of system-of-systems operations, disrupting an adversary's system of systems while preserving one's own can deprive them of strategic initiative and allow Chinese forces to rapidly achieve battlefield dominance.

- Information operations are offense-dominant. Cyber and intelligence operations in particular are fragile, sensitive to changing circumstances, and rely on techniques and access methods that lose much of their power once they have been put to use and the element of surprise is lost. Cyber accesses that enable these effects are frequently more effective in the initial stages of a conflict.

- "Prepositioning" and "massing on the border" manifest differently in information warfare. Whereas other domains prioritize geographic prepositioning, readiness and advantage in the information domain place a priority on timing, blurring the distinction between peacetime and wartime. This in turn partially blurs the distinction between intelligence operations and military preparations.

- Information advantage can be traded for space and time on the battlefield. A key belief in the Chinese understanding of information operations is that prepositioned effects and capabilities, achieved through either cyber implants in an adversary's systems or an intelligence advantage enabled by strategic information support, can be utilized at strategic

> times to anticipate, delay, and disable an adversary's ability to defend himself or project power. This means that an information domain advantage can effectively be traded for physical space and time in conflict in order to enable the achievement of China's strategic objectives.

PLA theorists believe that these characteristics of information warfare are not unique to any one nation's armed forces but instead are universal operational precepts that need to be recognized and adhered to regardless of a nation's strategic culture. It is therefore unsurprising that China's understanding of information warfare looks remarkably similar to that envisioned by the United States.

Where the Chinese view differs is in the strategic context and scenarios where they see these options being employed, stemming from a recognition of their vulnerabilities, limitations, and strategic objectives vis-à-vis those of their potential adversaries. Bureaucratic factors also play an important role. The organizational implementation of China's cyber force, for example, reflects both the similarities and differences between the Chinese and U.S. approaches. One of the key differences between USCYBERCOM and the SSF's cyber force lies in their respective scopes of responsibilities. The SSF appears to be responsible for *all* of information warfare, overseeing the employment of a broad spectrum of tools for kinetic, cyberspace, electromagnetic, and psychological domains.

The SSF reflects another point of divergence between China and the United States in the degree of organizational emphasis it places on the space domain as a core arena of information warfare. The United States certainly recognizes the intersection between the information domain and outer space; however, in both strategic writings and official publications, the PLA has continuously emphasized the link between space and cyber networks, viewing them not in isolation but as extensions of one another through their common use of the electromagnetic spectrum as a transmission medium. This may be due to the PLA's understanding that the most extreme threat scenarios it faces, such as a full-scale invasion by a foreign power, an adversary's long-range precision strike and force projection would both largely be enabled by space-based infrastructure, which would serve as both an extension of terrestrial cyber networks and a means of contesting dominance in the electromagnetic domain.

At the strategic level of war, China's plans for the defense of these three domains converge to the degree that combining them not only creates natural efficiencies but also verges on being a requirement for an effective force. The comparative lack of emphasis on operational cohesion among cyber, space, and electronic warfare in the United States can be understood as a mani-

festation of differing strategic priorities and threat perceptions. In the wars the United States has fought since the end of the Cold War—against armed insurgencies, terrorist groups, and relatively low-tech powers—cyber, space, and electronic warfare could be treated as separate, complementary disciplines without a demand for convergence at the strategic level as would be required when facing a technologically developed near-peer military power with a mature C4ISR system. It is possible that the U.S. 2017 National Security Strategy, which shifts focus away from combating terrorism to confronting "strategic competitors," will presage a realignment within the Department of Defense toward an organizational concept that more closely resembles the Strategic Support Force.[136]

Another key point of divergence between the SSF Cyber Force and USCYBERCOM is in the inclusion of psychological operations within the former's remit. Chinese Communist Party and PLA thinkers have long understood cyber operations to be a primary vehicle for psychological manipulation, a point not fully grasped by the U.S. Government, particularly the defense establishment, until the recent discovery and analysis of Russian interference in the U.S. Presidential election in 2016. The United States tends to view cyber warfare in terms of destruction and denial, with a particular focus on the potential for cyber attacks with kinetic effects and the destruction and manipulation of data in a conflict. Chinese leaders, on the other hand, view manipulation of information more broadly as their chief vulnerability and worry about the societal effects of an adversary undermining Chinese domestic information control. This view manifests in China's civilian cybersecurity establishment, which has taken on an expansive scope that extends beyond computer networks to physical devices, broadcast airwaves, online content, and propaganda. This understanding that failure to control information threatens the Chinese Communist Party's political power and stability in a way that it does not in democratic countries is a view shared by China's civilian and military establishments. Maintaining information control is thus viewed as a preemptive defense that obviates the need for more forceful measures, such as armed domestic actions, to be employed. For the SSF, the inclusion of content and a more information-centric approach to cyber operations is translated into the expansive remit of the cyber force, which appropriately includes psychological operations in alignment with the expansive Chinese view of cybersecurity.

## Remaining Challenges

Simply reorganizing command structures and relationships is but one step in a lengthy and likely painful process the Strategic Support Force must undertake in fully integrating its myriad components into a cohesive operational force. Removing silos and integrating forces

will eliminate potential barriers, but without deeper changes within the space and cyber forces, the SSF will be limited in its ability to fully play its information support and information warfare roles. Similarly, in some cases there are deeper organizational tensions at play that may limit or impede overall PLA progress in the long term, such as centralizing strategic capabilities vice diffusing them and balancing the cyber mission between civilian and military components. How the PLA handles these challenges is vital in realizing its goal to be a modern military able to fight and win informationized wars.

### Centralization vs. Diffusion of Control and Development of Strategic Capabilities

The SSF's dual responsibilities for both "force construction" and operations are in direct tension with one of the key purposes of the reforms, namely, to transition operational responsibilities away from the services to joint force theater commands. This fundamentally defies the "CMC leads, theaters fight, and services build" paradigm implemented across the force. Although the Strategic Support Force appears to take the U.S. Strategic Command as its conceptual inspiration, the SSF diverges markedly in implementation. USSTRATCOM supports U.S. combatant commands as a joint force construct rather than as a singular service in the model of the Strategic Support Force. As a joint functional combatant command, USSTRATCOM coordinates among a number of subordinate elements from the Army, Marine Corps, Navy, and Air Force to prosecute its primary missions of nuclear operations, space operations, information warfare, strategic C4ISR support, and ballistic missile defense.

While the PLA created joint, regional theater commands analogous to U.S. geographic combatant commands, the PLA stopped short of creating functional combatant commands. Instead, the SSF was created as a service-like force that serves a PLA-wide functional role. A similar approach was taken with the PLA Rocket Force, whose functional role of employing China's nuclear and strategic missiles has been similarly distilled into a single service in a manner that appears incongruent with the overall intent of the reforms.

The most obvious explanation for these inconsistencies may be that the current arrangement is transitional, and the PLA intends to eventually create joint functional combatant commands—or some analog—in the future. However, there may be deeper organizational dynamics at play. In both circumstances, responsibilities for nuclear, space, and information warfare may have been deemed sufficiently strategic that the CMC elected to keep both operational and force construction functions contained within a single service, where their use and development could be more easily controlled. The lack of equivalent, mature development of these capabilities in the other services, coupled with a still-nascent joint force construct, may have

convinced PLA planners that operational control and development of these capabilities were, for now, best kept contained. Chinese defense commentators have explained that the decision to construct the SSF as a separate force rather than a joint force construct was driven by lessons learned from observing foreign militaries where the distribution of strategic support across the different services resulted in redundancies in force development and a counterproductive rivalry for funding and resources.[137]

If taken at face value, this approach highlights some of the broader challenges the PLA faces in modernization and reform. The centralization of new-type force development and cutting-edge missions, such as space, cyber, and electronic warfare, seems to run counter to the objective of modernizing the PLA force-wide. The consolidation of these capabilities under the SSF, either for resource conservancy, desire to control strategic capabilities, or desire to more closely guide their development, may act as a limiting factor for other services, preventing the development of space, cyber, and information capabilities in their own missions. This raises further questions about the future of both the space and cyber missions, which in the former case may be shared with the PLA Rocket Force and PLA Air Force and in the latter case shared with the theater commands and other services. Given the above logic, it seems likely that the desire to centralize and reduce redundancy, for whatever reason, may translate to a monopoly of force, command, and development over these missions on the part of the SSF. The creation of functional services like the SSF and PLA Rocket Force appears to be a bureaucratic compromise, allowing theater commands access to these capabilities without ceding operational control, diffusing force development across other services, or risking the adoption of an unfamiliar joint force construct like USSTRATCOM by a PLA already acclimating to a new organizational model.

### Mission and Force Integration

Force integration at lower organizational and administrative layers also remains a distinct challenge for both of the SSF's two main forces. The Space Systems Department is a motley mixture of higher grade bases, launch and ground stations, and experimental technology development facilities contained within a force structure that has traditionally not been optimized for combat operations. To align and coordinate its disparate component parts, the SSD will almost certainly need to stand up new administrative structures. Since the SSD's space mission brings together a disparate set of mission components from the GSD and GAD, systems integration poses an additional challenge. Each of these organizations comes to the SSD with its own operations plans, technical data sources, and infrastructure, with missions as diverse

as communications, navigation, surveillance and reconnaissance, and telemetry, tracking, and control. For the SSD to fulfill the SSF's (and the PLA's) broader mandate of system-of-systems integration [*tixi ronghe*, 体系融合], it will need not only to integrate these systems together but also to seamlessly feed this information into force-wide networks such as the Integrated Command Platform [*yitihua zhihui pingtai*, 一体化指挥平台] to support both strategic missions and theater command operations.[138]

The Network System Department faces several challenges of its own. First and foremost, it will need to reform the former 3PLA's administrative structure to accommodate an expanded mission set and a newfound focus on cyber domain operations, which had previously been dispersed across multiple bureaus and treated as a subdiscipline of technical reconnaissance.[139] Further reorganization is likely to center on consolidating myriad cyber espionage elements and integrating them with cyber and EW elements from the former 4PLA. However, these missions were deeply embedded in the force structure of their respective departments and separating these elements out to reconstitute them along either functional or organizational lines will likely require deeper reorganization.

Beyond organizational mergers, the Network Systems Department will also need to reform its personnel system. The organizational integration of all the PLA's strategic cyber and EW capabilities fulfills the long-held goal of integrated network and electronic warfare in a more comprehensive way than the previous structure, but the NSD still faces steep hurdles in integrating the two disciplines on a human level. In the past, 3PLA and 4PLA appear to have largely maintained separate personnel systems, including distinct officer corps, noncommissioned officer corps, and technical cadre career paths, all of which will need to be merged if the NSD is going to fully embrace and realize INEW. The Network Systems Department's management of professional military education and billeting will be a critical factor in any such reform. The consolidation of the Information Engineering University as the sole military academy for the cyber and electronic warfare arms of China's network-electronic forces is an important step forward that may help unify professional military education to meet the disparate needs of both forces. At this time, however, assessments of how the NSD will manage its personnel are complicated by the existence of the Network-Electronic Bureau, whose responsibilities for force-wide management of education and training in this sphere are still unclear.

It also remains an open question how the Strategic Support Force will manage conflicting or overlapping responsibilities between its space and cyber forces. For instance, a number of organizations now under the Network Systems Department once had space mission components; these presumably moved over with them to the SSF. The technical reconnaissance–focused

former GSD 3rd Department's 12th Bureau [*zongcan san bu di shi'er ju*, 总参三部第十二局] or Unit 61486 [*61486 budui*, 61486 部队] has historically been responsible for space-based signals intelligence collection and the interception of satellite communications, and may also control a number of ground-based space sensing stations.[140] The transfer of units from the former 4PLA, which maintained at least two satellite ground stations and whose operational brigades possess ground-based satellite jammers, presents a similar situation.[141] If transferred to the NSD, a conflict in responsibilities with the Space Systems Department's space mission components might arise and require ironing out, either via further below-the-neck reorganization or through redesign of these units' operational responsibilities.

## Challenges in Cyber Operations

While the reforms that created the SSF can be favorably compared to the reforms that occurred in U.S. military structure between 2009 and 2014 with the creation of USCYBERCOM, there are key differences between each side's baselines for reform. For the United States, a key challenge has been keeping USCYBERCOM separate enough from the National Security Agency to allow for independent action and planning without losing the necessary resources, expertise, and reconnaissance required to inform military targeting and carry out operations. The Chinese face the opposite challenge of integration. Of China's myriad agencies with cyber portfolios, the Ministry of State Security (MSS) and PLA are the two primarily responsible for cyber operations, including both espionage and offensive action. The Mandiant report in 2014, the Xi-Obama agreement on cyber-enabled intellectual property theft in 2015, and the creation of the Strategic Support Force each in various ways forced a realignment of responsibilities between the two agencies, with the MSS focusing on foreign intelligence, political dissent, and economic espionage, and the PLA redoubling its focus on military intelligence and warfighting.

This broad division of responsibilities serves a key purpose, deconflicting their missions and targeting efforts without requiring in-depth coordination. Both the PLA and MSS have previously resisted greater integration in their intelligence efforts, with the PLA in particular heavily rebuffing oversight and coordination with civilian authorities.[142] As their political and bureaucratic power is largely secured by controlling exclusive intelligence sources, any sharing of information could mean a diffusion of power at the expense of their influence. In China's 2017 National Intelligence Law, the provisions discussing national governance of intelligence activities exempt the military, writing that the Central Military Commission, not civilian authorities, are exclusively in control of military technical reconnaissance efforts (and thus cyber operations).[143] Despite this arrangement offering greater clarity in a bureaucratic space with

clashing interests, the arrangement ultimately deprives both civilian and military missions of the resources, insight, and technical skill available from each other's reconnaissance and capabilities development efforts.

The PLA's cyber operational challenges go beyond the civilian-military divide. Even under the new structure, the PLA faces crucial challenges in its ability to credibly field a modern cyber force. For one, it remains unclear how the PLA will integrate the SSF's cyber operations, which appear to be overwhelmingly focused on espionage and offense, with the PLA's cyber defense mission. Currently, primary responsibility for PLA network protection remains with the Information Support Base under the Joint Staff Department's Information and Communications Bureau. Placing cyber defense within JSD-ICB rather than the SSF runs counter to the U.S. model, where the mission is under USCYBERCOM's Joint Force Headquarters DOD Infomation Network (JFHQ-DODIN). A potential merger of JFHQ-DODIN and the Defense Information Systems Agency would veer further from that model, as it would bring a wider range of network operations under USCYBERCOM's remit, including those that would be under the JSD-ICB Information Support Base in the PLA model. It is unclear how the SSF will work with the JSD-ICB to help secure PLA networks from cyber threat, or how its broader space information support mission will integrate with the JSD-ICB's role as a service provider to the PLA writ large.

Even less clear is what responsibility, if any, the SSF will have for cyber defense of private, civilian, and critical infrastructure networks. In an early description of the SSF, retired navy Admiral Yin Zhuo broadly suggested that the SSF plays an "important role" in "protecting the country's financial security and the security of people's daily lives."[144] It is not clear where the SSF would have sourced the personnel or capabilities to serve in this role, as it was not a known mission area of either the 3PLA or 4PLA, the two cyber-focused organizations from which the SSF drew the bulk of its cyber forces. Given the lack of preexisting units responsible for a "national cyber protection" mission, Yin's comments, if meant literally, suggest that the SSF would need to create this capability from scratch. As of this writing, there has been no indication that such units have been created, and it is not clear who among the PLA's forces would have national, regional, or local responsibility for such a mission.

It is also not clear how any SSF cyber defense and protection mission would conflict or be coordinated with the Ministry of Public Security [*gongan bu*, 公安部] and Cyberspace Administration of China [*guojia hulianwang xinxi bangongshi*, 国家互联网信息办公室], both of which are charged with maintaining the security and defense of China's critical information infrastructure.[145] Overlapping responsibilities for defense and security of critical infrastructure is a common issue in national cybersecurity governance, one equally felt by the United States.

The Chinese government would likely face challenges in clarifying roles and responsibilities and establishing necessary legal, procedural, and technical means of operational coordination and incident response in order for critical infrastructure security and protection to be meaningful. This would in turn require a level of maturity and foresight in the notoriously fraught relationship between civilian and military authorities that is not likely to be achieved in the short term.

Finally, although the structural and organizational barriers between cyber attack and espionage appear to have been decreased, PLA units responsible for operations planning have little experience in anticipating and balancing equities between the two missions. Nor does it appear that the PLA has developed a doctrine for the use of force in cyberspace under which consistent judgments can be made in a crisis. Freed from its previous organizational structure, the PLA now faces the very real challenge of defining its own ways of war in cyberspace. These peacetime decisions will shape the development of the SSF's cyber force, network warfare capabilities, espionage priorities, and operational preparation of the battlespace. Unlike in other areas of warfare, when it comes to wartime cyber operations the PLA has precious few real-world examples upon which it can draw to inform its own doctrinal development. The PLA, like many other militaries, will have to answer critical questions about peacetime and wartime targeting, escalation in situations where the divide between peacetime and wartime is not always clear, battlespace prepositioning, and the viability and wisdom of utilizing cyber operations to achieve specific strategic military objectives. Although the PLA has developed its own theories on the strategic use of cyber operations in a conflict, these ideas have not yet been tested against the hard reality of operational and organizational implementation. The restructuring of the SSF (and the PLA more broadly) will put those ideas to the test, pushing Chinese cyber operations into unfamiliar territory.

## Conclusion

The creation of the Strategic Support Force heralds a new era for China's strategic posture. Its very existence is both predicated on and a reinforcement of China's growing military strength, strengthening China's preparations for "local informatized war" and shifting the PLA's horizons to projecting power farther from China's shores. The SSF demonstrates the evolution of Chinese military thought about information as a strategic resource in warfare, recognizing both the role it plays in empowering forces and the vulnerabilities that result from reliance on information systems. The inclusion of responsibilities for both information support and information dominance in the same organization is a wise decision. As China continues to develop technologically and operate beyond the first and second island chains, the asymmetric advantages it has relied

upon as a land-based, technologically inferior power will narrow, and it will increasingly have to contend with adversaries on more equal terms. From this standpoint, the introduction of an organization designed to balance those equities is forward-thinking.

Success in the various roles that Chinese scholars—and Xi Jinping himself—have envisioned for the SSF will largely depend on the efficacy of the unique and unproven model of "strategic support" that the Chinese have chosen to pursue. In one sense, centralizing these components into a service rather than dispersing them in a joint manner can be seen as innovative. On the other hand, the model can be viewed as an attempt by the PLA to grapple with its deeper and more systemic issues rather than a simple desire to try something new. Since an emphasis on top-down control and distrust of bottom-up decisionmaking has been an enduring hallmark of the PRC's strategic culture, this new centralization of information power may be more a function of persistent paranoia and the need for control than a desire to explore innovative means of warfighting. China certainly has the technical and operational capability to use its strategic resources in a punctuated manner for critical operations, but its ability to do so at scale in a sustained way will require deeper cultural and organizational innovation.

## Notes

[1] Sources on specific units are available to qualified researchers upon request.

[2] Ye Zheng [叶证], *Lectures on the Science of Information Operations* [信息作战科学教程] (Beijing: Military Science Press [军事科学出版社], 2013), 69.

[3] See M. Taylor Fravel, "Shifts in Warfare and Party Unity: Explaining China's Changes in Military Strategy," *International Security* 42, no. 3 (Winter 2017/2018), 37–83.

[4] Joe McReynolds and James C. Mulvenon, "The Role of Informatization in the People's Liberation Army under Hu Jintao," in *Assessing the People's Liberation Army in the Hu Jintao Era*, ed. Roy Kamphausen, David Lai, and Travis Tanner (Carlisle Barracks, PA: Strategic Studies Institute, April 2014), 207–256.

[5] Clay Wilson, *Network Centric Operations: Background and Oversight Issues for Congress*, RL32411 (Washington, DC: Congressional Research Service, March 15, 2007), available at <https://fas.org/sgp/crs/natsec/RL32411.pdf>.

[6] Both the 2013 Academy of Military Science (AMS) edition of *Science of Military Strategy* and Ye Zheng's *Lectures on the Science of Information Operations* (hereafter LSIO) remark on transfer over space-based intelligence, surveillance, and reconnaissance (ISR) networks in support of operations in the 1991 Gulf War, 1999 strikes on Kosovo, and 2003 invasion of Iraq. Analysts observe that the U.S. military's appetite for information appears to have grown in lockstep with its relative technological sophistication. See Shou Xiaosong [寿晓松], ed., *Science of Military Strategy* [战略学] (Beijing: Military Science Press [军事科学出版社], December 2013), 95–96; and Ye, LSIO, 50–51, 69–72.

[7] James C. Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in *Beyond the Strait: PLA Missions other Than Taiwan*, ed. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle Barracks, PA: Strategic Studies Institute, 2009), 275.

[8] Andrew S. Erickson, "Chinese Air- and Space-Based ISR: Integrating Aerospace Combat Capabilities over the Near Seas," in *China's Near Seas Combat Capabilities*, ed. Peter Dutton, Andrew S. Erickson, and Ryan Martinson (Newport, RI: U.S. Naval War College Press, 2014), 88–89.

[9] *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: Office of the Secretary of Defense, 2011), 37.

[10] Leonard David, "China's Anti-Satellite Test: Worrisome Debris Cloud Circles Earth," *Space.com*, February 2, 2007, available at <www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html>.

[11] Dennis J. Blasko, "The 'Two Incompatibles' and PLA Self-Assessments of Military Capability," *China Brief* 13, no. 10 (May 2013), available at <https://jamestown.org/program/the-two-incompatibles-and-pla-self-assessments-of-military-capability/>.

[12] Shou, *Science of Military Strategy*, 169.

[13] Christopher H. Sharman, *China Moves Out: Stepping Stones Toward a New Maritime Strategy*, China Strategic Perspectives 9 (Washington, DC: NDU Press, April 2015), 5.

[14] For an expansive discussion of this concept, see Zhou Bisong [周碧松], *Strategic Frontiers* [战略边疆] (Beijing: National Defense University Press [国防大学出版社], 2016); and Shou, *Science of Military Strategy*, 73.

[15] Shou, *Science of Military Strategy*, 73.

[16] "China's Military Strategy" [中国的军事战略], Xinhua [新华], May 26, 2015, available at <www.mod.gov.cn/auth/2015-05/26/content_4586723.htm>.

[17] Zhou Bisong [周碧松], "Strategic Frontiers" [战略边疆]; excerpts available online at <http://zlzy.81.cn/tb/2016-08/15/content_7231775.htm>.

[18] Kevin Pollpeter et al., *China Dream, Space Dream: China's Progress in Space Technologies and Implications for the United States* (Washington, DC: U.S.-China Economic and Security Review Commission, 2017), 94–95.

[19] *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017* (Washington, DC: Office of the Secretary of Defense, 2017), 35.

[20] Ye, LSIO, 81.

[21] This information is derived from Costello's conversations with a credible People's Liberation Army (PLA) source who has direct knowledge of organizational logic behind the military reforms launched in 2015.

[22] For a more in-depth discussion of PLA military reforms of the four general departments, see Joel Wuthnow and Phillip C. Saunders, *Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications*, China Strategic Perspectives 10 (Washington, DC: NDU Press, March 2017), 10–11.

[23] It should be noted that the PLA does not classify its forces as "cyber" forces, but rather as "network" forces, owing to a conception of the "network domain" that overlaps but does not perfectly align with the U.S. military's concept of "cyberspace." When the term *cyber* is used in this chapter in descriptions of PLA concepts and developments, it should be taken as referencing PLA network warfare units that would fall under the U.S. definition.

[24] John Costello, "The Strategic Support Force: Update and Overview," *China Brief* 16, no. 19 (December 21, 2016), available at <https://jamestown.org/program/strategic-support-force-update-overview/>.

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

[26] Ibid.

[27] John Costello and Peter Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations," in *China's Evolving Military Strategy*, ed. Joe McReynolds (Washington, DC: Jamestown Foundation, 2016), 180–182.

[28] Public descriptions of the Strategic Support Force (SSF) vary considerably as to whether the SSF is a branch [兵种], meaning a subcomponent of another service, or a military service [军种] in its own right. Until clearer information is available on this point, it is best described as a "force" in English. Even if it were in some technical sense a branch, its command structure appears to connect directly to the Central Military Commission (CMC) without any intermediary from another military service. For a more involved discussion on the status of the SSF, see Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND, 2017), 21–22.

[29] Yue Huairang [岳怀让], "The Strategic Support Force: Gao Jin as Commander, Liu Fulian

as Political Commissar, Breastplate Revealed" [战略支援部队：高津任司令员，刘福连任政治委员，胸牌曝光], *The Paper* [澎湃], January 1, 2016, available at <www.thepaper.cn/newsDetail_forward_1415847>; Liu Guangbo [刘光博], "These Five 'Theater Command Leader-Grade' General Officers Were Just Promoted to the Rank of General" [这五位正战区级将领刚刚晋升上将], *Chang'an Street Knowledgeable* [长安街知事], July 28, 2017, available at <http://news.sina.com.cn/c/nd/2017-07-28/doc-ifyinwmp0572361.shtml>.

[30] Li Xuanliang, Zhang Xuanjie, and Li Qinghua [李宣良，张选杰，李清华], "Ceremony Establishing Army Leading Organ, Strategic Rocket Forces, and Strategic Support Force Held in Beijing" [陆军领导机构火箭军战略支援部队成立大会在京举行], Xinhua [新华], January 1, 2016, available at <http://news.xinhuanet.com/politics/2016-01/01/c_1117646667.htm>.

[31] "Former Eastern Theater Command Political Commissar Major General Zheng Weiping Transfers to the Strategic Support Force" [东部战区原政委郑卫平上将转岗战支部队], *United Morning Post* [联合早报], October 23, 2017, available at <www.unizw.com/mon/dapan/20171023/40725.html>.

[32] Although AMS conducts research and offers graduate degrees, its role in PLA doctrine formulation makes it more similar to parts of the U.S. Joint Staff Joint Force Development Directorate or the U.S. Army's Training and Doctrine Command than to a military academic institution.

[33] For a more involved discussion on the status of the SSF, see Pollpeter, Chase, and Heginbotham, *The Creation of the PLA Strategic Support Force*, 21–22.

[34] See "2018 Seventh Exhibition on New Technologies and Equipment for Military Logistics" [2018第七届军事后勤保障新技术与新装备展览会], *Meeting Spot* [会点], June 21–23, 2018, available at <www.hui.net/news/special/key/1sim4hc9rsgMu>. A senior colonel, Xiao Zhiyu [肖志宇], from the SSF Equipment Department, was referenced as a speaker and attendee to the 2017 China Civil and Military Dual-Use Technology Conference [2017中国军民两用技术研讨会] held in conjunction with an opening ceremony for the newly established Changzhou Military-Civilian Fusion Industrial Park [常州军民融合产业园] on May 21, 2017. See Wang Jinghui [王晶辉], "To Help With Civil-Military Integration, Casting the Country's Treasure: Changzhou Civil-Military Integration Industrial Park Officially Opened, Entering Enterprises Enjoy Comprehensive, One-Stop Service!" [助军民融合，铸国之重器：常州军民融合产业园正式开园，入园企业享受全方位，一站式服务！], May 24, 2017, available at <http://edp.hit.edu.cn/ba/07/c7876a178695/page.htm>; Lin Yunshi [林韵诗], "Major General Feng Jianhua Promoted to Director of Strategic Support Force Political Work Department" [冯建华少将升任战略支援部队政治工作部主任], *Caixin* [财新], February 29, 2016, available at <http://china.caixin.com/2016-02-29/100913753.html>; Feng Jianhua [冯建华] is listed as a deputy theater command leader grade and was subsequently promoted to lieutenant general in October 2017. See "Breaking News—Strategic Support Force Political Work Department Director Feng Jianhua Has Been Promoted to the Rank of Lieutenant General" [战略支援部队政治工作部主任冯建华已晋升中将军衔 澎湃新闻], *Military Report* [军事报道], August 30, 2017, available at <https://xw.qq.com/cmsid/20171030A0IZEL00>. The SSF Political Work Department deputy directors have been listed as Major General Chen Jinrong [陈金荣] and Huang Qiusheng [黄秋生]. See Yue Huairang [岳怀让], *The Paper* [澎湃], February 3, 2016, available at <www.thepaper.cn/newsDetail_forward_1429068>; and Yue Huairang [岳怀让], *The Paper* [澎湃], August 1, 2017, available at <www.thepaper.cn/newsDetail_forward_1749068>.

[35] "Strategic Support Force Space Systems Department Test Equipment Materials Purchasing Bureau Medical Equipment Advertisement for Public Open Bid and Tender" [战略支援部队航天系统部试验装备物资采购局医疗设备公开招标采购公告], China Government Procurement Bidding Network [中国政府采购招标网], August 25, 2016, available at <www.chinabidding.org.cn/PurchaseInfoDetails_pid_1558826.html>; "Our Board Convened the Eleventh Meeting of our Fifth Board of Directors and the 2017 Military-Industrial Enterprise Salon" [我会召开第五届第十一次理事会议暨2017军工企业沙龙], Shenzhen Promotion Association for Small and Medium Enterprises [深圳市中小企业发展促进会], August 31, 2017, available at <www.szsme.com/cn/dtdetail/81/755.html>.

[36] Liu Wei [刘伟], ed., *Theater Command Joint Operations Command* [战区联合作战指挥] (Beijing: National Defense University Press [国防大学出版社], 2016), 340.

[37] The block falls between the one used by units assigned to the CMC (31001 to 31999) and the one used by the PLA ground forces, which starts at 32100.

[38] For the pre-reform bases, see Kevin Pollpeter and Kenneth W. Allen, eds., *PLA as Organization 2.0* (Vienna, VA: Defense Group, Inc., 2015), 145–148.

[39] The unit appears to operate under the Military Unit Cover Designator (MUCD) 32020 and is located in Wuhan. See "Historic, Proud, Responsible: *Zhongdian Jinjiang* Joins Hands with 35th Base to Create a New Era Magnificient Atmosphere" [有历史、有自豪、有担当——中电锦江拟携手35基地开创新时代宏伟 "气象"], *Zhongdian Jinjiang* [中电锦江], January 15, 2018, available at <www.jec784.com/news_detail/newsId=134.html>.

[40] Xu Nanqi [徐南启], "The Second 'Jointly Build a Strong Military Dream' Themed Party and the National Defense 2018 New Year's Party Have Ended" [我校第二届"同心共筑强军梦"主题晚会暨国防生2018年元旦晚会落幕], Nanjing University [南京大学], December 25, 2017, available at <http://news.nju.edu.cn/show_article_1_48249>.

[41] See Leigh Ann Luce and Erin Richter, "Handling Logistics in a Reformed PLA: The Long March Toward Joint Logistics," in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, ed. Phillip C. Saunders and Joel Wuthnow (Washington, DC: NDU Press, forthcoming).

[42] Kenneth Allen, "Assessing the PLA's Promotion Ladder to CMC Member Based on Grades vs. Ranks—Part 1," *China Brief* 10, no. 15 (July 22, 2010), available at <https://jamestown.org/program/assessing-the-plas-promotion-ladder-to-cmc-member-based-on-grades-vs-ranks-part-1/>.

[43] Ibid.

[44] "Most Recent News on the Military Reforms: The Central Military Commission Comprehensively Implement the Three Tiered Structure of 'Departments-Bureaus-Offices'" [军改最新消息：军委机关总体实行"部—局—处"三级体制], *Guancha* [观察], October 5, 2016, available at <www.guancha.cn/military-affairs/2016_10_05_376239.shtml>.

[45] "The Most Mysterious and Newest Force—The Strategic Support Force" [最神秘的年轻部队—战略支援部队], China Military Network [中国军网], September 20, 2016, available at <www.81.cn/jwsj/2016-09/20/content_7268473.htm>.

[46] For Kang Chunyuan, see Wang Jun [王俊], "Officer in a Deputy Military Region Grade Position Kang Chunyuan Has Been Promoted to the Rank of Lieutenant General, Formerly Served as Deputy Political Commissar of the Lanzhou Military Region" [副大军区职军官康春元已晋升中将军衔，曾任原兰州军区副政委], *The Paper* [澎湃], August 29, 2016, available at <www.thepaper.

cn/newsDetail_forward_1521187>. For Hao Weizhong, see Lin Yunshi [林韵诗], "The Space Systems Department of the Strategic Support Force Appears, Shang Hong as Commander" [战略支援部队航天系统部亮相 尚宏任司令员], *Caixin* [财新], April 25, 2017, available at <http://china.caixin.com/2017-04-25/101082917.html>. For Fei Jiabing, see "Leaders of the Space Systems Department Come to Our Academy to Research and Direct Work" [航天系统部领导来我院调研指导工作], China Academy of Space Technlogy [中国空间技术学院], March 31, 2017, available at <www.cast.cn/item/show.asp?m=1&d=5700>.

[47] Lin, "The Space Systems Department of the Strategic Support Force Appears."

[48] For an excellent analysis of the status of these missions prior to the reforms, see Mark A. Stokes and Dean Cheng, *China's Evolving Space Capabilities: Implications for U.S. Interests* (Washington, DC: U.S.-China Economic and Security Review Commission, April 26, 2012), 4–5.

[49] Pollpeter, Chase, and Heginbotham, *The Creation of the PLA Strategic Support Force*, 28.

[50] Zhang Zhanyue and Zhu Shuguang [长占月， 祝曙光], "Trends of Space-Based Information Support Development" [天基信息支援发展趋势], *Satellite Applications* [卫星应用], vol. 9 (September 2016), 67–71.

[51] In April 2016, it was confirmed that former Aerospace Reconnaissance Bureau Chief Zhou Zhixin [周志鑫] transferred to the SSF to head up a "certain bureau" [某局]. This is good indicator that the bureau has moved to the SSF and, given its mission, has been reassigned to the Space Systems Department. See Yue Huairang [岳怀让], "Chinese Academy of Sciences Academician Zhou Zhixin to Become the Bureau Chief of a Certain Bureau in the Strategic Support Force" [中科院院士周志鑫出任战略支援部队某局局长], *The Paper* [澎湃], April 9, 2016, available at <www.thepaper.cn/newsDetail_forward_1454253>. Zhou Zhixin is now the Commandant of the Space System Department's newly created Space Engineering University. See "Zhou Zhixin Becomes the Commandant of the Strategic Support Force's Space Engineering University" [周志鑫任战略支援部队航天工程大学校长], *Sohu* [搜狐], October 8, 2017, available at <www.sohu.com/a/196776059_495232>. For more on the Aerospace Reconnaissance Bureau's mission, see Kevin Pollpeter and Amy Chang, "The General Armament Department," in *PLA as Organization 2.0*, 145–148.

[52] Costello, "The Strategic Support Force."

[53] "Einstein Probe Successfully Passes Project Comprehensive Demonstration Review" [爱因斯坦探针卫星工程顺利通过立项综合论证评审], Chinese Academy of Sciences National Astronomical Observatories [中科院国家天文台], July 5, 2017, available at <www.bao.ac.cn/xwzx/zhxw/201707/t20170721_4835406.html>.

[54] Bill Gertz, "China Carries Out Flight Test of Anti-Satellite Missile," *Washington Free Beacon*, August 2, 2017, available at <http://freebeacon.com/national-security/china-carries-flight-test-anti-satellite-missile/>.

[55] The SY-7 satellite has a robotic arm that is claimed to be used to grapple onto target satellites for inspection and maintenance. Experts contend, however, that the satellite's arm could be used for co-orbital attack intended to destroy or disable an adversary satellite. For a discussion of the satellite's capabilities, see Robert Beckhusen, "China's Mystery Satellite Could Be a Dangerous New Weapon," *War Is Boring*, August 22, 2013, available at <https://warisboring.com/china-s-mystery-satellite-could-be-a-dangerous-new-weapon/>.

[56] Pollpeter, *China Dream, Space Dream*, 95.

[57] Stokes and Cheng, *China's Evolving Space Capabilities*, 45.

[58] Ibid. Up until the late 1990s, for instance, the PLA Air Force (PLAAF) was even limited in its ability to fly over water due to the maritime domain being considered the responsibility of the PLA Navy Air Force. In fact, it was not until the 1996 Taiwan Strait Crisis that a PLAAF plane was ordered to fly over water for the first time.

[59] Kenneth Allen and Jana Allen, "Assessing China's Response to U.S. Reconnaissance Flights," *China Brief* 11, no. 16 (September 2, 2011), available at <https://jamestown.org/program/assessing-chinas-response-to-u-s-reconnaissance-flights/>.

[60] "The Strategic Support Force Has Renamed the Former General Staff Department's Third Department as the Cyberspace Operations Force" [战略支援部队成军 原总参三部更名网络空间作战部队], *Boxun.com*, January 19, 2016, available at <www.boxun.com/news/gb/china/2016/01/201601192251.shtml>.

[61] Pollpeter, Chase, and Heginbotham, *The Creation of the PLA Strategic Support Force*, 19.

[62] "General Staff Personnel Changes; Wang Huiqing Becomes Director of the Strategic Planning Department; Zheng Junjie Becomes Director of the Third Department" [总参人事变动王辉青任战略规划部部长郑俊杰任三部部长], *Jiangwutang* [讲武堂], November 1, 2015, available at <https://web.archive.org/web/20161018223115/http://j.news.163.com/docs/99/2015110114/B7BFICQ405158ED3.html>.

[63] Wang Jun [王俊], "Chengdu Military Region Political Department Director Chai Shaoliang Becomes Military Region Deputy Political Commissar" [成都军区政治部主任柴绍良改任军区副政委], *Ta Kung Online* [大公网], December 31, 2013, available at <http://news.takungpao.com/mainland/zgzq/2013-12/2143144.html>.

[64] See Guo Rui and He Xiaoyuan [郭瑞， 贺筱媛], "Pretreatment Method for Intelligent Analysis of Battlefield Situational Data" [面向战场态势数据智能分析的预处理方法], *Electronic Technology and Software Engineering* [电子技术与软件工程], vol. 16 (2017). Guo Rui's affiliation is listed as the Fifth Bureau of the Strategic Support Force's Third Department [战略支援部队第三部第五局].

[65] For a more comprehensive analysis of the former Third Department's Technical Reconnaissance Bureaus, see Mark A. Stokes, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure* (Arlington, VA: Project 2049 Institute, 2011).

[66] For the General Staff Department (GSD) 56th Research Institute, see "Network Systems Department 56th Research Institute National Postgraduates Enrollment Exam Subject Catalog" [网络系统部第五十六研究所2017考研专业目录], Exam Training Camp [考研集训营], November 22, 2016, available at <www.kyjxy.com/yuanxiao/zhuanye/33616.html>. For the GSD 57th Research Institute, see "Shengxi Elementary School 2017 Spring Games Grand Opening Ceremonies" [胜西小学2017春季运动会隆重开幕], *Wenji8.com*, April 4, 2017, available at <www.wenji8.com/p/8cbbE3F.html>. For the GSD 58th Research Institute, see "Strategic Support Force 58th Research Institute" [战略支援部队第五十八研究所], Researcher Recruitment Network [研招网], available at <http://yz.chsi.com.cn/sch/schoolInfo--schId-367828.dhtml>.

[67] "School Introduction" [学校简介], People's Liberation Army Information Engineering University Admissions Information Network [解放军信息工程大学招生信息网], available at <http://

zhaosheng.plaieu.edu.cn/contents/249/508.html>.

[68] See, for example, "Announcement on the Publication of the 2017 Chinese Academy of Sciences List of Preliminary Candidates Selected for Academician" [关于公布2017年中国科学院院士增选初步候选人名单的公告], Chinese Academy of Sciences Work Office of the Academic Department [中国科学院学部工作局], August 1, 2017, available at <www.cas.cn/tz/201708/t20170801_4610395.shtml>.

[69] Note that this mission only appears to extend to protecting the PLA's own network, not government or nation-wide networks more generally. See Wang Weiming and Guo Biying [王伟明，郭碧莹], "Stopping Leaks, Military Cyber Experts Teach You the Path of Solving 'Poison'" [防泄密，军队网络专家教你解"毒"之道], *China Military Online* [中国军网], May 23, 2017, available at <www.81.cn/jmywyl/2017-05/23/content_7613285.htm>.

[70] Both Unit 31003 and the Network-Electronic Bureau have been listed at the address No. 226 North Middle Fourth Ring Road, Haidian District, Beijing [北京市海淀区北四环中路226号], the known address of the former GSD Fourth Department. For Unit 31003's address, see "Huading Decorations Successfully Signed Unit 31003" [华鼎装饰成功签约31003部队], Huading Construction [华鼎建筑], December 16, 2016, available at <www.hdzs.com.cn/index.php?m=content&c=index&a=show&catid=5&id=92>. For the Network-Electronic Bureau's address, see "XXX Network-Electronic Bureau Service Unit Single Occupant Housing Refurbish Project Open Bid Advertisement" [XXX网电局勤务队和单身干部宿舍整修改造工程施工招标公告], June 23, 2017, available at <www.bidchance.com/calggnew/2017/06/23/20745058.html>.

[71] "Army Artillery Air Defense Academy and National University of Defense Technology Electronic Countermeasure Institute Debut in Hefei" [陆军炮兵防空兵学院， 国防科技大学电子对抗学院亮相合肥], *The Paper* [澎湃], August 1, 2017, available at <www.thepaper.cn/newsDetail_forward_1748674>.

[72] "Announcement on the Publication of the 2017 Chinese Academy of Sciences List of Preliminary Candidates Selected for Academician."

[73] Zhang Qiaosu [张樵苏], "This Squad Leader Is a Little 'Zhou'—The Journal of Grade Three Sergeant Zhou Yunxiao of a Certain Strategic Support Force Brigade" [这个班长有点"轴"——战略支援部队某旅三级军士长赵云霄记事], Xinhua [新华], June 4, 2017, available at <http://news.xinhuanet.com/politics/2017-06/04/c_1121083630.htm>; Zeng Shijing, Huang Qiyuan, and Li Wen [曾世京，黄琪渊，李雯], "What Are the Highlights for the Military Services Symposium?" [为军服务座谈会都有啥看点?], *China Military Online* [中国军网], May 16, 2017, available at <www.81.cn/zghjy/2017-05/16/content_7603928.htm>.

[74] These units include an electronic countermeasure brigade at Langfang and an air defense electronic countermeasure brigade at Beidaihe, detachments in both Shanghai Nicheng and Yingtan, and satellite stations in Beijing and Sanya. See Liu Yanqian [刘燕倩], "Visit to Give Condolences, Strong Civilian Military Relations" [慰问走访 军民情浓], Shanghai NiCheng Government [中共浦东新区泥城镇委员会], February 13, 2015, available at <https://web.archive.org/web/20160318214622/http://www.nichengdj.gov.cn/html/ArticleShow11343.aspx>; Zhu Fenni [朱芬妮], "City Investment Corporation: Carry out 'August 1st' PLA Day Memorial Activities" [城投公司： 开展"八一"建军节慰问活动], Shanghai NiCheng Government [中共浦东新区泥城镇委员会], July 28, 2016, available at

<http://webcache.googleusercontent.com/search?q=cache:L1wu4NnF6CIJ:www.nichengdj.gov.cn/html/articleshow14968.aspx+&cd=1&hl=en&ct=clnk&gl=us>; "On the Issue of Illegal Burning Near Unit 61906 Troops Stationed in the Area" [关于61906部队驻地附近非法焚烧排放问题], Yingtan Municipal Government [鹰潭市人民政府], December 5, 2016, available at <www.yingtan.gov.cn/gzcy/zxts_1/hbj_1/201612/t20161205_408367.htm>; Stokes, Lin, and Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, 15.

[75] Xiao, *The Science of Military Strategy*, 268. Ye, LSIO, 44.

[76] Costello and Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations," 170–171.

[77] Dai Qingmin [戴清民], "On Integrating Network Warfare and Electronic Warfare" [网电一体站], *China Military Science* [中国军事科学], vol. 1 (February 2002), 112–117.

[78] Costello, "The Strategic Support Force."

[79] It is worth noting that from a purely organizational standpoint, the former GSD Fourth Department only managed a relatively small cadre of bureaus, brigades, and ground stations, which, compared with the organizational heft of the General Armament Department and GSD Third Department, may not have been enough to warrant a separate, third department in the SSF to focus exclusively on electronic warfare.

[80] Li Xiaobiao and Xu Kai [李小彪， 徐凯], "Lei Feng Spirit Motivates Us to Go Forward" [雷锋精神激励我们前行], *db.81.cn*, March 28, 2016, available at <http://db.81.cn/content/2016-03/28/content_6979623.htm>.

[81] Costello and Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations," 178. For an informative discussion on PLA Three Warfares strategic thought, see Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *China Brief* 16, no. 13 (August 22, 2016), available at <https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/>.

[82] The 311 Base operates under MUCD Unit 61716 (61716部队). For a more in-depth discussion of the 311 Base and Liaison Department, see Mark Stokes and Russell Hsiao, *The People's Liberation Army General Political Department Political Warfare with Chinese Characteristics* (Arlington, VA: Project 2049 Institute, October 14, 2013), available at <www.project2049.net/documents/PLA_General_Political_Department_Liaison_Stokes_Hsiao.pdf>.

[83] On the organizational makeup of the 311 Base, see ibid., 29. On its wartime structure, see Kevin McCauley, "System of Systems Operational Capability: Operational Units and Elements," *China Brief* 13, no. 6 (March 15, 2013), 13–17; and Ye, LSIO, 135.

[84] Major General Mei Huabo [梅华波], political commissar of the 311 Base before the reforms, was listed in that position as late as August 2016. In December, it was reported that Mei Huabo was appointed political commissar for an unnamed base under the Strategic Support Force. Other personnel transfers provide further indication the base has moved. In 2016, Mou Shan [牟珊] changed his affiliation from "China Huayi Broadcasting Company" [中国华艺广播公司], the commercial persona of the 311 Base, to a "Certain Department in the Strategic Support Force" [战略支援部队某部]. See Huang Xiaowei and Yu Shan [黄晓伟， 牟珊], "Discussion and Analysis of Taiwan Military Recruitment Promotion Advertisment and Its Effect" [台军招募文宣广告及其效果评析], *Modern Taiwan Studies* [现

代台湾研究], no. 1 (2014), available at <www.cqvip.com/QK/97723X/201401/49213060.html>; Yu Shan [牟珊], "Analysis of NATO Strategic Communication Strategy" [北约战略传播策略探析], *Military Reporter* [军事记者], no. 6, (2016), available at <www.cqvip.com/qk/81377x/201606/669378161.html>.

[85] For an in-depth discussion of the Three Warfares, see Wu Jieming and Liu Zhifu [吴杰明, 刘志富], *An Introduction to Public Opinion Warfare, Psychological Warfare, Legal Warfare* [舆论战心理战法律战概论] (Beijing: National Defense University Press [国防大学出版社], 2014).

[86] An indicator of the uniqueness of the 311 Base's position is its MUCD, which fell under the GSD MUCD block even as the organization was subordinate to the former General Political Department.

[87] Costello and Peter, "Electronic Warfare and the Renaissance of Chinese Information Operations," 188.

[88] The actual grade of the Joint Staff Department may be equal to the Strategic Support Force; however, as a component of the Central Military Commission it acts under its authority in relaying operational decisions.

[89] *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011*, 2.

[90] "The Tenth China Air Show Flight Command Leading Small Group Meeting Was Held in Zhuhai" [第十届中国航展飞行组织指挥领导小组会议在珠海召开], Civil Aviation Administration of China [中国民用航空局], October 29, 2014, available at <www.caac.gov.cn/XWZX/MHYW/201410/t20141029_13886.html>; "The Ministry of Defense Discloses Three Operational Ways Used by Our Naval Forces to Combat Piracy" [国防部披露我国军舰打击海盗三种作战方式], *Sina.com* [新浪], December 23, 2008, available at <http://mil.news.sina.com.cn/2008-12-23/1052536044.html>; Li Yangyang [李杨洋], ed., "Chinese-Pakistan 'Friendship-2011' Joint Anti-terrorism Training Helicopter Unit Arrives in Pakistan" [中巴"友谊–2011"反恐联合训练直升机大队今日启程赴巴], *China Military Online* [中国军网], November 15, 2011, available at <http://military.people.com.cn/GB/42967/16251957.html>; "Writing Style of Major General Liu Xingren" [刘兴仁少将书法作品], *Chinese Army Friendship Net* [中国军谊网], October 29, 2014, available at <www.chinajunyi.org.cn/show.asp?id=1198>.

[91] "Transcript of March 2016 Ministry of National Defense Routine Press Conference" [2016年3月国防部例行记者会文字实录], People's Republic of China Ministry of National Defense [中华人民共和国国防部], March 31, 2016, available at <www.mod.gov.cn/info/2016-03/31/content_4648220.htm>.

[92] "Du Qiang Becomes Central Military Commission Operations Bureau Air Control Office Office Chief" [杜强任中央军委联合参谋部作战局空管处处长], *The Paper* [澎湃], January 19, 2016, available at <http://news.163.com/air/16/0119/08/BDM9D03N00014P42.html>.

[93] Ye, LSIO, 108.

[94] Ibid., 124–131.

[95] Ibid., 134.

[96] Ibid., 127.

[97] Ibid., 134.

[98] Peter Mattis and Elsa Kania, "Modernizing Military Intelligence: Playing Catchup (Part Two)," *China Brief* 16, no. 19 (December 21, 2016), 15–27.

[99] For a deeper discussion on "intelligence" versus "technical reconnaissance," see Peter Mattis, "Chinese Military Intelligence at 90: Consistent Evolution," prepared for CAPS-RAND-NDU Conference, October 2015, 4–7.

[100] Samantha Hoffman and Peter Mattis, "Chinese Legislation Points to New Intelligence Coordinating System," *IHS Jane's Intelligence Review*, September 5, 2017, 7.

[101] Cheng Yongliang and Zhang Xiqing [程永亮，张希庆], "Forging Abilities: Joint Iron Fist Tempers Students" [能力重塑，联合铁拳淬火生], *China Military Online* [中国军网], October 14, 2017, available at <www.81.cn/jfjbmap/content/2017-10/14/content_189717.htm>; Peter Mattis, "China Reorients Strategic Military Intelligence," *IHS Jane's Intelligence Review*, December 2016, available at <www.janes.com/images/assets/484/68484/China_reorients_strategic_military_intelligence_edit.pdf>.

[102] Mattis, "China Reorients Strategic Military Intelligence."

[103] "Professor Huang Zhixiong Holds a Seminar on International Law on Cyberspace for Relevant Military Departments" [黄志雄教授为军队有关部门讲授网络空间国际法], Wuhan Universtiy School of Law [武汉大学法学院], November 2, 2016, available at <http://fxy.whu.edu.cn/archive/detail/102263>.

[104] "Beijing Municipal People's Procuratorate Holds Symposium for Beijing Municipal People's Congress Delegate in Beijing" [北京市人民检察院召开驻京部队市人大代表座谈会], *Suibi8.com*, December 2, 2016, available at <https://webcache.googleusercontent.com/search?q=cache:ju7u3SqBfI8J:https://www.suibi8.com/essay/abf77b-11270011.html+&cd=1&hl=en&ct=clnk&gl=us>.

[105] Li and Xu, "Lei Feng Spirit Motivates Us to Go Forward."

[106] For the former Nanjing Military Region electronic countermeasure center (ECM center), also known as Unit 73677 (73677部队), see Wang Xiaowen [王晓文] et al., "Image Fusion Method Based on Visual Saliency Map" [基于视觉显著图的图像融合方法], *Journal of Jilin University (Engineering Edition)* [吉林大学学报（工学版）] (2014). For the former Guangzhou Military Region ECM center, see Xie Zhiyong [谢志勇], "PLA Representatives of the 18th Party Congress: 'Big Defense' Covers Seas and Space" [解放军十八大代表："大国防"职责涵盖海洋太空], *Beijing News* [新京报], November 14, 2012, available at <http://military.china.com.cn/2012-11/14/content_27104914.htm>.

[107] This is based on papers published under the byline of the ECM centers, which include such topics as "A New Method of PRF Detecting Based on DTFT" [基于DTFT的一种新的PRF检测方法] and "Principles and Realization of Surface Wave Driven Plasma Antenna" [表面波激励等离子体天线的原理与实现].

[108] "After a Year of Military Reform, Review of '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* [解放军报], December 2, 2016, available at <http://military.people.com.cn/n1/2016/1202/c1011-28919716.html>.

[109] Zhang Qiang, Qiao Xuewei, and Zhang Kunping [张强，乔学伟，张坤平], "Who Let 'Command Nerve' Be More Sensitive" [谁让"指挥神经"更灵敏?], *Science and Technology Daily* [科技日报社], July 31, 2017, available at <http://digitalpaper.stdaily.com/http_www.kjrb.com/kjrb/html/2017-07/31/content_374917.htm>.

[110] Ni Guanghui [倪光辉], "Secrets of Our First Strategic Support Force" [揭秘我军首支战略支援部队], *People's Daily* [人民日报], January 24, 2016, available at <http://military.people.com.cn/n1/2016/0124/c1011-28079245.html>.

[111] Peng Guangqian and Yao Youzhi [澎光谦，姚有志], eds., *The Science of Military Strategy* [战略学] (Beijing: AMS Press, 2001), 179.

[112] *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015* (Washington, DC: Office of the Secretary of Defense, 2015), 14.

[113] "Prepared Statement of Mark A. Stokes, Executive Director Project 2049 Institute, before the U.S.-China Economic and Security Review Commission," *Hearing on Chinese Intelligence Services and Espionage Operations* (Washington, DC: U.S.-China Economic and Security Review Commission, June 9, 2016), available at <www.uscc.gov/sites/default/files/Mark%20Stokes_Written%20Testimony060916.pdf>.

[114] Liu, *Theater Command Joint Operations Command*; Shou, *Science of Military Strategy*, 81.

[115] Li Dan [李丹], "What Kind of Force Is the Strategic Support Force Inspected by Xi Jinping?" [习近平视察的战略支援部队是一支怎样的力量?], *CCTV* [央视网], August 30, 2016, available at <http://news.cctv.com/2016/08/30/ARTI2Xi1zgynCfj6TYsecOcb160830.shtml>.

[116] For a detailed discussion of Chinese thinking on counter-intervention, see M. Taylor Fravel and Christopher P. Twomey, "Projecting Strategy: The Myth of Chinese Counter-Intervention," *Washington Quarterly* 37, no. 4 (Winter 2015), 171–187.

[117] A good indicator of this change of terminology is the transformation of the former GSD Survey, Mapping, and Navigation Bureau into the Joint Staff Department Battlefield Environment Support Bureau.

[118] "China to Launch 30 Beidou Navigation Satellites in Next 5 Years," Xinhua, May 19, 2016, available at <http://news.xinhuanet.com/english/2016-05/19/c_135372622.htm>.

[119] Stokes and Cheng, *China's Evolving Space Capabilities*, 23.

[120] Richard D. Fisher and Sean O'Connor, "Space Invaders—China's Space Warfare Capabilities," *IHS Jane's Intelligence Review* available at <www.janes360.com/images/assets/557/40557/Space_invaders.pdf>.

[121] *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015*, 38.

[122] Pollpeter, *China Dream, Space Dream*, 15.

[123] Li Xuanliang and Li Guoli [李宣良，李国利], "Xi Jinping: Strive to Establish a Powerful, Modern Strategic Support Force" [习近平：努力建设一支强大的现代化战略支援部队], Xinhua [新华], August 29, 2016, available at <http://news.xinhuanet.com/politics/2016-08/29/c_1119474761.htm>; Li, "What Kind of Force Is the Strategic Support Force Inspected by Xi Jinping?"

[124] Li, Zhang, and Li, "Army Leading Organs, Rocket Force, and Strategic Support Force Established."

[125] Zou Weirong [邹维荣], "New-Quality Weapons Decide Victory on the Future Battlefield" [新质利器决胜未来战场], *PLA Daily* [解放军报], March 11, 2016, available at <http://jz.chinamil.com.cn/zhuanti/content/2016-03/11/content_6954336.htm>.

[126] Shou, *Science of Military Strategy*, 129.

[127] Zhang Yuliang [张玉良], ed., *Science of Campaigns* [战役学] (Beijing: National Defense University Press [国防大学出版社], 2006); Ye, LSIO, 145–150.

[128] Ye, LSIO, chapter 2.

[129] Ye Zheng [叶征], "Ye Zheng: The 'Seven Weapons' in the Strategic Game of Cyberspace" [叶征：网络空间战略博弈的七种武器], *China Youth Daily* [中国青年报], August 8, 2014, available at <http://theory.people.com.cn/n/2014/0808/c40531-25427203.html>; Costello and Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations," 161–163.

[130] Ye, LSIO, 146–147.

[131] Ibid.

[132] Wang Jinsong, Wang Nanxing, and Ha Junxian [王劲松，王南星，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).

[133] For a more involved discussion of this concept, see Joe McReynolds, "China's Military Strategy for Network Warfare," in *China's Evolving Military Strategy*, 215–216.

[134] Part of the difficulty in understanding this is in usage of Chinese terms. The United States generally differentiates between the terms *information operations* and *information warfare*, with the former being operations conducted in peace and the latter in war. The Chinese do make this distinction; however, they more generally use the term *information operations* [信息作战] interchangeably with *information warfare* [信息战争] and *information countermeasures* [信息对抗], with few consistent differences.

[135] Xiao, *The Science of Military Strategy*.

[136] *National Security Strategy of the United States of America* (Washington, DC: The White House, 2017), available at <www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

[137] Tong Lei [童磊], "Strategic Support Force: Striding Toward the Future's New Type of People's Army" [战略支援部队：迈向未来的新型人民军队], September 29, 2016, available at <www.qstheory.cn/laigao/2016-09/29/c_1119646359.htm>.

[138] Marcelyn L. Thompson, "PLA Observations of U.S. Contingency Planning: What Has It Learned?" in *The People's Liberation Army and Contingency Planning in China*, ed. Andrew Scobell et al. (Washington, DC: NDU Press, 2015), 44–46; Elsa Kania, "PLA Strategic Support Force: The 'Information Umbrella' for China's Military," *The Diplomat*, April 1, 2017, available at <https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/>.

[139] "Prepared Statement of Mark A. Stokes."

[140] Stokes, Lin, and Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, 7. While it is highly likely that the 12th Bureau has moved to the SSF, it has not yet been confirmed whether it has been placed under the Space Systems Department or Network Systems Department.

[141] Stokes, Lin, and Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, 15.

[142] Hoffman and Mattis, "Chinese Legislation Points to New Intelligence Co-ordinating System."

[143] "National Intelligence Law of the People's Republic of China (Draft)," *China Copyright and Media*, May 16, 2017, available at <https://chinacopyrightandmedia.wordpress.com/2017/05/16/national-intelligence-law-of-the-peoples-republic-of-china-draft/>.

[144] "Experts: The Strategic Support Force Will Be the Key to Success Throughout the Entire

Combat Operations Process" [专家：战略支援部队将贯穿作战全过程是致胜关键], *People's Daily* [人民日报], January 5, 2016, available at <http://military.people.com.cn/n1/2016/0105/c1011-28011251.html>.

[145] Lu Xiaomeng, "Scoping Critical Information Infrastructure in China," *The Diplomat*, May 22, 2018, available at <https://thediplomat.com/2018/05/scoping-critical-information-infrastructure-in-china/>.

## About the Authors

***Mr. John Costello*** is Director of the Office of Strategy, Policy, and Plans in the National Protection and Programs Directorate at the Department of Homeland Security. He coauthored this paper before taking his current position. Previously, he served as a Cybersecurity Policy Fellow in New America's Cybersecurity Initiative and a Senior Analyst for Cyber and East Asia at Flashpoint. He is also a former Congressional Innovation Fellow for majority staff in the U.S. House of Representatives Committee on Oversight and Government Reform. During his time on the Hill, Mr. Costello helped investigate the 2015 breach into the Office of Personnel Management and assisted in overseeing Federal information technology management. Previously, Mr. Costello was a Research Analyst at Defense Group. Inc., where he concentrated on Chinese cyber espionage, information warfare, and intellectual property theft. He is a U.S. Navy veteran, former National Security Agency Analyst, and is fluent in Mandarin Chinese, having graduated with honors from the Defense Language Institute. His insights have appeared in *Wired*, the *Wall Street Journal*, the *New York Times*, Reuters, and the Jamestown *China Brief*. Mr. Costello's research focuses on Chinese cyber forces, evolving technology and innovation environment, and quantum technologies.

***Mr. Joe McReynolds*** is a Principal Cyber Analyst at SOS International. His research interests primarily center on China's approach to computer network warfare and defense science and technology development. Mr. McReynolds has previously worked with the Council on Foreign Relations and the Pacific Council for International Policy, and is a graduate of Georgetown University's School of Foreign Service and Graduate Security Studies programs. He speaks and reads Chinese and Japanese and has lived and studied in Nagoya, Guilin, and Beijing.

**China Strategic Perspectives Series**
***Editor*, Dr. Phillip C. Saunders**

No. 12 ***Chinese Perspectives on the Belt and Road Initiative: Strategic Rationales, Risks, and Implications***
by Joel Wuthnow (09/17)

No. 11 ***Chinese Military Diplomacy, 2003–2016: Trends and Implications***
by Kenneth Allen, Phillip C. Saunders, and John Chen (07/17)

No. 10 ***Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications***
by Joel Wuthnow and Phillip C. Saunders (03/17)

No. 9 ***China Moves Out: Stepping Stones Toward a New Maritime Strategy***
by Christopher H. Sharman (03/15)

No. 8 ***Red China's 'Capitalist Bomb': Inside the Chinese Neutron Bomb Program***
by Jonathan Ray (01/15)

No. 7 ***"Not an Idea We Need to Shun": Chinese Overseas Basing Requirements in the 21st Century***
by Christopher Yung and Ross Rustici, with Scott Devary and Jenny Lin (10/14)

No. 6 ***China's Forbearance Has Limits: Chinese Threat and Retaliation Signaling and Its Implications for a Sino-American Military Confrontation***
by Paul H.B. Godwin and Alice Miller (04/13)

No. 5 ***Managing Sino-U.S. Air and Naval Interactions: Cold War Lessons and New Avenues of Approach***
by Mark E. Redden and Phillip C. Saunders (09/12)

No. 4 ***Buy, Build, or Steal: China's Quest for Advanced Military Aviation Technologies***
by Phillip C. Saunders and Joshua Wiseman (12/11)

No. 3 ***China's Out of Area Naval Operations: Case Studies, Trajectories, Obstacles and Potential Solutions***
by Christopher Yung and Ross Rustici, with Isaac Kardon and Joshua Wiseman (12/10)

No. 2 ***Civil-Military Relations in China: Assessing the PLA's Role in Elite Politics***
by Michael Kiselycznyk and Phillip C. Saunders (08/10)

No. 1 ***Assessing Chinese Military Transparency***
by Phillip C. Saunders and Michael Kiselycznyk (06/10)

For a complete list of INSS publications, researchers, and staff, visit http://inss.ndu.edu


ISBN 978-0-16-094959-3