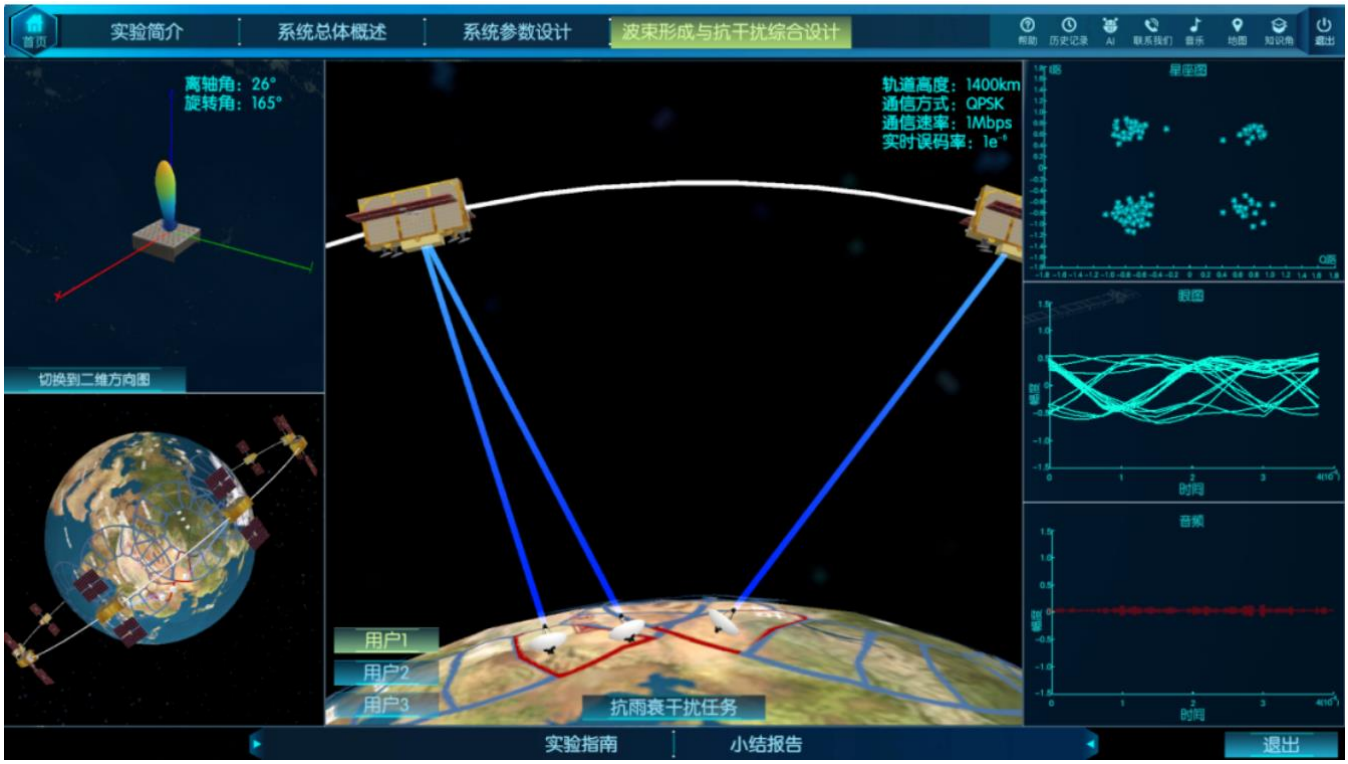
航 空 航 天

CHINA AEROSPACE STUDIES INSTITUTE

PLA Counterspace Command and Control



Kristin Burke

December 2023

Printed in the United States of America
by the China Aerospace Studies Institute

To request additional copies, please direct inquiries to
Director, China Aerospace Studies Institute,
Air University, 55 Lemay Plaza, Montgomery, AL 36112

All photos licensed under the Creative Commons Attribution-Share Alike 4.0 International license, or under the Fair Use Doctrine under Section 107 of the Copyright Act for nonprofit educational and noncommercial use.
All other graphics created by or for China Aerospace Studies Institute

E-mail: Director@CASI-Research.ORG
Web: http://www.airuniversity.af.mil/CASI
https://twitter.com/CASI_Research @CASI_Research
https://www.facebook.com/CASI.Research.Org
https://www.linkedin.com/company/11049011

Disclaimer
The views expressed in this academic research paper are those of the authors and do not necessarily reflect the official policy or position of the U.S. Government or the Department of Defense. In accordance with Air Force Instruction 51-303, Intellectual Property, Patents, Patent Related Matters, Trademarks and Copyrights; this work is the property of the U.S. Government.

Limited Print and Electronic Distribution Rights
Reproduction and printing is subject to the Copyright Act of 1976 and applicable treaties of the United States. This document and trademark(s) contained herein are protected by law. This publication is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal, academic, or governmental use only, as long as it is unaltered and complete however, it is requested that reproductions credit the author and China Aerospace Studies Institute (CASI). Permission is required from the China Aerospace Studies Institute to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please contact the China Aerospace Studies Institute.
Cleared for Public Release, Distribution unlimited.

China Aerospace Studies Institute

CASI's mission is to advance understanding of the capabilities, development, operating concepts, strategy, doctrine, personnel, organization, and limitations of China's aerospace forces, which include: the PLA Air Force (PLAAF); PLA Naval Aviation (PLAN Aviation); PLA Rocket Force (PLARF); PLA Army (PLAA) Aviation; the PLA Strategic Support Force (PLASSF), primarily space and cyber; and the civilian and commercial infrastructure that supports the above.

CASI supports the Secretary, Chief of Staff of the Air Force, the Chief of Space Operations, and other senior Air and Space leaders. CASI provides expert research and analysis supporting decision and policy makers in the Department of Defense and across the U.S. government. CASI can support the full range of units and organizations across the USAF, USSF, and the DoD. CASI accomplishes its mission through conducting the following activities:

- CASI primarily conducts open-source native-language research supporting its five main topic areas.
- CASI conducts conferences, workshops, roundtables, subject matter expert panels, and senior leader discussions to further its mission. CASI personnel attend such events, government, academic, and public, in support of its research and outreach efforts.
- CASI publishes research findings and papers, journal articles, monographs, and edited volumes for both public and government-only distribution as appropriate.
- CASI establishes and maintains institutional relationships with organizations and institutions in the PLA, the PRC writ large, and with partners and allies involved in the region.
- CASI maintains the ability to support senior leaders and policy decision makers across the full spectrum of topics and projects at all levels, related to Chinese aerospace.

CASI supports the U.S. Defense Department and the China research community writ-large by providing high quality, unclassified research on Chinese aerospace developments in the context of U.S. strategic imperatives in the Asia-Pacific region. Primarily focused on China’s Military Air, Space, and Missile Forces, CASI capitalizes on publicly available native language resources to gain insights as to how the Chinese speak to and among one another on these topics.

Acknowledgements

The author would like to thank CASI's Director, Dr. Brendan Mulvaney, for his leadership and foresight in empowering researchers to achieve long-term projects. The author similarly thanks CASI's Research Director, Rodrick Lee, for asking challenging questions, paired with generous evidence sharing. The author also thanks J.J. Long and Josh Fritzjunker at BluePath Labs for their initial deep-dive support, and the Secure World Foundation's (SWF's) Director of Program Planning, Dr. Brian Weeden, and SWF Washington Office Director, Victoria Samson, for their comprehensive final review. CASI's Marcus Clay and Josh Baughman's previous work also contributed to this report. To everyone else who weighed in, thank you.

Table of Contents

Acronyms

2PLA	General Staff Department's Intelligence Department
4PLA/ECM	Electronic Countermeasures and Radar Department
AMS	Academy of Military Sciences
APT	Advanced Persistent Threat
BACC	Beijing Aerospace Command and Control
BMD	Ballistic Missile Defense
C2	Command and Control
CASIC	China Aerospace Science and Industry Corporation
CETC	China Electronics Technology Group Corporation
CMC	Central Military Commission
COMINT	Communications Intelligence
DA-SAT	Direct-Ascent Anti-Satellite
DIA	Defense Intelligence Agency
DoD	Department of Defense
DoJ	Department of Justice
DoS	Denial of Service
DSP	Defense Support Program
ECM	Electronic Countermeasures and Radar Department
EP	Electromagnetic Pulse
EW	Electronic Warfare
GAD	General Armaments Department
GEO	Geosynchronous Earth Orbit
GSD	General Staff Department
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HEO	Highly Elliptical Orbit
HPM	High-Powered Microwave
ISR	Intelligence, Surveillance, and Reconnaissance
JAXA	Japanese Aerospace Exploration Agency
JOCC	Joint Operations Command Center
JSD	Joint Staff Department
KKV	Kinetic Kill Vehicle
LEO	Low-Earth Orbit
MEV	Mission Extension Vehicle
MR	Military Region
MSS	Ministry of State Security

NASIC	National Air and Space Intelligence Center
NDU	National Defense University
NSD	Network Systems Department
ODNI	Office of the Director of National Intelligence
PLA	People's Liberation Army
PLAAF	PLA Air Force
PLASA	PLA Second Artillery Force
PRC	People's Republic of China
RF	Radio Frequency
RPO	Rendezvous and Proximity Operations
S&T	Science and Technology
SAR	Synthetic Aperture Radar
SATCOM	Satellite and Communications
SBIRS	Space-Based Infrared System
SCS	South China Sea
SEU	Space Engineering University
SIPO	State Intellectual Property Office
SMS	Science of Military Strategy
SSA	Space Situational Awareness
SSD	Space Systems Department
SSF	Strategic Support Force
TC	Theater Command
TEL	Transporter-Erector Launches
TRB	Technical Reconnaissance Bureau
TT&C	Telemetry, Tracking, & Control
USG	United States Government
VSAT	Very Small Aperture Terminal

Introduction

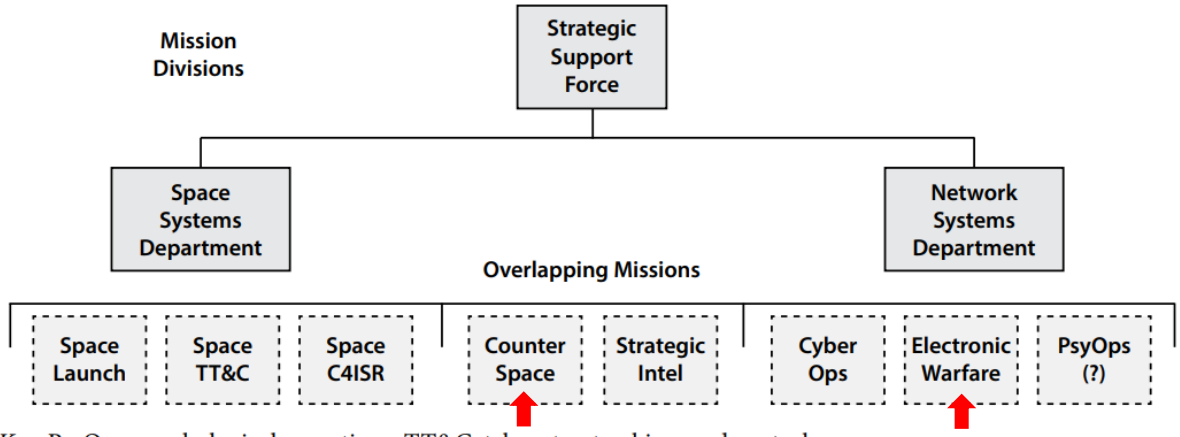
This report started as an effort to answer two questions about each of six counterspace weapon classes typically referenced in unclassified counterspace reports. The weapons discussed in this report include:

Direct-ascent anti-satellite missiles	Directed energy counterspace weapons
Terrestrially-based satellite electronic jammers	Space-based grappling counterspace weapons
Offensive cyber counterspace weapons	Space-based satellite electronic jammers

Questions:

1. Who in the People's Liberation Army (PLA) will operate counterspace weapons in wartime?

2. Who will task the operators and how will the operators use counterspace weapons in wartime?



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

Each of the above six chapters includes a brief summary of the findings, areas for follow-up research, and dedicated sections for each question. Only official People's Republic of China (PRC) and PLA media and books, as well as technical reports by at least one PLA author are included. Each chapter answers the first question differently, based on the publicly available information. For example, some chapters include a likely operator, and other chapters include the most likely operator trainer. In terms of the second question, each chapter describes if the PLA has discussed destructive or reversible uses, and answers if the PLA described those effects as directed by the Central Military Commission (CMC) or a Theater Command (TC).

The goal of such an approach is to bring more fidelity to unclassified reports on the PRC's counterspace command and control (C2) to benchmark and better track organizational changes.

Improved unclassified discussions specific to PLA counterspace weapons C2 supports military planning, and coordination with allies and partners. This research not only empowers the warfighter, but also the diplomat. Dialogue with allies, partners, and Chinese counterparts demonstrates U.S. leadership in the establishment of norms for responsible behavior in space.

This report's initial hypothesis was that counterspace capabilities had been centralized under the Strategic Support Force's (SSF's) Space Systems Department (SSD) and Network Systems Department (NSD), as shown above. Up to now, most western publications describing the SSF have focused on the NSD or on China's military space program generally, without a tailored focus on counterspace weapons. This report attempts to disaggregate the counterspace weapons operated by the SSD and NSD, and highlight any other PLA services' involvement. The research revealed that, at least based on the publicly available information reviewed for this report, this hypothesis may not be accurate. Additionally, the two tailored research questions led to other surprising findings described below.

- **An examination of former General Armaments Department (GAD), General Staff Department (GSD), and new SSF units indicates that it is highly likely not all counterspace weapons will be operated by the SSF.** There are equally strong arguments that, on the one hand, centralizing counterspace weapons under the SSF was never the PRC's intention, and on the other hand, that PLA thinking on integrating weapon developers and operators has impacted decisions regarding the actual PLA operators. Indeed, limited experimental space-based counterspace weapons are probably operated exclusively by the SSF's SSD. However, CMC or TC tasking of other counterspace weapons, to the SSF or other PLA services, is less cut and dry, but seems to depend on if the weapons' effects are limited to in-theater targets.
- **PLA TC commanders may have more ease in tasking low-powered directed energy counterspace weapons and some network-electromagnetic spectrum weapons than terrestrially-based satellite electronic jammers.** Contrary to popular belief, it seems that while terrestrially-based satellite electronic jammers are prevalent across the TCs, the CMC must pre-approve specific usage, in order to limit spectrum interference within the PLA, as well as with Chinese civilian and neighboring country users. Checking with the CMC would presumably also be required for newly identified spectrum use in wartime. When limited to in-theater targets, reversible satellite laser dazzling and weapons to disable systems using space information, such as microwave weapons and network-electromagnetic spectrum weapons, can probably be readily tasked at the TC level.
- **There is limited publicly available information to support that the SSF is the service training with direct-ascent anti-satellite (DA-ASAT) missiles. Rather, there is more information to support those missiles may be operated by other PLA services.** Authoritative PLA texts repeatedly state that kinetic space attacks should be a limited method of achieving space control, and primarily used as a deterrent against strong opponents. The PLA seems more focused on using other types of space control, specifically space situational awareness, satellite maneuverability, and improved encryption.

Hypothesized* PLA Units to Operate Counterspace Weapons in Wartime

Unit Number	Counterspace Weapon	PLA Organization	Location
Interested parties have included PLA Air Force, Rocket Force and former GAD	DA-ASAT Missiles	(?)	Launch pads at multiple SSF and probably at least Rocket Force bases across China
61768	Electronic Jamming	GSD to SSF	Hainan
61764	Electronic Jamming	GSD to SSF	Hainan
32090	Electronic Jamming	GSD to SSF and New SSF	Beijing, Hubei, Jiangxi, Shanghai, Jiangsu, Hainan, Xizang (Tibet)
Multiple PLA Air Force, Navy, and Rocket Force	Electronic Jamming	PLA Air Force, Navy, and Rocket Force Units under new TCs	Multiple
61486	Cyber	GSD to SSF	Shanghai
75770	Cyber	MR to SSF	Guangdong
91746	Cyber	Navy TRB to (?)	Beijing
92762	Cyber	Navy TRB to SSF	Fujian to Yunnan
32082	Cyber	New SSF	Beijing
Multiple non-PLA actors	Cyber	Civilian organization or independent	Across China
63891 and 63892	Directed Energy	GAD to SSF	Henan
32026, 32027, and 32033(?)	Directed Energy	New SSF	Henan and Xinjiang 32033 (multiple)
63660	Directed Energy	GAD to SSF (?)	Henan and Xinjiang
Multiple PLA Air Force, Navy, and Rocket Force	Directed Energy	PLA Air Force, Navy, and Rock Force Units under new TC	Multiple
32032	Space-Based Grappling Weapons	GAD (and GSD?) to SSF and New SSF	Beijing
32039	Space-Based Electronic Satellite Jamming	GSD and GAD to SSF and New SSF	Beijing and Henan

*Some units may not be operators, but rather in charge of training operators.
Striped boxes indicate which counterspace weapons or units are not SSF.
GAD = General Armaments Department; GSD = General Staff Department; SSF = Strategic Support Force; CMC = Central Military Commission; TC = Theater Command

Summary of Central- or Theater-Level Command and Control

Direct Ascent Anti-Satellite Missiles

- Command of missiles for kinetic, destructive attacks that cause debris in space are controlled at the CMC level, and are primarily maintained for a deterrent.

Terrestrially-Based Satellite Jamming Weapons

- All types of PLA electronic jamming operations, including reversible satellite downlink and uplink jamming, must be pre-approved by the CMC. Once approved, the TCs can direct non-SSF PLA services, who will be the primary operators, to attack in-theater targets. The SSF might operate some terrestrially-based satellite jammers as well.

Offensive Cyber Counterspace Weapons

- Network-electromagnetic spectrum operations for both reversible and destructive effects of in-theater targets will probably be prevalent at a tactical level, under TC direction. These operations may be executed by the SSF or other PLA services. The SSF seems primarily focused on electromagnetic spectrum operations to enable cyber intrusion of strategic targets. The effects that transcend a theater or campaign will be directed by the CMC.

Directed Energy Counterspace Weapons

- Reversible satellite laser dazzling operations, with ground-based platforms, are probably commanded at the TC level for in-theater targets. High-power microwave jamming operations, for reversible and destructive effects against space users' equipment, are probably also commanded at the TC level for in-theater targets.

Space-Based Grappling Counterspace Weapons

- If ever miniaturized, these systems would be commanded centrally with the SSF executing the CMC's commands.

Space-Based Satellite Electronic Jamming Weapons

- If operationalized, reversible space-based satellite jamming would be directed at the CMC level, with the SSF executing the CMC's commands.

Key Implications

IMPLICATIONS FOR MILITARY PLANNERS

This report attempts to provide unclassified support to military planners so that they can have wider discussion on how the PLA might use counterspace weapons in wartime. The counterspace weapons deployed to PLA Theater Commands (TCs), and the ease with which TC commanders can task the weapon operators, potentially indicates which type of attacks the U.S. and allied forces could encounter first.

While electronic satellite downlink jamming capabilities are prevalent across different services under the TC commander's control, this report finds that approval for jamming of any kind still must be approved at the Central Military Commission (CMC) Joint Operations Command Center (JOCC). In other words, if a TC in battle detects spectrum usage that was not pre-approved for jamming, commanders probably have to get approval to jam the new spectrum, regardless of if their systems are able to jam that spectrum band or not. CMC spectrum pre-approval is probably also required for high-powered microwave weapons.

CMC consent for usage of other types of counterspace weapons seems to depend on if the weapons' effects go beyond the theater of use. TC commanders can probably readily task low-powered directed energy satellite dazzling, cyberattacks, and radiofrequency delivered malware weapons, assuming they achieve only in-theater, target-specific effects. In the case of beyond-theater effects, such as other spectrum enabled cyberattacks or spoofing, a CMC controlled unit of the Strategic Support Force (SSF) is probably the primary operator. The CMC probably directs cyberattacks on satellite ground stations in theater, especially attacks to deliver malware to adversary satellites, because of the beyond-theater effects.

U.S. and allied military planning for missile defense of direct-ascent anti-satellite (DA-ASAT) missiles should include considerations that the PLA's DA-ASAT missiles may be deployed from SSF, PLA Air Force, or PLA Rocket Force bases and positions. There is evidence to indicate that the SSF is not the exclusive owner of those mobile launchers. While finding current evidence that the PLA Air Force or the Rocket Force has these missiles is out of scope for this report, unclassified imagery analysts and planners are encouraged to expand their examination of non-SSF bases. While DA-ASAT missiles potentially could be deployed from many more places than expected, the PLA's primary intention for the missiles is to be a credible deterrent, and only the CMC would cautiously approve their use.

On-orbit satellite jamming is the one counterspace weapon this report found to be operated exclusively by the SSF. TC Commanders most likely have a role in tasking satellites for in-theater use, to include debris maneuver plans that accommodate continued in-theater use, but on-orbit jamming to support a TC will most likely be decided and executed from the CMC. On-orbit grappling is unlikely to be used as a counterspace weapon until those systems can be miniaturized.

IMPLICATIONS FOR POLICYMAKERS

U.S. Department of Defense (DoD) Directive 3100.10 Space Policy, as updated in August 2022 calls for continued effort towards establishing, demonstrating, and upholding norms of safe and responsible behavior, as well as updating classification for DoD space programs. Towards these aims, this report provides an unclassified basis on which to include space-based satellite jamming as the next area for norms development. The findings further emphasize the need for better rules regarding commercial space operators' reporting of cyber intrusions. Regarding classification challenges, differentiation between campaign and tactical level counterspace weapons, rather than lumping them all erroneously into a strategic category, could improve allied and partner participation in wargaming.

This report raises important questions for policymakers. First, is the U.S. In-Space Servicing, Assembly, and Manufacturing National Strategy sufficient, considering that the PLA is training its space operators to conduct debris-removal operations, and may institutionalize the capability? Second, if the PLA leverages psychological operations as a counterspace weapon, such as by limiting international trust in the U.S. space catalog, how will policymakers mitigate the fallout? Third, the PLA seems to be modeling the United States in developing a dedicated unit to conduct defensive and offensive orbital warfare, like Space Force Delta 9, and orbital warfare exercises like Red Skies. How can policymakers better monitor the incremental impact of United States messaging on foreign perceptions and mitigate miscommunication?

IMPLICATIONS FOR PLA RESEARCHERS AND CYBERSECURITY EXPERTS

This report can help drive cross-sectoral collaboration between the PLA expert community, the counterspace community, and the corporate cybersecurity community. This report needs to be analyzed, picked apart, and built upon, as it is one of the first unclassified reports to attempt to bridge the literature and thinking across respective fields.

Initial cross-sectoral research on counterspace weapons elevated potential confusion researchers may cause when using certain terms. Overuse of words like "strategic," "campaign," and "tactical," without clear, mutually agreed upon definitions outside of the nuclear field might overemphasize the SSF's role in counterspace. Discussion on electronic jamming and reversible directed energy weapons as separate weapon groups, rather than approaching the electromagnetic spectrum wholistically, could limit researchers when shining a light on PLA electronic warfare planning. Repeated use of PLA terms like "network-electromagnetic spectrum" operations while not explaining its similarity to historical U.S. "RF-enabled cyber" or "electronic warfare and cyber convergence" initiatives, may unintentionally mislead military planners and policymakers to think this is new or specific to the PLA.

Chapter 1: Reevaluation of Pre-SSF Debates on PLA Space Organization, with a Focus on Counterspace

In the chapters that follow, the reader may be surprised to learn that the wartime operation of the People's Liberation Army's (PLA's) counterspace weapons highly likely continues to be spread across PLA services, as well as the Strategic Support Force (SSF). While most western analysis on the SSF states that it centralizes strategic or national space, cyber, electronic, and psychological warfare missions and capabilities for the PLA, most analysts are referring to the PLA space sector broadly, not specifically counterspace weapons.

As displayed in the PLA's 2019 Military Parade pictured below, PLA services transferred some of their personnel to the SSF. In some cases, these new SSF transfers who wear PLA service uniforms with SSF patches may be SSF liaisons, science and technology personnel, or operators of weapons now managed by the SSF. This report finds that at least currently, not all counterspace weapons are managed by the SSF.

Given that the People's Republic of China (PRC) planned for the PLA reform, which included the establishment of the SSF, to be completed by 2020—and at the time of publication, it is nearly the end of another five-year plan in 2025—the current setup is likely to persist. There is still some movement of PLA service components to the SSF, and restructuring of the former Central Military Commission (CMC) general departments within the SSF, but now is the time to consider that any service in the PLA could use reversible counterspace weapons for in-theater effects. This acknowledgement could enable many possible mental shifts, such as to consider what the SSF is freed up to do better, if they are not strapped will all counterspace operations. For

example, the SSF Space Systems Department certainly is improving space-information support to the PLA's joint forces. It is possible they are doing that better than some assume. Another shift could be to reevaluate commercial imagery of PLA Rocket Force and PLA Air Force bases for equipment that could actually be counterspace systems.

Recalling internal PLA debates about the space sector in the lead up to the eventual establishment of the SSF presents an opportunity to better understand the PLA's command and control (C2) of counterspace weapons. Provided in this section is a snapshot, not a thorough review of those debates.

During the timeframe when the PLA was achieving counterspace technology test milestones for technology funding they had requested in the 1980s, such as successfully dazzling a U.S. National Reconnaissance Office satellite, and successfully launching a missile at a Chinese satellite, PLA services and the CMC general departments were in active debate over how to organize command authority for wartime space operations. These debates were not specific to counterspace, but specifically how to ensure space information would be available to the PLA warfighter and their weapon systems. The common complaint against the former General Armaments Department (GAD), which then managed the PLA's space launch and tracking centers, was that it was not sufficiently nimble for responsive space operations, such as quickly launching replacement satellites, and quickly providing tailored space information to the PLA warfighter.[i]

A review of past western accounts of the PLA's pre-reform debates on the organization of its space capabilities, with an eye towards what western researchers now know about the SSF, illustrates that the PLA's debates were primarily about improving the PLA warfighters' access to a variety of space information, especially in a wartime scenario. The PLA's debates were not primarily about centralizing counterspace weapons. At the time, the PLA Second Artillery Force (PLASA) and the PLA Air Force (PLAAF) both had developed teams thinking about how to ensure they could use space information in their missile and air-defense missions, including how to protect their ability to use space and counter others, with direct ascent anti-satellite (DA-ASAT) missiles, and satellite electronic jammers. The GAD was involved with both the PLASA and PLAAF in supporting their satellite launch and tracking needs, as well as weapons testing and development, to include developing reliable laser capabilities for multiple services' platforms. The GAD and the General Staff Department (GSD) were also developing their own on-orbit capabilities.

While all were increasing their usage of space, an additional complaint was that no one was in charge of coordinating and commanding all these systems for a wartime scenario. While there were many actors involved, none of them seemed to want to take over the others' existing capabilities; however, they all pushed for a better way to readily access space information in wartime, and agreed there needed to be a reorganization.

While it may have seemed that the creation of the SSF scrapped the PLAAF's CMC approved "integrated air and space" strategy and it may have seemed that the elevation of the PLASA to the Rocket Force required them to focus more on other strategic missiles, rather than

[i] Former GAD organizations then managed, and continue to manage, the PLA's space launch and tracking centers, as well as many equipment and weapon test bases. PLA and PRC commentators have continuously referred to them as science, technology, and engineering personnel, not operational troops. Even now that they have largely transferred to the SSF, they are still primarily technology support units.

DA-ASAT missiles, these assumptions may need to be reevaluated. Upon rising to power, Xi Jinping made a speech in 2012 to the PLASA, which the Global Time's Mandarin language paper interpreted as Xi supporting the PLASA to, "step up the construction of ground-based anti-satellite operational forces and ensure the on-schedule formation of combat capability." Global Times is not an official PRC media outlet and represents the nationalist's view, but the paper still can't significantly misrepresent the PRC leader's views. In a 2014 speech to the Chinese Communist Party Central Committee, Xi Jinping cast his support behind the Air Force's role in the integration of air and space saying that, "building a strong People's Air Force with integrated air and space and both offensive and defensive [capabilities] is a major mission entrusted to the Air Force." In a 2021 PLA book called A Conceptualization of Outer Space Military Application Strategy, the authors still reference "persist[ing] in the strategic guiding principles of…the integration of air and space."

It is possible that Xi would establish the SSF, and keep the existing counterspace weapon setup for some weapons. After the creation of the SSF, PLA commentators described the types of weapons that the SSF would absorb as being "information warfare weapons." From the PLA perspective, information operations certainly include space information, though this may be different from the U.S. Department of Defense's (DoD's) thinking. Neither the PLA nor the U.S. seems to go as far as to say that counterspace weapons are a counter-information operation weapon. The PLA National Defense University's Science of Military Strategy in 2020 stated that, "Because of the decisive influence of space control on cyberspace and other military spaces, it will become the key to defeating the enemy in information warfare." This could mean that using the SSF to better coordinate information operations, and presumably counter-information operations, for the PLA joint forces would not require that only SSF personnel operate counterspace weapons in wartime. Alternatively, it could also mean that counterspace operators sit in their same locations, with other service uniforms and new SSF patches.

Chapter 2: Direct Ascent (DA)-ASAT Missiles

SUMMARY

The PLA has at least one direct ascent (DA) anti-satellite (ASAT) missile currently fielded on a road-mobile platform, and Chinese official media, in Mandarin, has indicated that the platform is basically the same as a PLA anti-aircraft missile chassis, but with a different missile. Based on the Office of the Director of National Intelligence's (ODNI's) reports to the United States Congress, the PLA has been "training" with this missile since at least 2018. The ODNI, former National Air and Space Intelligence Center (NASIC), and Defense Intelligence Agency's (DIA's) public reports do not state that there is a specific unit or service training with DA-ASAT missiles, nor do they clarify the mode of training. These public reports do, however, indicate that the PLA has a specific DA-ASAT-capable missile, which the reports say is intended to target low Earth orbit (LEO) satellites flying over China. In mid-2021, Chinese official media published an interview with a PLA Northern Theater engineer who stated that the PLA has three DA-ASAT-capable missiles, the DN-1, DN-2, and DN-3 that can reach low, medium, and high orbits.[ii]

This chapter does not investigate which of the PLA's medium-range ballistic missiles enabled the January 2007 destructive DA-ASAT test, nor what advances were tested in the non-destructive July 2014 test, which are the only two tests that have been publicly confirmed by the United States Government (USG) as DA-ASAT tests. The U.S. Department of Defense has been more forward leaning on its assessment of the May 2013 launch from Xichang, Sichuan Province, but only in the department's elimination of supporting evidence for China's claim of a high atmospheric test. Chinese official media in mid-2021 confirmed these three as DA-ASAT tests, and confirmed an additional July 2017 test.

This report initially hypothesized that it must be the Strategic Support Force (SSF) that is training to launch DA-ASAT-capable missiles, because much of the western descriptions of counterspace issues focus on the SSF. Ultimately, this research did not find evidence to support that hypothesis. Instead, the SSF is training to support different PLA services with probably multiple types of road-mobile missiles, probably to include the DA-ASAT-capable missile. This distinction implies that researchers have been over focused on the SSF when analyzing command and control (C2) for DA-ASAT missiles. PLA academy textbooks repeatedly state that the PLA Air Force, Rocket Force and Army will be the likely operators of DA-ASAT-capable missiles, but it is still unknown if the operators are SSF-badged personnel wearing Rocket Force uniforms, for example. Upon Xi Jinping's rise to power in 2012, some Chinese PLA commentators claimed Xi supported the, then Second Artillery Force, to operationalize the DA-ASAT missile. Below, this report includes an example with pictures of what might be the SSF training with a DA-ASAT

[ii] The specific reference says, "2007 年 1 月 11 日，我国在西昌卫星发射中心发射了一枚 SC-19，也叫作 DN-1 的反卫星导弹，该导弹携带动能弹头，以每秒 8 公里的速度，击毁了轨道高度 863 公里，重 750 公斤已报废的"风云一号"气象卫星，这是我国第一次成功地拦截人造卫星，自此，我国正式踏入了反卫星技术领域.

之后，我国又相继研制出了第二代 DN-2 和第三代 DN-3 两款最新反卫星导弹，并在 2013 年 5 月和 2017 年 7 月 23 日分别进行了 2 次成功试验。DN-1、DN-2 和 DN-3 反卫星导弹的成功研发，将低、中、高轨道全面覆盖，人造卫星基本都处于我国反卫星导弹的打击范围之内，这标志着我国在该领域技术已进入世界一流水平."

missile together with other PLA services, but this is far from certain. The example could also be a mobile satellite launcher, or a mixing of photos from different locations and trainings.

Ensuring multiple services are capable of launching DA-ASAT-capable missiles is the best way for the Central Military Commission (CMC) to achieve its primary intention, which is to deter and develop other capabilities. The emphasis on DA-ASAT missiles as a deterrent is evidenced by decades of repeated PLA textbooks and official media statements. From the PLA's perspective, as is generally consistent among other DA-ASAT-missile-enabled countries, ballistic missile defense (BMD) capabilities can be developed first through a test with a cooperative target, like a satellite. There is prevalent evidence that initial tests of DA-ASAT capabilities supported PLA Air Force and Rocket Force missile developments. The PLA also often co-locates missiles, such as strategic and conventional missiles, and may consider making transporter-erector-launchers (TELs) capable of launching both BMD and DA-ASAT-capable missiles, intentionally, as a deterrent.

Publicly available information reviewed in this report indicates that at least space experts from General Armament Department (GAD) organizations in Beijing, i.e. not at the launch centers, and the PLA Air Force were both active in setting up and evaluating the 2007 test. There is evidence to suggest that, in addition to GAD organizations, the now Rocket Force was similarly involved in the 2013 high-altitude test. Chinese official media, in mid-2021, confirmed a technology development feedback loop between ASAT tests as support for BMD. Specifically, the PLA Northern Theater engineer stated that, "At present, anti-satellite technology is mainly developing in the following aspects: combining anti-satellite and anti-missile, and using the development of missile defense systems to further improve the anti-satellite capability of kinetic energy weapons."

Below, this report describes evidence of the SSF's support to other services' missile units, and shares the best available example that could indicate the SSF might have a dedicated DA-ASAT missile unit. This report does not attempt to disaggregate which of the other services' units are equipped with exo-atmospheric BMD-capable missiles. The evidence of the Air Force and Rocket Force's involvement in early tests should support pertinent follow-up research for anyone trying to understand where those weapons are likely to be deployed across China. The first section attempts to answer, "Who in the PLA will use DA-ASAT missiles?"

PLA UNITS INVOLVED IN CONFIRMED AND PROBABLE XICHANG TESTS

Before PLA reform, and during the time of China's first ASAT test from Xichang City, Sichuan Province, the PLA Air Force, and space experts under GAD organizations in Beijing, were the most active military organizations writing about DA-ASAT and kinetic kill vehicle (KKV) related plans and technology. None of the technical reports discussed below show joint authorship between the Air Force and the space organizations. However, it is important to note that the GAD was one of many organizations that was primarily staffed by PLA Army personnel and operated as part of an Army headquarters.[iii] With that in mind, some GAD organizations did support some joint space capabilities, for example, the astronaut corps has always been entrusted to PLA Air

[iii] A PLA Army Headquarters was not established until the 2015 reform.

Force pilots, until recently. All of that is to say that there could have been coordination not obvious from the articles.

The scientific and technical publications from the time do, however, clearly indicate that technology development for ballistic missile defense (BMD) and satellite interceptors were both drivers for both the GAD and PLA Air Force. In fact, U.S. scientists and Chinese military experts have pointed out that an incremental approach to BMD development often begins with targeting a satellite; using a cooperative object enables testing of fundamental missile and support capabilities.

- The PLA Air Force Missile Academy, in Sha'anxi Province, and the PLA Air Force Air Defense Equipment Academy, in Beijing, between 2001 and 2009, wrote about KKVs for both missiles and satellites, and built an "anti-satellite intercept simulation system" based off their earlier work on anti-missile systems. The 2007 PLA Air Force paper on anti-satellite intercept simulation states that the simulation system was confirmed to be accurate in January 2007, which is the month of China's first test.
- A GAD organization called the PLA Equipment and Command Institute, which is now the SSF's Space Engineering University, published on the factors for selecting an orbit for a space interceptor test in 2007, the analysis of which did not include debris. The Equipment and Command Institute and the Beijing Aerospace Command and Control Center (BACC), both GAD organizations, collaborated on a different paper that they submitted in late 2006. Their paper was about a method to translate coordinates for a KKV against a space target, and it was published in May 2007.

Interestingly, this report did not find evidence of PLA units under the Xichang Satellite Launch Center, also known as Base 27, working on related topics in the 2005-2008 timeframe; this report also did not find evidence of PLA units under the Jiuquan Satellite Launch Center, also known as Base 20, active in Xichang at the time. This could confirm that, like launch base personnel in other countries, units at Xichang accommodate whoever is scheduled to use the launch pads. One would think, at least, the Base 27 leadership would have some input or oversight. Along those lines, from 2003 to 2013, recently removed General Li Shangfu was, at the time, the Commander of Base 27, and the Political Commissar (PC) between 2006-2009 was a Second Artillery Commander, now recently retired PC of the Rocket Force, General Wang Jiasheng. Prior to the recent anti-corruption campaign, Li had been replaced by Rocket Force commander, Zhang Zhenzhong. The PC that was most likely in charge during the probable 2013 test was Major General Sun Baowei, now an advisor to the China Space Foundation; Sun's deputy, now General Wang Jingzhong, became the PC at the end of 2013.

It is an often-overlooked detail that the Rocket Force has had strong leadership, and probably technician-level presence at Xichang during China's destructive ASAT test and probable high-altitude test. The now Rocket Force's scientific and technical literature from the time also demonstrates their simulations and tests on intercepting satellites in geosynchronous Earth orbits (GEO) and elliptical orbits in the 2012-2014 timeframe. Upon Xi Jinping's rise to power in 2012, some Chinese PLA commentators writing in the Global Times claimed that Xi supported the then Second Artillery Force to operationalize the DA-ASAT missile. The PLA author said the then Second Artillery Force should, "step up the construction of ground-based anti-satellite operational forces and ensure the on-schedule formation of combat capability."

SSF SUPPORT FOR TRAINING WITH DA-ASAT-CAPABLE WEAPONS

After the May 2013 launch, which China has acknowledged was an ASAT test, out of Base 27, testing moved out to the Korla Missile Test Complex (Korla) in Xinjiang Province, construction of which was completed in late 2009. Korla is jointly managed by SSF units (formerly GAD) out of Jiuquan Satellite Launch Center (Base 20) and the Shuangchengzi Missile Test Complex in south central Inner Mongolia Province, near Jiuquan City in Gansu Province. U.S. government agencies did not start to report PLA units training with ASAT missiles intended for LEO satellites until after the shift to Korla, and the later establishment of the SSF in late 2015.

While unclassified evidence indicates that the PLA began "training with ASAT missiles" around 2018, it does not tell us who in the PLA was training, nor the mode of training. The Base 20 subordinate units stationed out in Korla start around Unit 63610, and their scientific and technical publications, and online activities, indicate they support missile testing for ballistic missile defense (BMD), to include managing the testing, tracking, and training areas in Korla.[iv] Units after 63620 are also doing missile testing and BMD support, but more than exo-atmospheric BMD, to include hypersonic cruise missiles, and are primarily stationed at Base 20 facilities in Inner Mongolia and Gansu provinces. As an initial hypothesis, this report focused research on units located in Korla.

- Units 63610-63618 are all located in Korla, and support missile testing and BMD through developing new, and managing existing, early warning radars at the Korla Missile Test Complex. This includes support work on the development and integration of early warning satellite data to fill gaps identified in radar tracking. Their activities are consistent pre-and-post PLA reform, based on their online presence and authorship of scientific and technical journals.
- Because SSF units are sometimes composed of members from other PLA services, and the PLA intends the SSF and its training to support deeper integration of joint forces, training at Korla and elsewhere probably regularly includes members from other PLA services. For example, SSF unit 63611, has together with the SSF Space Engineering University (SEU), written proposals for space training exercises similar to the U.S. Schriever and Space Flag war games, that integrate multiple services and commands, and which seem focused on training with missiles.
- In a joint article with the China Aerospace Science and Industry Corporation (CASIC) in 2021, CASIC, SEU and Unit 63611 thoroughly analyzed the positioning of a "weapons system" across China that considers the need for launch sites, standby sites, and other logistics such as fuel. It seems unlikely that this article is about the SSF's training for responsive launch, in which they don't normally refer to Kuaizhou launchers as a weapon system.

Mobile missile launch trucks usually need other support equipment to be road mobile as well. Targeting for missiles or non-cooperative satellites would need some of the same space

[iv] The unit number for Base 20 is 63600. It is one of many former GAD launch bases that transferred to the SSF and maintained its original identifier.

situational awareness information. When investigating the mobile telemetry, tracking, and control (TT&C) units, and separate mobile communications units, this report found recent examples of these groups discussing how to support new combat training tasks.

- Korla-based Jiuquan Unit 63611, SEU, and Taiyuan-based Unit 63723, in 2021, jointly authored a paper on how to better support the "increasing scale and frequency" of PLA training that needed satellite monitoring and forecasting support. The SSF units supported other PLA services to know when satellites were overhead during training, or during transit across China.[v]
- Unit 63726 is a forward deployed Taiyuan subordinate unit based in Yinchuan, Ningxia Province, the location of which is probably to support missile testing in transit west towards Korla. In mid-2019, Unit 63726, together with authors from the Air Force Dalian Communications Academy, argued that, at the time, they couldn't support each battle unit in training, but that the solution was not to have more communications trucks. They proposed that the Joint Logistics Support Force should require the mobile TT&C units to focus their support on "emergency launch drills" and conventional combat testing tasks, while also training the existing mobile units to be better prepared to camp in harder conditions for longer.
- Unit 63726, in June 2022, proposed solutions to maintaining their equipment in a deployed environment, which might indicate they are implementing lessons learned from proposed training in the above 2019 paper.
- The Xi'an Satellite Control Center, also known as SSF Base 26 and Unit 63750, also has mobile tracking and recovery teams. One of those aforementioned mobile recovery teams is Unit 63762, in Weinan, Sha'anxi Province. Unit 63762 collaborated with Base 26 and another subordinate unit, 63751, which is called the satellite communications station, to author a paper in 2018 which explained that their normal methods for calibrating antennas is not suitable for rapid deployment and mobility during wartime. They proposed a quick fix solution for mobile teams to be able to "construct missile and satellite launch sites" with acceptable accuracy.

[v] The Taiyuan Satellite Launch Center, also known as Base 25 or Unit 63710, is based in Shanxi Province.

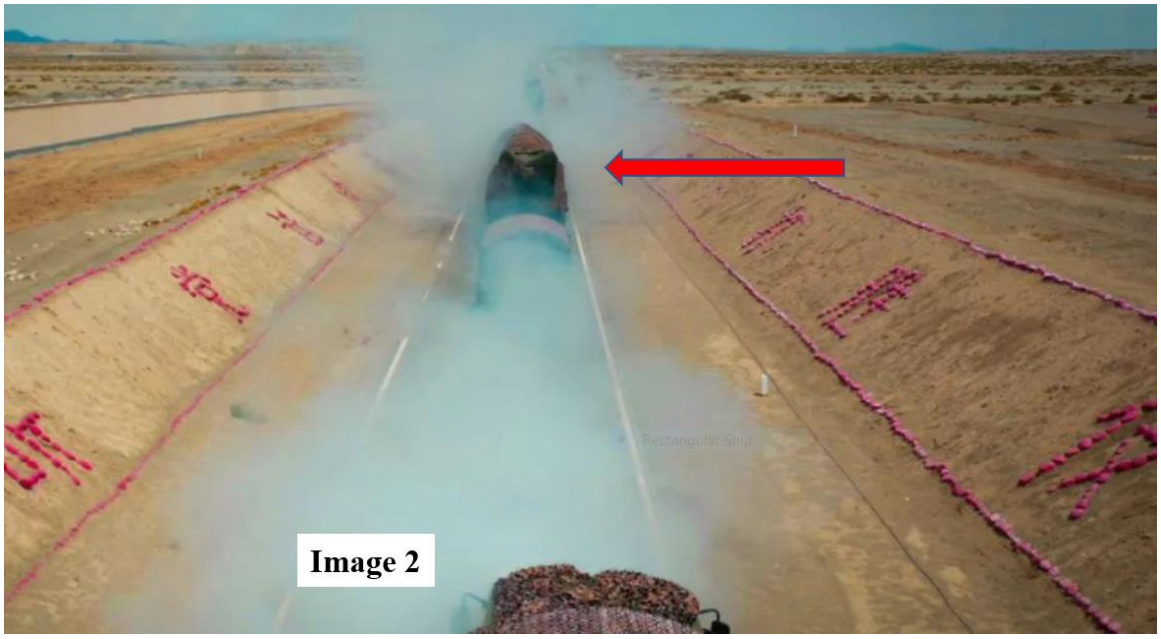
POSSIBLE SSF MOBILE MISSILE TRAINING

The best available example of SSF units either, training directly with missiles, training in support of another service's mobile missile units, or training with mobile satellite launchers in Xinjiang Province, is a July 2022 training that included at least two units, one of which is not stationed in Xinjiang, but is probably SSF. These units conducted a red-on-blue training, where the red team simulated a "launch," the satellite-supported navigation for which was jammed by the blue side. Image 1 below is from a PLA social media posting, and shows what appears to be a type of transporter erector launcher (TEL) in the vehicle train (indicated by a red arrow). Most images of Kuaizhou TELs show that the rocket hangs well over the front of the truck, but in Image 1, the unidentified equipment is tucked into the truck more like a missile, and appears to be much larger than what was shown in PLA video coverage of its 2010 BMD test. In image 2, also taken from the July 2022 PLA social media article, the probable missile (indicated by a red arrow) doesn't appear to be in a containerized setup, while other missiles such as the Rocket Force's DF-21s deployed in Xinjiang, and the double missile HQ-19s that the Air Force tested in Xinjiang, are both in a containerized configuration.

The vehicle train in Image 1 could be driving East out of what is thought to be one of the SSF's facilities supporting ASAT tests near Korla at 41.3111N, 86.2111E. This judgement is based on the smokestacks in the background, left of the red arrow, which would be consistent with those to the facility's Southwest at 41.31.46N, 86.1833E. However, there was no obvious recessed road through which to drive in a contaminated environment, as seen below in Image 2. Image 2 appears to take place next to a fence, but this nor the recessed road was visible in the imagery this report reviewed near the Korla facility. The camouflage over the probable missile also appears to be different colors in the images, further indicating that these photos are possibly not from the same location or even the same training type.

The importance of correctly locating Image 2 rests in the fact that it seems to show the back of what might be a missile TEL, providing additional detail on the type of missile. The text of the report states that the training took place in the northwest Gobi Desert (戈壁滩), which, if geographically accurate, would actually indicate it was well north of Korla, closer to where

Image 1



Xinjiang Province borders Gansu Province. However, just like many western analysts who inaccurately refer to all of northern China's deserts as the "Gobi," so do many Chinese. Large sections of Gansu, Ningxia, Inner Mongolia, Sha'anxi, and Shanxi provinces have deserts and missile launch support facilities, which means that the picture could have been taken in any of those locations. Yet another possibility is that the term used for Gobi Desert is sometimes associated with a desert farther west of Korla, near Kashgar City in Xinjiang Province. In any case, more open-source imagery analysis is needed to correctly confirm the location of these images. The images do at least confirm SSF training probably somewhere in Xinjiang, to support either their own or other services' missiles, potentially even DA-ASAT missiles.

As indicated in the PLA social media posting, at least one SSF unit that participated in the red-on-blue training had never traveled to Xinjiang for training. Image 3 below reveals one vehicle's license plate reads YZ, which is the indicator for SSF units from the Central Theater Command. Taiyuan's Base 25, and Xian's Base 26, are both in the Central Theater, and as indicated above, they and their subordinate units have authored scientific and technical reports examining methods to more frequently participate in training needed to support rapid launch capabilities, probably for both rockets and missiles.

Image 3

Further complicating this assessment is that the SSF hosts its entry level training in Xinjiang, as well as hosts SSF units and possibly other services from other provinces for basic and advanced testing and training with new technology in Xinjiang. Other PLA social media reports, though without images of potential TELs, further confirm that, at least in the 2020-2021 timeframe, units from the Central Theater traveled to Xinjiang. The purpose of the travel to Xinjiang was to help the troops get experience using equipment, like microwave communications towers and possibly mobile tracking and guidance antennas, in the rougher conditions, similar to what they might face in a deployed environment. See Image 4 and 5. The specific location in Xinjiang Province still remains speculative, as some articles refer to the often misused "Gobi Desert." In a separate example from late 2022, a base in central China set up a communications substation in Kashgar and traveled more than 3,000 kilometers from its base to finish the installation and run checks, indicating it could be a Base 25 or Base 26 substation.

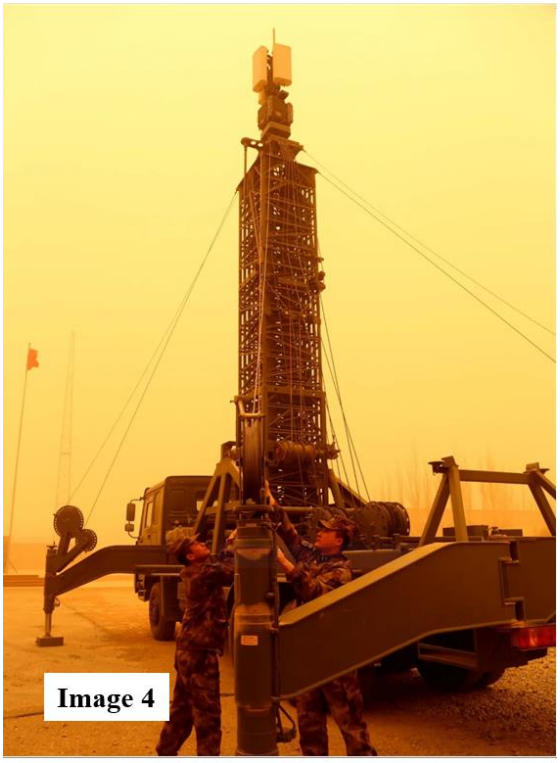


Image 4

When considering these findings with other chapters in this report, an alternative hypothesis is that the Central Theater equipment is a relic of many

Image 5

of the Xinjiang-based SSF facilities transferring under a new SSF Base 36 in Kaifeng, Henan Province. Base 36 "undertakes weapons and equipment demand demonstration, testing, appraisal and evaluation tasks," and it is possible that when a related training or test takes place, the PLA ships their equipment from Henan via train.

Yet another possibility is to return to the idea that the SSF is supporting another service's simulated launch. In February 2018, the SSF and the Rocket Force conducted a joint training from an underground facility. This training consisted of the Rocket Force identifying an incoming missile, requesting the SSF provide satellite navigation support, and simulating a counter-missile launch.

HYPOTHESIS OF PLA COMMAND AND CONTROL (C2) FOR DA-ASAT MISSILES

In an attempt to bring more fidelity to China's counterspace C2, this section will attempt to answer two questions. First, "What is the most likely chain of command for the PLA to decide when to use DA-ASAT missiles?" This first question relates to the first section's question which attempted to answer, "Who in the PLA will use DA-ASAT missiles?" The second question is, "In what way will the PLA be directed to use DA-ASAT missiles?"

All available PLA academy literature, from the early 2000s to 2020, describe that the decision to use a kinetic space attack weapon during a conflict would be made at the central level, through something like the newly established Central Military Commission's (CMC's) Joint Operations Command Center (JOCC). Publications from different organizations have confirmed that the decision to use kinetic space weapons would be centralized, but have discussed different potential users.

An early textbook recommended kinetic space attack weapons should be commanded from something like the new Space Systems Department (SSD) of the SSF, directly under the CMC, probably in order to ensure an informed decision regarding the space environment and other space operations. For example, in 2014, the PLA National Defense University (NDU) authored a book called Space Information Assisting-Support Operations, which outlined recommendations for the future organization of China's space information support units. The text specifically distinguished between space information support units and ground-based ASAT missile units. The authors recommended that the former should be managed at each theater level, with coordination and prioritization at the central level, and that a space command under the center should provide organizational command of space weapons in wartime.

In a different book, which has been authored at different times by the PLA Academy of Military Sciences (AMS) and separately the PLA NDU, called the Science of Military Strategy (SMS), the authors have continuously reiterated that a centralized and unified command is of utmost importance for successful PLA joint operations in informatized, and now intelligentized, warfighting conditions. While the SMS books have been getting gradually less detailed, the 2020 version does clarify that kinetic space weapons are a type of strategic power and must be used in support of the overall mission, indicating that the decision to use them is still probably centralized.

While the agreement that any use of kinetic space weapons should be determined through a centralized decision-making mechanism persists, the complexities discussed in the first section, regarding which unit would operate DA-ASAT missiles are also reflected in PLA training and theory textbooks. Leading up to the establishment of the SSF, PLA academy books that focused on space, from both the AMS in 2013 and the PLA NDU in 2014, referred to either "ground space

defense units" and "ground-based ASAT operational strengths," respectively. The AMS book called Lectures on the Science of Space Operations further distinguished between "strategic missile units," and "space service and support units." The PLA NDU had separate categories for ground-based ASAT units and space-based ASAT units. These different categories probably indicate that leading into the establishment of the SSF, PLA theorists were undecided on which unit would receive the tested and ready weapon.

Looking at one of the possibilities, the implications for C2 of having potentially dedicated DA-ASAT units could imply that a non-SSF PLA service has received those weapons and is training with them. Indeed, the 2013 SMS written by AMS indicated that, at the time, what is now the Rocket Force, was in charge of maintaining DA-ASAT units. The 2013 SMS states that,

> *"An example during a joint fire strike is the use of Second Artillery Corps conventional missile units for preliminary strikes against the enemy's reconnaissance and early warning systems, EW systems, air-defense/antimissile positions, and aviation force bases…Under special circumstances, [the Second Artillery] also can exploit the distinct superiority of missiles by using missile weapons to strike at the enemy's space network…and thus create the conditions for us to gain the strategic initiative and as rapidly as possible achieve the strategic goals."*

If the recommendations of the 2013 AMS and 2014 NDU texts are taken literally, and assumed to be reflective of current times, the same texts that advocated for dedicated DA-ASAT units also indicated that kinetic counterspace weapons should be commanded by a specialized space command at the central level. That could potentially mean that, during wartime, the new SSD, under the SSF, would potentially command another force's DA-ASAT missiles. That would mean that the DA-ASAT missiles would be operated by either another service's units, or SSF-badged personnel deployed with another service.

This hypothesis does hold water, as references to a dedicated ground-based space defense or ASAT unit have gradually disappeared, and are missing from the 2015, 2017, and 2020 PLA NDU SMSs. A gradual shift may have occurred in the PLA NDU 2015 text called Study on Asymmetric Operations, which outlined theoretical methods for conducting asymmetric operations. In that book, the authors explained that a general air force and a general missile force's asymmetric operations would include carrying out operations in their respective domains, as well as carrying out attacks against targets in space. In the author's explanation of a space force's asymmetric operations, it does not include ground-based space units conducting kinetic attacks on space.

The trend away from a dedicated DA-ASAT missile unit towards potentially multiple services maintaining the capability to deploy counterspace missiles, hypothetically commanded by a dedicated space command at the central level, persists in the 2015-2020 SMSs. The 2020 SMS no longer clearly indicates that the Rocket Force has DA-ASAT capable missiles, but instead clarifies that the PLA Air Force has exo-atmospheric BMD responsibilities, and that "strategic anti-air strikes have evolved from traditional air defense to a comprehensive combat operation combining air defense, space defense and anti-missile defense. The defense of various missiles

and space-based weapons has become an important part of strategic anti-air strikes."[vi] The 2020 SMS is probably referring to what it says is a new PLA Air Force mandate and the SSF when it states that, "space offensive and defensive capabilities mainly include: strategic early warning and surveillance capabilities, ballistic missile long-range precision strike capabilities, space-to-ground fire strikes, and counterspace defense capabilities." In the section on future capabilities, the SMS recommends the PLA Army should "vigorously develop surface-to-air missile units and anti-aircraft artillery units with medium and high-altitude protection capabilities…" "High-altitude" capabilities could indicate an ASAT capable missile, though this is speculative. The 2015-2020 SMS written by the PLA NDU seems to be maintaining what was stated most clearly in the 2013 SMS written by AMS, which stated that, "Within space defensive operations, the participating strengths not only include the space forces, but also include the correlated strengths of [other services]."

The last portion of this chapter attempts to answer the second question, "In what way will the PLA be directed to use DA-ASAT missiles?" For the last two decades, Chinese official media in Mandarin and PLA academy textbooks repeat that, DA-ASAT missiles are a necessary component of space deterrence. This intended use would also still require that the PLA train with DA-ASAT-capable missiles, as generally speaking, the strength of a deterrent must be linked to its operational effectiveness. This might mean that, in order for an adversary to view the weapon as a real threat, the mobile ASAT missiles and their support equipment need to be dispersed across China in secret locations, available for PLA targeting of adversary military satellites. As one of the few counterspace weapons potentially widely dispersed across the theater commands, but with usage being centrally controlled, it is important to attempt to understand how the CMC would decide to use the missiles as a deterrent.

Evidence of deterrence as the primary intent for DA-ASAT missiles is evident even from the timeframe of the PLA's destructive test in 2007. PLA academy books describe the significant negative spillovers of DA-ASAT missiles, which limits their operational usefulness. For example, the 2007 PLA NDU textbook called, A Study on the Space Information Support of Integrated Joint Operations, directly states that, "anti-satellite weapons primarily consist of four types, which are anti-satellite satellites, anti-satellite missiles, directed energy weapons, and kinetic energy weapons. The first two can only deal with satellites in low orbits, and they are a one-time use; thus, their costs are very high." Later, the AMS, in Lectures on the Science of Space Operations in 2013, explained that it is relatively easy and low cost for one side in a conflict to create space obstacles and debris for the opponent, however, the same obstacles then directly impact the Chinese side. It concludes that the PLA, "must analyze the space battlefield posture in an all-around and careful way, and as much as possible…avoid "self-blockade" or setting off an international dispute." The authors in 2013 seemed to think that the PLA could use an ASAT missile and only create debris in orbits in which the PLA did not have any spacecraft, which today, with the expansion of China's on-orbit systems, is an unlikely perspective for them to still maintain.

The PLA has historically used the co-location of strategic and conventional missiles as a type of deterrent, and they believe that the U.S. intertwines its defensive missile capabilities with

[vi] Regarding the Rocket Force the 2020 SMS states that "[the Rocket Force's] conventional missiles usually focus on attacking the enemy's important military targets. In a campaign, such targets are both strategic and operational, and they are large in number."

its offensive missile capabilities, so the PLA should as well. Towards this end, PLA commentators and official media often state that, "Direct-ascent anti-satellite weapons can be considered a special type of anti-ballistic missile." In another instance, PLA commentators stated that, "Because the targets are outside the atmosphere, direct-ascent anti-satellite missiles are inextricably linked to ballistic missile defense systems, in other words, weapons that can intercept ballistic missiles outside the atmosphere have anti-satellite capabilities to some extent." It is possible that the PLA would attempt to develop TELs capable of launching both DA-ASAT missiles and BMD missiles to confuse opponents.

Methods of ensuring a deterrent effect, but without debris, have been discussed in Chinese official media in Mandarin. In 2013, the People's Daily described ways to make the 2007 destructive DA-ASAT test continue to have deterrent effects, such as by making the missiles road-mobile and demonstrating higher orbit capabilities. Regarding the latter, Chinese media has often explained in Mandarin that higher orbit ASAT tests are the most capable of deterrence because, according to them, military satellites are at higher orbits. Even in 2019, in response to India's DA-ASAT test, a Chinese PLA media commentator stated that tests have to be above 800km in order to be of use against military satellites.

The clear-eyed concern about debris limiting the operational usefulness of DA-ASAT missiles has continued even after the creation of the SSF. The 2015, 2017, and 2020 SMSs each state that debris is an issue of concern for the PLA, and that China must be involved in the international debates on space debris. In 2020, the SMS stated that, "the existing international treaties and agreements on outer space … are unable to solve the problem of space pollution… How to deal with the ever-increasing amount of space garbage and debris, how to allocate its disposal costs among the relevant countries, and how to bear the relevant responsibilities will be a long-term dispute in the international community."

Of course, a deterrent must not only be technically and operationally believable, but the opponent must also believe that the CMC will approve the use of DA-ASAT missiles. The 2015, 2017, and 2020 SMSs state that space confrontation, to include ground-to-space and space-to-space attacks, would be "a limited method of achieving space control." It seems very reasonable to assume that the CMC would not approve wide-scale usage of DA-ASAT missiles, because they realize that using, even just one, can negatively impact their own satellite usage.

Chapter 3: Terrestrially-Based Satellite Electronic Jamming Weapons

SUMMARY

The PLA and western militaries divide electronic warfare (EW) operations into units covering technical reconnaissance, electronic attack, and countermeasure development. This chapter attempts to narrow in on one of these three areas, electronic attack, and only when it is specific to countering space systems, such as jamming satellite uplink and downlink. Based on this tailored scope, this report agrees with other analysts that the PLA Strategic Support Force (SSF) did not absorb all of the PLA's electronic and electromagnetic spectrum warfare capabilities, even for counterspace. With the approval of the Central Military Commission (CMC), theater Command (TC) commanders can still task subordinate non-SSF military services to operate electronic attack platforms in their joint air, maritime, and ground operations, including systems that can jam satellites and their users. A key takeaway is that the best examples of dedicated ground-based satellite uplink and downlink jamming capabilities are those operated by non-SSF units.[vii] The SSF, on the other hand, is the more dominant operator of experimental electronic jammers in space, as discussed in the separate Chapter called Space-Based Satellite Electronic Jamming Weapons.

Many western reports state that the SSF absorbed all of the "strategic" electronic and electromagnetic spectrum warfare capabilities, but this research could not find commentator agreement on what "strategic" electronic warfare (EW) means.[viii] The PLA itself may still be working on the distinction. As recent as 2018, a PLA published book indicated that they were still trying to better coordinate and leverage the electronic attack equipment of the services and the SSF for seizing electromagnetic dominance. Yet another possible way the PLA may distinguish between strategic and campaign or tactical EW is to consider the type of attack a SSF Network Systems Department (NSD) unit might conduct on space systems. Some new SSF NSD units might be more focused on spoofing satellite signals and radio frequency (RF) enabled cyber operations, rather than temporary, reversible jamming. As early as 2013, authoritative PLA texts have defined space related "information jamming" as "the application of cyber warfare and electronic warfare." PLA academy books' references to degrading satellite services by way of intrusion into an adversary's telemetry, tracking, and control (TT&C) ground stations is probably an example of the SSF's work towards RF enabled cyber operations, which could be in line with a strategic mission, rather than a tactical, terrestrially based satellite service jamming mission.

Regardless of the division of strategic, campaign, or tactical operations, all of the PLA's electronic attacks, including those on satellite uplink and downlink, will be coordinated through the Central Military Commission's (CMC's) Joint Operations Command Center (JOCC). Electromagnetic spectrum jamming, because it could be more prolific and potentially more

[vii] A future examination regarding if there are SSF badged personnel deployed with the TCs and services which operate this equipment is planned. Additionally, PRC national strategic infrastructure probably maintains electronic warfare countermeasure capabilities to ensure security of their operations, but this report only investigates dedicated attack functions focused on space systems and services.

[viii] An additional difference in the way western researchers and PLA researchers discuss counterspace command and control is in the PLA's inclusion of directed energy weapons as a type of electronic warfare weapon. See the Chapter titled Directed Energy Counterspace Weapons for more information.

impactful on civilian and bordering countries, does not seem to be delegated to the TCs like reversible directed energy weapons. This might include the operations of the SSF NSD's "network-electromagnetic spectrum countermeasure" units, which are also organizationally under the command of the CMC.[ix] Select examples of PLA Air Force, Navy, and Rocket Force units that likely maintain satellite jamming capabilities are included below, but only enough to make the case that even after the establishment of the SSF, the TCs at least for now, with CMC JOCC coordination, will command more than just SSF EW units.

Still, this chapter explores a few options for follow-up research. The SSF units discussed below may be spread across the Space Systems Department (SSD) and the NSD. Units 61764 and 61768 are included because western analysts have historically referenced them as the former General Staff Department (GSD) Electronic Countermeasures and Radar Department's (4PLA's) operational electronic warfare units focused on space. They continue to operate with the same unit number even after PLA reform, and their location in Hainan Province's (Island) southern Sanya City makes them likely capable of being in an operationally relevant satellite's footprint. Lastly, this report included new SSF Unit 32090, which absorbed the GSD's non-space focused EW units. Unit 32090 is referred to as a network-electronic countermeasure unit and maintains multiple locations around the PRC periphery such that they could rapidly deploy and be in an operationally relevant satellite's footprint.

Future studies which might look at terrestrially based satellite jamming and spoofing should make some key clarifications. First, future studies should be cautious in assuming electronic countermeasure functions are the same as electronic attack functions, and note that much of the electronic attack capabilities are for terrestrially based systems, even those operated by NSD units. Additionally, it should be noted that the PLA does not seem to maintain the same division between electronic warfare and directed energy counterspace weapons as western researchers. PLA academy texts regularly refer to more than just the radio frequency portion of the electromagnetic spectrum to include radio, microwave, ultraviolet, and visible light jamming weapons as those fielded to the EW troops. For more information, review this report's Chapter called Directed Energy Counterspace Weapons.

SELECT PLA UNITS THAT OPERATE TERRESTRIALLY-BASED SATELLITE JAMMING OR SPOOFING WEAPONS

This section attempts to answer the question, "Who in the PLA will use terrestrially-based electronic satellite jamming weapons?" Every PLA service operating under the five Theater Commands (TCs) has historically maintained and most likely still maintains dedicated tactical electronic warfare units whose functions are subdivided into technical reconnaissance, electronic attack, and electronic countermeasures. Some western researchers have argued that all technical reconnaissance functions have transferred to the Strategic Support Force (SSF) and that electronic attack and countermeasures are still spread across the SSF and other services. This report only investigated electronic attack and much of what those units are doing is unrelated to satellite

[ix] See the Chapter titled Offensive Cyber Counterspace Weapons for more information on the PLA's drive to move cyber operations down to support joint operations, not only strategic operations.

signals and unrelated to counterspace.[x] The below examples cover navigation satellite and communications satellite (SATCOM) downlink jamming and spoofing, with some evidence of SATCOM uplink jamming.

- The PLA Air Force as recent as 2021 wrote about techniques for jamming U.S. GPS, including the U.S. military signal.
- The PLA Navy wrote in 2018 on global navigation satellite system (GNSS) spoofing, but specifically on the topic of ensuring PLA satellite receivers can detect spoofing. Early technical articles from the PLA Navy indicate a capability for GPS jamming, which likely persists. A different PLA Navy unit wrote about satellite communication uplink jamming in 2018.
- A 2022 review of the PLA Rocket Force includes examples of units with satellite navigation downlink jamming capability for guided missiles.

This report judges that units 61764, 61768, and the new 32090 are the best candidates for SSF units which are also capable of, but not exclusively engaging in, terrestrially-based satellite uplink and downlink jamming. Notably, 61764 and 61768 may either be NSD or SSD, but Unit 32090 is more likely a NSD unit based on numbering conventions. They are all formerly General Staff Department (GSD) operational electronic countermeasures units (ECM units). It is important to remember that the pre-reform GSD's Electronic Countermeasures and Radar Department, also known as 4PLA, which housed the technical reconnaissance units never exclusively focused on space, and its contribution to space-related electronic warfare continues to probably be primarily in technical reconnaissance satellite data processing and analysis for the development of countermeasures against systems that are below the atmosphere.

Unit 61764 and Unit 61768 historically focused on the space segment and are both located in Hainan Island's southern city of Sanya. There is evidence that at least some units under the former 4PLA, in the past, deployed with Navy units throughout the South China Sea (SCS) islands, as evidenced in a GSD employee's diary entry about a 2013 deployment. That would be around the time the PRC was building islands and dredging underground facilities, which indicates early GSD involvement that was most likely aimed at ensuring integration with the secure military communications network, and potentially other objectives. This may support an argument that these units could operate some of the technical reconnaissance and possible satellite jamming capabilities, which western researchers have identified on the various SCS islands.

Of the two units, this report argues that Unit 61768's technical publications and onsite satellite dish radomes make it more likely capable of satellite jamming. While the radomes are probably for standard equipment protection, they also cover the direction and movement of the system from imagery. Unit 61768 transferred to the SSF as of at least 2022, based on a below author's affiliation. As of 2022, Unit 61768 was still using the same unit number. It also continues

[x] When they publish technical reports on counterspace, the reports are mostly related to developing countermeasures for when they are jammed or spoofed. A skeptical reader might argue that units would not publish on electronic attack or that "countermeasures" is a way to say "attack." This research did not focus on refuting that claim, but does provide evidence to the contrary.

to not exclusively focus on space, nor jamming space systems, and continues to be involved in ingesting technical reconnaissance data from satellites. Examples that justify its inclusion are:

- In 2019, Unit 61768 wrote about attack methods and countermeasures for intentional interference in satellite remote sensing ground stations, primarily focused on securing its own systems.
- In 2020, Unit 61768 published on best practices in jamming SATCOM downlink, emphasizing that technical reconnaissance and other intelligence are needed to know the details of the adversary's communications frequency, and that the angle of the antenna is very important for carrying out deceptive jamming.

Unit 61764 also has visible onsite satellite dishes, but in publicly available imagery, they regularly face towards equatorial GEO satellites, indicating that the unit may be using the antennas for data uplink and downlink, not jamming. Unit 61764 also continues to support joint operations from Sanya City with the same unit number, even though after 2017, it transferred from the CMC's Joint Staff Department (JSD) to the SSF. In the early 2000s, Unit 61764 certainly played a role in developing the PLA's capabilities to jam and spoof U.S. GPS, based on their early technical studies. However, they seem to be focused more on technical reconnaissance and designing countermeasures, with only minimal references to jamming.

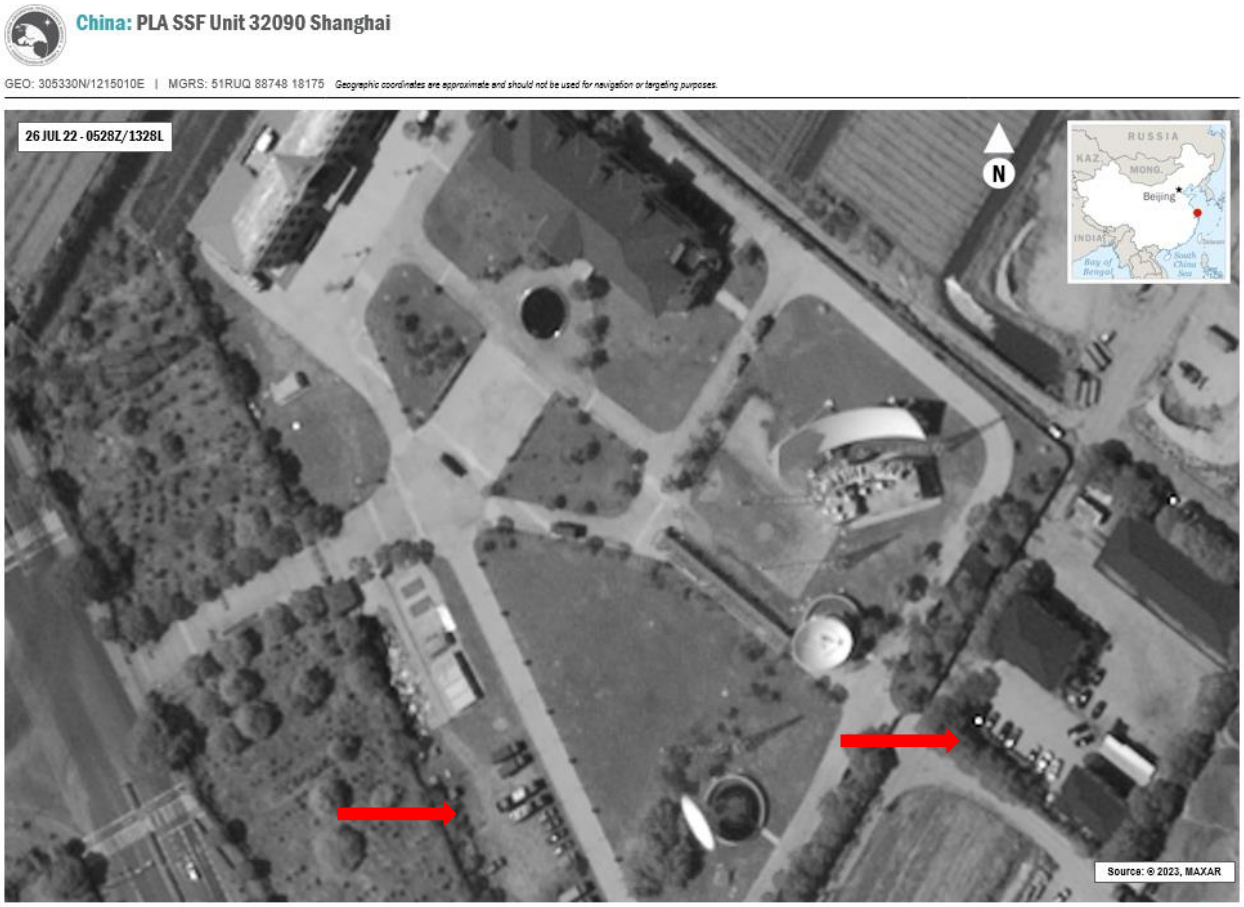
They more recently have written on efforts to make the PLA's technical reconnaissance data, which according to them has traditionally been considered "strategic," and too slow to support tactical operations, more quickly accessible to PLA services in wartime. This type of higher-level analysis would probably supplement the technical intelligence a non-SSF tactical unit gathers from its location in the battlefield. Better integrated electronic intelligence information would help the services in several ways, including optimizing their use of satellite jamming equipment for campaign, not just tactical effects.

Last, new SSF NSD Unit 32090 is the new unit number for another former GSD ECM Unit 61906, according to an official Chinese legal document. Unit 32090 may also have absorbed Unit 61521 because both were former GSD operational ECM units not focused on space, and Unit 32090 now has a location in Qinhuangdao, Hubei Province and Shanghai like the former 61521. Unit 32090 is referred to as a "network-electronic" countermeasure unit.

Western researchers have historically identified Unit 61906 and Unit 61521 with counter-air operations. While Unit 32090's technical papers are primarily about countering terrestrial radar and enabling network information operations, this report includes Unit 32090 because of its known participation in joint PLA exercises that consist of a space electromagnetic confrontation element, and also because of the unit's proliferation of identified truck-mounted antennas located around China's periphery, the capabilities of which require more analysis.

Unit 32090 has published reports self-identifying as a unit in Beijing and Qinhuangdao

Hubei Province; and government purchasing bids indicate they are also operating out of facilities in Jiangxi Province, Shanghai, Jiangsu Province, southern Hainan Island, and eastern Tibet, to name a few. Their dispersion around the border with mobile antenna trucks means that if those antennas are capable of satellite uplink and downlink jamming, they could be capable of moving into an operationally relevant satellite's footprint. After all, the PLA National Defense University's (NDU) Science of Military Strategy (SMS) in 2020 stated that, "Among the support-type forces, the early warning command aircraft and electronic jammers are the most important, and they must not only have a certain [quantity], but also have a considerable level of quality." Since there are so many 32090 locations with a similar type of truck, this research urges experts with an understanding of ground-based satellite jamming systems to perform more unclassified imagery analysis.



The examples of prior Unit 61906 and current Unit 32090 writing on satellite jamming include:

- Unit 61906 in 2010 coauthored a study on U.S. spatial information countermeasures, which included references to the now U.S. Space Force's Counter Communications System, which has been operational since 2004.

- Unit 32090 in 2018 authored a review of malicious SATCOM uplink jamming mitigation techniques to improve the security of the Chinese SATCOM system.
- Unit 32090 also in 2018 designed a GPS-reliant system to test their countermeasure equipment, which is not too surprising since the Chinese Beidou system reached global coverage only in mid-2020. More technical expertise is needed to understand if the countermeasure system was actually for jamming GPS.
- Unit 32090 in 2021 authored an analysis of presumably a foreign country's communications frequency hopping signals in order to analyze windows within hops for interference, though no specific reference to type, like SATCOM or terrestrial radio, was included.

This report's uncertainty regarding if the SSF's units capable of ground-based satellite electronic jamming are NSD or SSD is also based on evidence of a prior General Armaments Department (GAD) role. The earliest example of a military technical report on terrestrially-based synthetic aperture radar (SAR) satellite spoofing is from the former GAD out of its headquarters in Beijing in 2010. SAR uses the microwave frequency, which as discussed in the Chapter called Directed Energy Counterspace Weapons, could be considered by the PLA to be a high-power microwave weapon. A separate former GAD Unit 63888, in 2007, wrote that while they had the

capability to jam SATCOM downlink, it would be better to develop the power capacity for uplink jamming. Unit 63888, previously under the GAD Base 33 in Luoyang City, Henan Province has transferred to the SSF. Base 33 is a test and training base. Additional former GAD units such as Unit 63618 also continue to work on jamming of terrestrially based systems. GAD's contribution is probably in system development and testing, which is different from the GSD's historical role in fielding equipment to the joint forces and maintaining some operational units.

HYPOTHESIS OF PLA COMMAND AND CONTROL (C2) FOR TERRESTRIALLY-BASED SATELLITE ELECTRONIC JAMMING WEAPONS

In an attempt to bring more fidelity to China's counterspace C2, this section will attempt to answer two questions. First, "What is the most likely chain of command for the PLA to decide when to use terrestrially-based electronic satellite uplink and downlink jamming weapons?" This first question relates to the above section, which attempts to answer, "Who in the PLA will use them?" The second question in this section is, "In what way will the PLA be directed to use terrestrially-based electronic satellite uplink and downlink jamming weapons?"

The Central Military Commission (CMC) has two mechanisms for directing and coordinating plans for units that operate terrestrially-based electronic jamming weapons, only a small portion of which are focused on jamming satellite uplink and downlink. First, the CMC Joint Staff Department's (JSD's) Information and Communications Department probably continues to house the management functions for technical reconnaissance, electronic warfare, and electronic countermeasures previously under the GSD's Fourth Department (4PLA).[xi] This research agrees with earlier western assessments that the JSD's many roles probably includes establishing electronic warfare doctrine and deconflicting theater-level electronic warfare operations, to include satellite jamming, through the Joint Operations Command Center (JOCC). The deconfliction of jamming operations is highly likely enabled by the Information and Communication Department's spectrum management brigade which operates at the central and theater levels. Second, the CMC can direct the SSF's electronic warfare units, which are probably capable of satellite jamming and spoofing, to carry out different tactics. Terrestrially-based EW weapons can potentially be used to spoof satellite uplink and downlink signals to enable a cyber intrusion, also known as "RF enabled cyber," or in PLA parlance "network-electromagnetic spectrum" warfare.

The last portion of this chapter attempts to answer the second question: "In what way will the PLA be directed to use terrestrially-based electronic satellite uplink and downlink jamming weapons?" Towards that end, the below section describes PLA academy writings regarding usage in two different contexts. One context, which is most analogous to a Taiwan scenario off the PRC coast, would leverage wide usage of various types of satellite uplink and downlink jamming in line with a centrally pre-approved and deconflicted plan. A second context, one where the PRC seeks

[xi] This research could not find what other authors have referred to as a separate Network-Electronic Bureau, 网络电子局), or Network-Electronic Countermeasures dadui (网电对抗大队) under the JSD, except for an example from early after PLA reform. According to a university website, the Director and Deputy Director hosted a lecture on cyberspace and international law in late 2016, but other western reports' references are no longer accessible. (See: 武汉大学, "黄志雄教授为军队有关部门讲授网络空间国际法," 11/2016, http://web.archive.org/web/20210508092052/https://fxy.whu.edu.cn/info/1052/3061.htm)

early deterrence of the U.S.'s ability to enter a conflict, is more strategic and would rely on probably PLA special force's remote access into a U.S. or partner's space telemetry, tracking, and control (TT&C) facility to degrade or disable key systems.

In a PRC regional battle, satellite uplink and downlink jamming are both expected. The PRC's coastal and island equipment increase the likelihood that the PLA can deploy equipment with enough power in the footprint of an adversary's operationally useful satellite for uplink jamming. In particular, a battle off the PRC's coast enables ground, sea, and air-based SATCOM uplink jamming, assuming the PLA has all the technical information on adversary equipment and signals. It should be noted, however, that many of these satellites are presently in geostationary Earth orbit. The PLA's 2018 Mechanisms for Gaining Victory with Electronic Confrontation text states that, "Carrying out a focused electromagnetic attack against communications satellites, [communications] relay vehicles, and other nodes in this kind of communications network can optimize attacks in a highly effective manner against individual targets [and have] destructive results against the overall continuity of the enemy communications network." The 2020 NDU Science of Military Strategy acknowledges that the PLA will "use… satellite communication jamming forces to interfere with enemy communication satellites and maritime satellites."

Satellite downlink jamming, particularly of GNSS, but also SATCOM user terminals, will be the more prolific in a PRC regional battle, but will still require the jamming equipment to have line of site of the end-user's antenna. The PLA's 2018 Mechanisms for Gaining Victory with Electronic Confrontation text states, "airborne and satellite-borne electronic confrontation platforms have gradually become what electronic confrontation strengths mainly rely on." This is probably referring to the PLA Air Force's aircraft and unmanned aerial vehicles (UAVs) capable of at least satellite downlink jamming.[xii] The 2015 PLA book called A Study on Asymmetric Operations stated that, "the [PLA] Air Force [has] become one of the services whose level of informationization is highest; the emergence of electronic warfare aircraft, high-powered microwave weapons, and other new types of equipment has provided vigorous means for the Air Force to extend its own combat tentacles into network and electromagnetic spaces."

The PLA wants electronic attacks, including those to jam satellites, to be coordinated through the CMC. The 2014 PLA NDU Space Information Assisting-Support Operations book described that the PLA in an anti-air raid scenario will employ GPS jammers to interfere with adversary precision-guided missiles. The authors noted, however, that even this type of activity needs to be coordinated, probably through the JSD, to ensure the PLA's own use of GNSS is not disrupted. They call this phenomenon a "self-blockade." The need for coordination of jamming units is reiterated in a 2018 text which says, "electronic confrontation strengths are subordinate to joint operations strengths and the goals of electronic confrontation serve the goals of joint campaigns or combats." The PLA also widely acknowledges that while satellite jamming can support tactical and campaign level goals, it also must be used selectively because, "the electronic air defense strengths themselves may come under enemy positioning and attack because of emitting high-powered jamming signals."

In addition to coordinating satellite jamming to ensure the most tactical, campaign, and strategic positive spillovers, PLA texts also recommend that the best way to use jamming to deter

[xii] The satellite-borne electronic confrontation strengths are SSF units and discussed in the Chapter titled Space-Based Satellite Electronic Jamming Weapons.

an enemy is by the integration of electronic and cyber warfare. The 2013 Academy of Military Science's Lectures on the Science of Space Operations describes one such deterring operation as disabling an enemy's space TT&C bases or launch centers. It says, "information jamming means the application of cyber warfare and electronic warfare to sabotage the enemy space base's C2 net, and suppress and jam the enemy space measurement and control signals, so that the enemy space base cannot effectively fulfill its launch missions." The authors go on to say that, "by conducting electronic jamming of the enemy space system's space TT&C and command systems, [we can] render the enemy spacecraft unable to provide effective information assisting support for operational activities on the land, sea, and air battlefields." The 2018 Mechanisms for Gaining Victory with Electronic Confrontation book reiterates that to create early momentum in attempts to constrain the enemy, "cautionary electromagnetic attack" on "targets such as enemy communications hubs, large-scale power facilities, or important satellites" must be strictly controlled. The authors emphasize, "the issue of controlling the extent of the cautionary electromagnetic attack is crucially important," the reasons for which they describe are avoiding a self-blockade and ensuring the intended strategic impact, which they say is like "making the point without going into the details."

Depending on the means of carrying out an electronic warfare attack, the CMC may prefer the TCs and the SSF to operate in tandem or alone, to include even PLA special operations units going behind enemy lines. The 2015 PLA Study on Asymmetric Operations says:

> *"It is necessary to primarily have noncontact operations and to dare to carry out contact operations against the enemy. In systems of informationized warfare, there are large numbers of information network nodes … and these are broadly dispersed; moreover, the enemy does not have enough combat strengths and his defense strengths are weak. Special units are most suited to undertaking the task of sabotaging fragile node targets in the enemy's system of operations. Special operations units can… secretly infiltrate the enemy's depths; carry out precision reconnaissance, positioning, evaluation, and sabotage; and coordinate with the main forces in achieving the goal of attacking and destroying the enemy's system of operations in multiple areas."*

Chapter 4: Offensive Cyber Counterspace Weapons

SUMMARY

The below chapter attempts to highlight the publicly known Chinese cyber actors in the People's Liberation Army (PLA), which have included U.S.G., foreign partner, or defense contractor space systems in their attacks, with an eye toward understanding the PLA's potential for offensive cyber counterspace weapons. Cyber security experts frequently remind us that it is easy to spoof the origin of an attack, making attribution to a specific country, let alone a certain actor, very difficult. Other complications in conducting this type of analysis include the fact that the PLA is just one of many cyber actors in China empowered to exploit foreign information networks. The most up-to-date western research emphasizes that even PLA published books state that the Strategic Support Force (SSF) will not be the only PLA actor conducting cyber operations, and the coordination between the various PLA actors, as well as between the PLA and the civil cyber agencies, is still unclear.

This report includes two groups of cyber actors, and used two different methods to find them. Across both groups, there are five PLA units this research recommends for further analysis: units 61486, 75770, 32082, 92762, and 91746. The first group includes units 61486, 75770, and 32082. They have gained access to space systems information from cyber intrusions, or displayed a depth of space technical expertise by publishing related technical reports, and simultaneously, also wrote about cyberattack tools, like malware development. These units are included based on historical research on cyber intrusions in the space sector and other analysis. The second group includes Unit 92762 and Unit 91746. These two units are included based on research into cyber security reports that provided sectoral breakdowns of previously hacked companies. Well known Advanced Persistent Threats (APTs) in the cyber security sector are sometimes thought to be PLA groups originating from a certain province or region. This report attempts to provide more information on the possible PLA unit, while noting that researchers have not confirmed the PLA as the referenced APT. This chapter includes the second group to spur deeper cross-sectoral collaboration among researchers traditionally siloed in the PLA or cyber security expert community.[xiii]

Regarding the first group, Unit 61486 is the former General Staff Department (GSD) Technical Department's Twelfth Bureau, which historically supported the Technical Department's, also called the 3PLA's, communications intelligence (COMINT) mission. Unit 61486 supported by intercepting signals to and from communications satellites, probably with ground and space-based capabilities. Unit 75770 is the former Guangzhou Military Region (MR) Technical Reconnaissance Bureau (TRB). All of these units are confirmed to have transferred to the SSF.

Also in the first group is the new SSF Unit 32082 in Beijing, which is likely subordinate to also new Unit 32081. These two units deserve much more research; while Unit 32082 is discussed below as potentially having an offensive cyber counterspace weapon capability, its co-

[xiii] Apart from these, there are many other units included below which might be candidates for a counterspace cyber capability if merged with proprietary or classified data, like Unit 61398. Unit 61398 included U.S. and Danish communications satellite companies in its intrusions, but as far as this research could tell, the unit was more focused on intelligence gathering rather than counterspace attack tools.

located and probable parent organization, Unit 32081, is called an Information Technology Unit of the SSF. Units affiliated with the Network Systems Department (NSD) are often described as such, i.e. as NSD units, and the NSD is often considered the home for cyberattack units. With that in mind, Unit 32081 could instead focus on diagnosing space cyberattacks, which could also end up being a better description for Unit 32082.

Regarding the second group, this chapter includes Unit 92762 in Fujian Province and Unit 91746 in Beijing based on cyber security reports on Anchor Panda and APT14. Both are former PLA Navy TRBs. Unit 92762 has transferred to the SSF, but Unit 91746's status was still in question at the time of writing.

As early as 2013, PLA textbooks have specified two types of counterspace cyberattacks that the authors anticipate the PLA should be able to execute. One type is tactical, and the other type is strategic. These types of cyberattacks have been reiterated in the PLA's more recent literature, though in less detail. The first means of attack is something the U.S. calls "electronic warfare and cyber convergence," or in PLA parlance, "network-electromagnetic spectrum" attacks, which most likely can be conducted against ground-based and space-based space systems. These types of attacks would be executed by two different types of PLA units, as discussed in this report's Chapter titled Terrestrially-Based Satellite Electronic Jamming Weapons and also in the Chapter titled Space-Based Satellite Electronic Jamming Weapons. Network-electromagnetic spectrum cyberattacks on space system users is probably a PLA Theater Command (TC)-controlled weapon when used for limited in-theater effects. When used for strategic effects, this attack method would be centrally controlled by the Central Military Commission (CMC). The second type of counterspace cyberattack that the PLA anticipates it should be able to execute is a covert operation to implant computer malware on adversary space information systems by means of remote entry, or direct entry, with special operations forces. This would be a CMC directed operation.

While the PLA may have some clarity on the types of counterspace cyber operations it should be prepared to execute, PLA research has also indicated that regulations and procedures are still needed to clarify how and when those weapons should be used to support joint operations. To that end, the PLA published studies in 2018 and 2020 on systems designed to evaluate cyber offensive and defensive trainings, and commanders' responses, indicating that the formalization of offensive cyber operations at large is still a work in progress. More importantly, none of the above-mentioned units were from the former GSD's Electronic Countermeasures and Radar Department, also known as 4PLA, which historically was in charge of electronic and network offensive attack. The new SSF commander, formerly the NSD commander, General Ju Qiansheng, has spent most of his time on the espionage side of the house in 3PLA, not the attack side in 4PLA, the implications of which are not yet understood.

A REVIEW OF PLA CYBER ACTORS

It is important to note that, at least according to unclassified information, many of the largest intrusions into U.S. systems were led by the People's Republic of China's (PRC's) civilian intelligence agency, the Chinese Ministry of State Security (MSS), such as the Hafnium group's attack on Microsoft Exchange email servers. Even actors that regularly targeted the aerospace industry have been MSS affiliated, such as the Advanced Persistent Threat (APT) 10. Furthermore, some of China's early intrusions into the National Aeronautics and Space Administration (NASA) and the U.S. Department of Defense systems in the early 2000s, volumes of information from

which are probably still very valuable, and which were only slowly ingested and understood by the Chinese, may well have been carried out by neither the MSS nor the PLA.

When attempting to focus only on PLA cyber actors which have at some time gained access to space related information, it also necessary to distinguish between the various types of PLA cyber actors, especially as it is now commonly assumed that strategic cyber activities are centralized under the SSF. The lion's share of cyber activities out of the PLA have been focused on traditional intelligence collection, and sometimes industrial espionage, with an often unclear distinction between the two. The PLA's former General Staff Department's (GSD's) Technical Department, also known as 3PLA, and its regionally based technical reconnaissance bureaus (TRBs), which together have a large staff of translators, have historically managed communications intelligence (COMINT) to include that gathered by cyber intrusions. According to Western analysts, the 3PLA's units have transferred to the SSF.

In addition to the 3PLA, and its focus on intelligence gathering, other PLA organizations have also historically had an intelligence gathering role, as well as a responsibility for countermeasures development and attack. For example, the former PLA Military Regions (MRs) and service specific TRBs have similarly conducted cyber-enabled intelligence collection and industrial espionage. Another GSD organization, the Electronic Countermeasures and Radar Department, also known as 4PLA, has historically managed other types of signals intelligence and technical reconnaissance, such as radar signatures analysis, in order to develop countermeasures. Regarding these non-3PLA units, western analysts have written that the 4PLA units have probably transferred to the SSF, while not all PLA service TRBs have transferred, at least not yet. This research can confirm that not all service TRBs have transferred to the SSF.

Important to this report's focus on cyber counterspace weapons, western analysts have also argued that the 4PLA was in charge of electronic attack and may also have had some role in network, i.e. cyber, attack training. Other researchers have argued that the historical separation of espionage and offensive elements between the 3PLA and 4PLA was a problem that the establishment of the SSF would correct. One might assume that the organization historically associated with offensive attack capabilities would be a major source of PLA cyber intrusions into the U.S. DoD and defense contractors. However, there is only one example of a former 4PLA subordinate group, the 54th Research Institute, being indicted for hacking, and in this case, they seem to have been focused on traditional intelligence gathering; they hacked Equifax. This leads to some important questions for our assumptions about the PLA's use of cyber in a counterspace context.

PLA UNITS WITH PROBABLE ACCESS TO U.S. AND PARTNER SPACE SYSTEMS

The next several subsections attempt to answer the question, "Who in the PLA will use offensive cyber capabilities?" These subsections include all available information at the time of writing to support future research. It also includes an initial hypothesized framework for identifying new SSF units working on offensive cyber counterspace weapons. The examples are included in chronological order of their likely intrusions as a way to help identify the types of government or industry space information to which they may have had access. Again, the reader should especially note units 61486, 75770, and 32082, but the entire chronology is worth recounting.

Cyber security experts mark the 2003-2006 Titan Rain intrusions as one of the earliest publicly known Chinese cyberattacks that gained access to space related U.S. and foreign government-controlled and contractor-proprietary information and systems.[xiv] In 2009, technical experts provided testimony that, "The attacks were believed to be Chinese in origin, although their precise nature (i.e., state-sponsored espionage, corporate espionage, or random hacker attacks) remain[ed] uncertain." Even two decades later, cyber security experts and western PLA researchers have traced multiple different groups to Titan Rain, including non-PLA and non-PRC government affiliated actors. The below PLA units are the most often referenced as being involved in Titan Rain. This research finds that only two of the three, Unit 75770 and Unit 61398, have later publications indicating a space interest. All three are discussed below for reference.

Unit 75770 is the former Guangzhou MR Technical Reconnaissance Bureau (TRB) which in addition to being headquartered in Guangdong Province, oversaw at least eight offices, three of which were in Guangdong Province. This location is significant for tracking Titan Rain because affiliated hackers used a computer server there. As of 2022, Unit 75770 has transferred to the SSF and is still using the same unit number, based on a recruitment ad looking for international relations-savvy graduates, who have some network security understanding, indicating they are at least focused on cyber-enabled intelligence collection and analysis. In 2002, they authored a report making suggestions on how to manage increasing congestion resulting from network applications, indicating a concern with dropping data packets. While speculative, this could potentially be a result of their efforts to download volumes of data accessed via a cyber hack. Conversely, it could be related to China's eventual establishment of its national firewall to block foreign websites.

However, Unit 75770 has demonstrated a space interest, particularly regarding an understanding of NASA's ground systems. In 2015, together with the China Electronics Technology Group Corporation (CETC) and Xi'an Satellite Tracking and Control Center, i.e. SSF Base 26, they wrote about NASA's early 2000s research on uplink radio antenna array technology for the Deep Space Network, and made proposals on how China should implement a system for itself. While it is speculative, a paper in 2015 from this unit, referencing NASA's research from the early 2000s, might be leveraging Titan Rain's data exfiltration, which with such volume could have taken several years to digest and make technically relevant.

Unit 78006 is the former Chengdu MR 1st TRB, and as of 2021, was still active and using the same unit number. As of late 2020, they were building new facilities in Sichuan Province's Chengdu City, Tianfu New Area, and there was no indication that they had transferred to the SSF. There are also no indications in the unit's technical publications of an interest in space, despite Sichuan Province being home to the Xichang Satellite Launch Base, SSF Base 27. Unit 78006's publications indicate they are at least responsible for investigating cyber intrusions into PLA and

[xiv] According to a RAND study, which also included interviews with U.S. officials, the Titan Rain actors accessed unclassified information across many organizations, including the U.S. Department of Defense, NASA, U.S. Army Space and Strategic Command, U.S. Army Aviation and Missile Command, and various defense contractors, probably at least including Lockheed Martin. The 2003-2006 timeframe also would include the Marshall, Kennedy, and Goddard Space Flight Centers' intrusions, from which likely Chinese actors gained rocket engine and launch vehicle management intelligence, which could potentially help them understand vulnerabilities to delay launches. It is most likely they were collecting information to support the maturation of the Chinese space program.

PLA contractor systems; they investigated a 2017 HTTPS trojan intrusion into Tsinghua University.

In 2003, consistent with the timeframe of the Titan Rain attacks, Unit 78006 authored a report lamenting that PRC research organizations were struggling to control confidential information, as a result of the PRC having entered the World Trade Organization in 2001. In the same article, they noted that the 1999 "U.S.-led NATO bombing of the PRC Embassy in Yugoslavia," was a good reason, in their opinion, why Chinese science and technology experts should be more cautious sharing PRC information with western contacts. This example might be a reason to think Unit 78006 was potentially involved in supporting groups involved in Titan Rain, but there are no indications of a counterspace cyber focus.

3PLA Second Bureau Unit 61398, also known as Shady Rat, or Advanced Persistent Threat 1 (APT1) in most public reports, is reported to have been active starting in 2006, which is after Titan Rain. However, based on the often loose network of affiliated hackers in the early 2000s, some researchers argue that a few of the hackers were linked to both groups.[xv] Unit 61398 also intruded into U.S. and foreign companies in the space sector, and has been attributed to cyber industrial espionage, so this chapter covers Unit 61398 as a separate case below.

The U.S. Department of Justice's (DoJ's) 2014 indictment of three members of the 3PLA Second Bureau Unit 61398 named a few compromised companies from the 2006-2014 timeframe. The indictment did not name any of the aerospace companies targeted by Unit 61398, but cyber security experts at McAfee revealed in 2011 at least two, both in the satellite communications sector. According to McAfee, the intrusion into the Danish satellite communications company began in August of 2008 and lasted six months; the intrusion into the U.S. satellite communications company began in February 2009 and lasted twenty-five months. McAfee's assessment was based on the company's employees having gained access to one of the command and control servers used by the attackers. These two satellite communications companies are the most obvious space related targets, but McAfee also referenced an additional 13 defense contractors, and 22 U.S. and foreign government agencies included in the total of 72 victims, the attack logs for which they found on the above referenced server.

This report hypothesizes that Unit 61398 was absorbed by the SSF's NSD Headquarters, known as Unit 32069. Unit 61398's activities and publications dried up after 2016, but a confirmed researcher with Unit 61398, as of 2018, was photographed wearing a SSF uniform, indicating at least some members of the unit transferred to the SSF. Unit 61398 and many other, but not all, former 3PLA bureaus may have merged under the new NSD Headquarters, based on it sharing the same address as the former 3PLA Headquarters, which went by Unit 61195. As of November 2022, the NSD Headquarters logistics department was recruiting Masters and PhDs in mathematics, computer, information security, communication, and networking for jobs in Beijing, Shanghai, Guangzhou, Chengdu, Qingdao, Wuhan, Fuzhou, Kunming, and other large cities, some of which are locations shared with former 3PLA bureaus.

[xv] Each of the cited reports are quoting cyber security expert Thomas Rid's tweet which has since been taken down. The cached version only includes the title which says that the U.S. National Security Agency attributed Titan Rain to 3PLA in 2007, without reference to a specific unit. This report could not confirm why others indicated Titan Rain was "partially the work of PLA Unit 61398."

In 2015, together with PLA Air Force Unit 95839 in Fujian Province, Unit 61398 wrote about a new algorithm for multi-band spectrum sensing to identify unknown users and find available spectrum, which could be about deconflicting their respective spectrum usage, or could be about identifying targets for intelligence gathering.[xvi] Technical signatures of radar, if focused on foreign signals, would typically have been the work of the 4PLA, so this report hypothesizes they are deconflicting domestic spectrum usage. While speculative, this 2015 paper might be related to something for satellite communications, using information exfiltrated from the U.S. or Danish companies, but the paper refers to microwave signals, which could just as easily be about cellphone signals.

Unit 61419 is the Third Bureau of the former 3PLA, based in Qingdao City, Shandong Province, and may have worked with a MSS group, which cyber security experts have named Tick and Stalker Panda that has been active since at least 2006. According to the Japanese Ministry of Justice, Japanese police authorities have an arrest warrant for a former Chinese international student, who was influenced by the wife of a Unit 61419 member. A Japanese news outlet stated that the connection was discovered during an investigation into cyber intrusions into multiple Japanese organizations, including the Japanese Aerospace Exploration Agency (JAXA). As of 2020, JAXA had been breached at least three times since 2012, resulting in the exfiltration of information on Japanese launch vehicles and two of their system contributions to the International Space Station, the Kibo experimental module and the Kounotori/HTV resupply vehicle. The latest attack compromised a JAXA server which stored the ID and passwords of four other servers. The Chinese national's attempt to purchase a controlled antivirus system seems linked to Unit 61419's broader efforts to buy foreign, English language antivirus software, as revealed in a 2021 report.

In 2006, Unit 61419, CETC, and Sichuan University wrote about problems with Very Small Aperture Terminals (VSAT) for SATCOM, and made proposals to improve frequency drift, probably to ensure their own secure communications. However, as early as 2014, western cyber security experts have been urging companies to improve VSAT terminals' security, and the U.S. National Security Agency in May 2022 repeated this warning.

Unit 61486, also known as Putter Panda, has been targeting the space and telecommunications industries since at least 2007, based on cyber security firm CrowdStrike's 2014 investigation. European aerospace companies in the satellite and remote sensing sectors were of particular focus. The CrowdStrike report concluded that the "strategic objectives for this unit are likely to include obtaining intellectual property and industrial secrets relating to defense technology, particularly those to help enable the unit's suspected mission to conduct space surveillance, remote sensing, and interception of satellite communications."

Indeed, Unit 61486 is the unit number for the 3PLA Twelfth Bureau, which historically supported the 3PLA COMINT mission through intercepting signals from communications satellites, probably with ground and space-based capabilities. Space-based interception of COMINT has been considered as early as 1959 in the U.S., so this research assumes it is a capability under development, or currently deployed by the PLA. It may be the one area of peacetime COMINT collection that is not coordinated through the MSS. Contrary to CrowdStrike's hypothesis, other entities in the PLA are responsible for space surveillance and

[xvi] PLA Air Force Unit 95839 could be the unit number for the PLA Air Force's Second Technical Reconnaissance Bureau (TRB), as the First TRB unit number is 95830.

remote sensing, but Unit 61486's related intelligence collection probably supports those other units in their systems development, and with analysis of foreign space technology developments. As of 2021, the group had not changed its unit number, so based on this report's working hypothesis, they may not yet be, or may never be, included under the NSD Headquarters. It is possible that Unit 61486 may be reorganized under the SSF Space Systems Department (SSD) instead.

Unit 61486 with Shanghai University in 2003 submitted an article discussing how to trace the identity of denial of service (DoS) attacks, noting that such attacks could be used to bankrupt an institution or gain the information advantage to avoid a war. The authors made recommendations for Chinese network administrators, who they say at the time could not detect and trace DoS attacks, by explaining an international IP address tracking scheme introduced in a 1997 translation of Andrew Tanenlmum's work on computer networks.

Unit 61486 with Nanjing University in 2004 wrote about how to rediscover foreign satellites after a maneuver, with particular interest in understanding those satellites' response time in an "emergency." The report indicated that they used "intelligence information" to confirm that coplanar satellites followed some basic physics principles and could be rediscovered in most cases by applying said principles, without the need to again gather intelligence information in order to rediscover the satellites.

In 2006, Unit 61486 authored a report arguing that, while there was a trend towards adopting spread spectrum for VSAT satellite communications and electronic intelligence satellites, China should be cautious in quickly adopting this method. The reasons the author provided were that first, China had spent a lot of time and money in establishing its unified S-Band telemetry, tracking and control (TT&C) systems, which met most of their needs. Second, the most important systems to first adopt spread spectrum should be electronic intelligence satellites, which would increasingly carry more sensitive payloads and need more bandwidth to support a modern information war. Lastly, the author provided an initial analysis of how spread spectrum could still be interfered with and noted that those weaknesses must be considered in tandem with system development.

In 2009, Unit 61486 reviewed the U.S. military's doctrine and technology development for space information countermeasures, noting that ground-based and space-based space situational awareness (SSA) capabilities were the first step to having such countermeasure capabilities. After reviewing the U.S. system, the author made several recommendations for the PLA. First, the author recommended that the PLA gain a better understanding on space information warfare theory and focus on reducing cost. Second, they should develop several confrontation weapons as soon as possible, at a relatively small cost, and grasp the weak links of the opponent in order to attack its key points. Last, focus on offensive weapons and miniaturization, stating "offense is the best defense." They do not make any recommendation on cyber weapons, and are likely only responding to information they exfiltrated.

Lastly, in 2010, Unit 61486 together with Unit 61148 in Guangzhou City of Guangdong Province, and the Information Engineering University in Henan Province, which is now a part of the SSF, determined that the best way to resolve discoloration in black and white satellite imagery was to enable better identification and cataloging. Unit 61148 might be the Guangzhou location of the 3PLA's Twelfth Bureau.

NEW PLA SSF UNITS RESEARCHING MALICIOUS CODE AND SPACE SYSTEMS

One of the key challenges in identifying new SSF unit numbers that have an offensive cyber capability, is that there appears to be no available analysis on the logic of former 3PLA, i.e. intelligence collection, and former 4PLA, i.e. electronic and network collection and countermeasures, unit numbers. For example, 61768 and 61764 were 4PLA, but above and below those numbers are 3PLA units like 61726, 61785, 61786, and 61716. This makes it difficult to know, even when researchers can find a new and old unit number affiliation, if it came from 3PLA or 4PLA.

Another key challenge is that, while there is uncertainty about the reorganization of existing PLA units that had worked on offensive cyber, there is also a growth of new units to support PLA network security and defense. What is known, however, is that the overarching new block of SSF unit numbers is 32001-32099. The Space Systems Department (SSD) stops around 32040 and the NSD Headquarters starts at 32069. Towards identifying offensive counterspace cyber units, this section attempts to decipher between old network offensive and new network defense units. This report hypothesizes that the block between 32050 to 32069 is most likely new cyber units somehow supporting network security and defense.[xvii] This research further hypothesizes that the units after 32069 are cyber units that support the electronic warfare and radiofrequency enabled malware units. In other words, the latter block of units that work on cyber issues are more likely related to offensive cyber operations, not just intelligence collection.

Based on this very generalized working notion, which will benefit from additional updates and analysis, this report found one unit that had work consistent with offensive cyber and general space issues, SSF Unit 32082. This Unit, based in Beijing, is likely affiliated with co-located Unit 32081, with more information available on the latter. In recruitment notices, Unit 32081 is interestingly referred to as an Information Technology Unit of the SSF, not a NSD unit. In another example, Unit 32081 was referred to as having a logistics department and a security department. Unit 32082 and Unit 32081 are co-located with the former GSD 3PLA's Fifth Bureau, which historically focused on Russia. The former GSD 3PLA's Fifth Bureau was called Unit 61565, and they are still using this number as of 2022. Unit 32081 is also either collocated with, or has absorbed, a former 3PLA Beijing MR TRB also focused on Russia, the unit number for which was 66407, based on a 2018 Chinese domestic legal document identifying Unit 32081 as the new identifier for Unit 66407, even though the latter was still in use as of 2021. Unit 32081, in 2023, posted university recruitment advertisements for a few different locations in Beijing, as well as Shandong, Sha'anxi, and Inner Mongolia provinces. The advertisements solicit multiple majors

[xvii] As a result of this framework, this report did not include Unit 32053 as a new unit for possible offensive cyber capabilities related to space. Unit 32053 has written about satellite communications, but specifically how to model the security of new Inmarsat satellites on China's growing domestic constellation. In 2019 the unit was recruiting Masters and PhDs in communication engineering, electronic information science and technology, network and information security, and applied mathematics for jobs in the Yangcheng district of Guangzhou City, Guangdong Province. Their technical reports are network security related. Unit 32053 was described as a "new type of combat force established after the reform, focusing on technology research and development and application."

in computer science, cyber security, international relations, and more niche fields like "hydroacoustic confrontation" and English translation.[xviii]

Unit 32082 received at least two invention patents for computer network exploitation tools, both in mid-2019. The first is for a honeypot design intended to attract enemies already inside China's network. The second is a Trojan design for computer chip hardware supporting spread spectrum technologies. The patent authors claim the Trojan is new in that it can avoid detection by the "enemy military's" standard detection methods. While speculative, the latter example might enable access to satellite-based internet links like those used by non-Chinese cyber actor Turla. China regularly exports technologies with Chinese-designed computer chips to developing countries and is developing more advanced chips for satellites in the face of western export controls.

Unit 32082, in 2022, authored a technical study looking at multiple GNSS systems, including the newest Beidou-3, which uses various techniques to increase the speed of GNSS signal acquisition by a receiving terminal, to include auxiliary information like receiver position, satellite ephemeris, and receiver time. The researchers investigated the implications of inaccurate auxiliary information, such as how it would impact signal reception, which might indicate the unit's interest in developing a cyber-enabled GNSS spoofing capability, or mitigating such a capacity for Beidou. The authors cite English and Mandarin research covering Beidou, Galileo, and GPS.

HYPOTHESIZED PLA UNITS FOR OTHER KNOWN CYBER ACTORS

Cyber security firms have not publicly associated two Chinese actors, Anchor Panda and APT 14, with a specific Chinese actor, despite the similarity of the malware used and targets. Cyber security experts have however noted that Anchor Panda and APT 14 have targeted satellite communications equipment and maritime satellite information. Anchor Panda may be associated with the PLA Navy's southern fleet, according to one Western cyber security firm. Anchor Panda's activities are distinct from another Chinese cyber actor, referred to by cyber security experts as Thrip, Lotus Blossom, and Billbug, similarly interested in satellite data specifically from Southeast Asian countries.

Based on the available references provided by the cyber security experts, this research investigated several possible PLA units, noting that Anchor Panda and APT 14 might end up being related to MSS actors or freelancers, not the PLA, but this investigation did find some possible candidates for additional follow-up research.

Regarding a possible Anchor Panda or APT 14 association, the PLA Navy historically has had two of its own TRBs, one based out of Beijing, and one based out of Fujian Province, directly across from Taiwan. While Fujian Province is technically in the new Eastern Theater, it has historically overseen offices in Guangdong and Hainan provinces. Unit 91746 is the former PLA

[xviii] "The recruitment majors mainly include underwater acoustic signal processing, hydroacoustic engineering, hydroacoustic confrontation, computer science and technology, cyberspace security, software engineering, communication engineering, information security data science, big data, machine learning, artificial intelligence, mathematics, journalism and communication, political science, economics, finance, international relations, international business, English translation and other disciplines." The unit is mainly located in in Beijing Haidian District and Beijing Daxing District, with a small amount located in Jinan City, Shandong province, Xi'an City, Sha'anxi Province, and Hohhot City, Inner Mongolia Province.

Navy first TRB in Beijing and the unit number was still in use as of 2021, according to construction bids for the unit in Beijing, Heilongjiang, and Henan provinces. However, this research could not find confirmation that the unit was still with the PLA Navy, or if it had transitioned to the SSF; the unit is only referred to as a PLA unit, with the last Navy reference being around 2016. As of 2018, Unit 91746 had moved an antenna, probably for satellite communications or maritime intelligence, surveillance, and reconnaissance (ISR) from Beijing to Xuchang, Henan Province, approximately 2 hours south of Kaifeng, a project expected to be complete by 2020, which might be related to the SSF Base 36 in Kaifeng.

Unit 91746 might be either Anchor Panda or APT14, based on its reports discussing the need to integrate satellite information into Navy systems, and separately writing in-depth about cyber intrusions.

For example, in 2017, the unit coauthored a paper, with what has become the Space Engineering University of the SSF, on integrating space ISR support into the naval command system. The authors described that the intelligence support system, as of 2017, was trying to adjust to meet the requirements of the 2015 military reform, and indicated that there was still some uncertainty as to if the PLA Navy would "use its own ocean surveillance satellites," have the SSF onboard Navy vessels, or have to apply to "higher authorities" for space intelligence support. The relocation of the antenna to just outside the SSF's new Base 36 could indicate that the SSF will have a role in optimizing the PLA Navy's existing satellite equipment to provide better space-information support.

Unit 91746 in 2017 also wrote about assembly-level malicious code analysis, and in 2011 wrote about developing methods for hiding files at a deeper level on a system driver, for virus and anti-virus development.

Another contender for Anchor Panda or APT 14 could be Unit 92762, which is the PLA Navy's Second TRB in Fujian Province. As of 2022, a group working with fishermen still used the unit number in Jiangsu Province, indicating that potentially the unit is still a PLA Navy unit, though recent information is sparse. However, the unit seems most active in Yunnan Province, wearing SSF patches on Navy uniforms and in SSF uniforms, indicating it is in the process of transferring to the SSF.

Unit 92762 has coauthored reports in 2006 and 2008 on communication hardware and spread spectrum security, both of which can be used in satellites themselves, or systems integrating space information. These reports are connected with the space sector, based on the authors stated a research focus on satellite communications, and their publication in China's Space Electronics journal. Unit 92762 independently authored on cyber intrusion monitoring in 2009 and 2012.

In an effort to determine the affiliation of the actor referred to as Thrip, Lotus Blossom, and Billbug, this research considered other PLA units with a known focus on cyber intrusions into Southeast Asian countries and then investigated if they also had written on space-related information. Former Chengdu MR Second TRB Unit 78020, attributed to at least the group called Naikon, which has not been identified as having a space interest, is still active as of a 2022 university graduate recruitment notice for computer and software engineers, which clearly states it has transferred to the SSF. While speculative, this research found that at least two of their papers were about general technologies that are also frequently used in satellite image processing and satellite video broadcast. The articles discuss decrypting image pixels and also spoofing video,

which could hypothetically connect with Thrip's space geospatial imagery interest, but this is speculative and requires additional technical review.

HYPOTHESIS OF COMMAND AND CONTROL (C2) OF CYBER COUNTERSPACE WEAPONS

In an attempt to bring more fidelity to China's counterspace C2, this section will attempt to answer two questions. First, "What is the most likely chain of command for the PLA to decide when to use offensive cyber capabilities for a counterspace application?" This first question relates to the above section, which attempts to answer, "Who in the PLA will use offensive cyber capabilities?" The second question in this section is, "In what way will the PLA be directed to execute a cyberattack on space systems?"

Of the PLA counterspace weapons reviewed in this report, the cyber weapons have the most complicated C2, with more actors empowered to exploit foreign information networks, reconnaissance from which provides the first step in cyber weapon development or execution. In addition to the SSF, which is directly under the command of the Central Military Commission (CMC), and may deploy or maintain cyber stations to support Theater Commands (TCs), the TCs maintain their own cyber command operation centers. Additionally, at least in the past, individual PLA service technical reconnaissance bureaus (TRBs) also executed cyber operations. Apart from military actors, other PRC actors include the civilian Ministry of State Security (MSS), loosely coordinated military-civilian cyber militias, and patriotic hacking groups.

Most up-to-date western research on the SSF's role in the PLA's offensive cyber operations reiterates that even PLA sources confirm that the SSF will not be the only PLA force conducting cyber operations. Western researchers are still trying to assess if there will be coordination or baton-passing between civilian and military organizations during a transition from peacetime to wartime operations.[xix] This is especially important if early, strategic cyber operations are led in peacetime by the MSS, but are brought to fruition in wartime operations under the SSF or a TC. Furthermore, determining the command structure and the extent of delegation from the CMC to the TCs, and services, depends largely on uncertain distinctions between "strategic-," "campaign-," and "tactical-" level cyberattacks.

Authoritative PLA books, as recent as the PLA National Defense University's (NDU's) 2020 Science of Military Strategy (SMS), state that cyber, or network, operations are one type of information operations, and these types of operations will happen in advance of, and throughout a conflict. Other types of information operations include space information operations, electromagnetic spectrum operations, and phycological operations. This section discusses the connection between space information operations and network operations after first addressing information operations more generally. The 2020 SMS describes an information attack as,

[xix] Additionally, there is analytic tension between the arguments that the PLA has access to everything in China and the nature of intelligence operations, which are highly classified and shared only with those that have a "need-to-know." There are many unknowns regarding if the PLA, with its mandate for wartime cyberattack, can metaphorically scroll through all the MSS's information to identify good cyberattack vectors, or if the MSS upon finding one has to share it with the PLA. Alternatively, maybe the PLA is in charge of finding its own entry points.

"*The organiz[ation of] military and local information attack forces to attack the enemy's command, early warning, air defense, and anti-missile systems. The main methods are: the use of electronic jamming drones… the use of satellite communication jamming forces to interfere with enemy communication satellites and maritime satellites; the use of electronic warfare aircraft to detect and guide the enemy's early warning radar…use [of] various interference forces to interfere with enemy early warning aircraft and data links; organize network [cyber] warfare forces as appropriate to attack the enemy's potential target network for war."*

The selected 2020 SMS caption includes "as appropriate" when including cyber operations in information attacks, which is important because the book later states that, "It is necessary to develop strategic guidance for active defense in cyberspace," indicating that wartime cyberattack plans, at least as of 2020, were not fully fleshed out.

Towards that effort, the book says, the PLA will, "take the development path of comprehensive integration and build a cyber and electromagnetic spectrum combat force system that integrates reconnaissance, offense and defense." In this case, the 2020 SMS indicates that network-electromagnetic spectrum operations would probably be led under TC Joint Operations Command centers, after overarching coordination of electromagnetic spectrum operations such as jamming were pre-approved by the CMC. The PLA's description seems similar to U.S. plans for "electronic warfare and cyber convergence," which in the U.S. has been planned and coordinated for all domain-related activities at the tactical and more recently at the joint campaign level.

Regarding the presumably pre-war strategic cyber operations, the 2020 SMS indicates that the PLA might consider even these to be attacks with network-electromagnetic spectrum operations. The book first emphasizes that cyberattacks need to be integrated into joint operations by stating, "Under unified leadership and command, the goal of cyberspace combat force construction is to maximize the formation of an overall joint force, rather than the ability to fight alone."

Referencing what western researchers usually identify as strategic level cyber goals, the 2020 SMS states that, "Cyber warfare is an offensive and defensive operation carried out in the entire cyberspace…The purpose is to gain information superiority and then seize the initiative in war. Its combat object may be a military network information system, or it may be a civilian network information system." The text then describes this type of "strategic" cyber operation as related to network-electromagnetic spectrum operations, stating, "The main means of implementing cyber warfare are: using the network characteristics and electromagnetic characteristics of computer information systems to conduct network reconnaissance; using computer viruses, logic bombs, and chip weapons to implement network attacks."

An additional and more recent example that the PLA may consider network-electromagnetic spectrum operations to also be a type of campaign or strategic cyberattack is the following quote from a December 2022 PLA media article. The author stated, "The continuous deepening of the process of informationization and intelligence and the practical needs of military struggle have blurred the boundaries of the level of integrated network and electromagnetic operations, and the purpose and tasks of integrated operations are also expanding and extending. Sometimes it is a tactical operation, but it often has a strategic role in the campaign."

When thinking through the chain of command for the use of a cyberattack on a space system, readers need to be familiar with the connection between space information operations and the PLA's drive to converge network and electromagnetic spectrum operations. In the PLA NDU 2015 book called Study on Asymmetric Operations, the author connects the concept of information operations with space operations. The book says,

> *"In informationized warfare, the status and roles of such domains as the land, sea, air, outer space, electromagnetics, the network, and knowledge differ. Of these, the electromagnetics domain and the network domain are the intermediaries that link the weapons platforms that are spread all over the natural spaces— the land, sea, air, and outer space — and people. These two domains have a linking and controlling role for the various spaces of the land, sea, air, and outer space; they are the foundational domains. By attacking these two domains and targets in their related domains, it is possible to deprive the enemy of the use of these two domains; to damage the links in the enemy's land, sea, air, and outer space combat domains; and to thus greatly reduce the enemy's overall combat capabilities."*

As a result of PLA space operations being first and foremost about space information support to joint operations, the book further states, "An outer space battlefield and a network-electromagnetic battlefield are the basis for an informationized battlefield." The PLA considers space to be important in its thinking on cyberattacks and jamming generally because space is a strategic military domain, and populated with systems that support and enable information carried by way of network-electromagnetic spectrum.[xx]

The last portion of this chapter attempts to answer the second question, "In what way will the PLA be directed to execute a cyberattack on space systems?" The Academy of Military Science's (AMS's) 2013 Lectures on the Science of Space Operations gives some indications of how the CMC will direct either the SSF or separate TC components to use cyber weapons against space systems, including ground-based and space-based systems. The book clarifies that, at the time, the PLA was preparing for two kinds of space-information specific cyberattacks:

> *"There are primarily two kinds of network attacks against space-based weapons systems. The first is to get data chaining parameters and communications protocols by deciphering satellite signals and to inject viruses, logic bombs, and false information signals into the opponent's information system by means of his data chaining, thus creating malfunctions in the satellite information system or thoroughly paralyzing it. The second is to conceal computer viruses in computers in the opponent's satellite information system in advance*

[xx] The 2013 AMS Lectures on the Science of Space Operations states that, "future space operations will be mainly manifested as space information support" and "struggling for dominance in space information will inevitably become a focus of operational actions, and the two hostile sides will inevitably mobilize all means to cut off information links between the opponent's space and other battlefield spaces. Therefore, the two combatants' powerful struggle for space information dominance will inevitably increase the level of intensity in information confrontations." In PLA parlance, "information confrontation" usually means jamming and deception, or spoofing.

by means of covert channels and to activate the viruses when necessary, thus damaging the opponent's information system."

The first example seems to be discussing network-electromagnetic spectrum attacks on space systems, without using the specific term. The 2013 AMS text clarifies that the type of information confrontation, which it defines as deception or jamming, that the "space forces" would participate in is, "information jamming by means of the application of cyber [network] warfare and electronic warfare to sabotage the enemy space base's C2 net, and suppress and jam the enemy space measurement and control signals, so that the enemy space base cannot effectively fulfill its launch missions." As discussed in this report's Chapter titled Terrestrially-Based Satellite Jamming Weapons, the ground-to-space jamming units may also be referred to as a network-electromagnetic spectrum unit, and their attack purview includes primarily navigation and communications satellite downlinks, and in some cases, uplinks. PLA space-based jamming units do not appear to be referred to as "network-electromagnetic spectrum" units and they are organizationally a different SSF component, but this report is unclear on the implications of this for determining if a space-based network-electromagnetic cyberattack is in the PLA's toolbox.

The second example listed by the AMS would seem to be a strategic-level operation, and would highly likely involve coordination with the PRC's civilian intelligence agencies, but could hypothetically be managed by the former General Staff Department's Intelligence Department, also known as 2PLA, the post reform responsibilities of which may have gone to either or both the SSF or the new CMC Joint Staff Department. Western researchers have historically referred to the 2PLA as like the U.S. Department of Defense's Defense Intelligence Agency.

For the purpose of considering what type of counterspace mission might fall under "conceal computer viruses in computers in the opponent's satellite information system in advance by means of covert channels," and at the same time avoiding an analytical bias of mirroring, this research will take the AMS 2013 text literally when it emphasizes an interest in interfering with space launch missions.[xxi] The text states, "space forces" would participate in "information jamming by means of the application of cyber [network] warfare and electronic warfare … so that the enemy space base cannot effectively fulfill its launch missions."

While speculative, the early 2000s cyber intrusion into the National Aeronautics and Space Administration's (NASA's) Kennedy Space Flight Center space shuttle vehicle assembly building may have been to learn more than just complex launch vehicle preparation operations. The 2008 attack is one of many NASA cyberattacks, but one of the very few which have been publicly traced to servers, in this case, in Taiwan. The PLA's mandate to protect the PRC's right to launch into space and the need to be ready to rapidly launch when satellites have been damaged is prevalent throughout many PLA texts. The most recent example is in the 2020 SMS, which says the PLA must provide "emergency" space launch capabilities. Also of note, in May 2022, Chinese media reported that the PLA identified a car-based, commercially available, navigation signal jammer

[xxi] In the U.S., the concern over direct ascent anti-satellite missiles was initially addressed by ideas about responsive launch missions, but now the emphasis has shifted to proliferated constellations. The PRC still perceives the need for responsive launch to be important even as of 2020, potentially because they are behind in proliferated constellations, but also potentially because they highly likely view the problem and solution set differently.

within 32 feet of one of the Jiuquan satellite launch pads, which could have disrupted navigation systems and caused a rocket to deviate from its trajectory. The extremely close proximity to a very remote launch center with good security would indicate this was likely an unintentional PLA-on-PLA accident, but it highlights the PLA's concern with launch interference.

Chapter 5: Directed Energy Counterspace Weapons

SUMMARY

The directed energy (DE) counterspace weapons discussed in this chapter are ground-based mobile laser weapons and mobile high-powered microwave (HPM) weapons. The PLA has already demonstrated a DE counterspace laser for reversibly dazzling low-orbit, probably imagery satellites, as early as 2005. PLA researchers, as early as 2007, have begun attempting to increase the power of the technology for high-orbit reversible interference with early warning satellites, such as the U.S. Defense Support Program (DSP) and Space-based Infrared System (SBIRS). According to the U.S. Defense Intelligence Agency (DIA), "China has multiple ground-based laser weapons of varying power levels," which when used against satellites are primarily for targeting the electro-optical sensors. The DIA has additionally stated that possibly by the mid-to-late 2020s, the PLA may field higher powered systems to damage other satellite structures. The DIA's report does not address the PLA's HPM weapons. This chapter includes several references to the PLA's claims of mature ground-based HPM weapons systems in PLA textbooks.

Low-powered, reversible DE counterspace weapon testing, training support, and potentially usage is primarily the purview of the Strategic Support Force's (SSF's) Base 33 in Luoyang City, Henan Province. This base is often referred to as Unit 63880. A new SSF base called Base 36 and unaffiliated Unit 63660 are also heavily involved in DE technology, potentially with a focus on higher-powered weapons, but with only a few clear examples of counterspace applications. SSF Base 36 and Unit 63660 are also primarily based in Henan Province within a few hours of Bass 33; they also maintain facilities in Xinjiang Province. For these reasons, this chapter includes SSF Base 36 and Unit 63660 for additional analysis.

Two trends indicate that PLA command of DE counterspace weapon operators is still in transition. First, there continues to be PLA concern with a disconnect between the science, technology and engineering units and the forces who will actually use the weapons. Second, non-SSF units continue to describe their planning for reversible and destructive counterspace lasers, even after the creation of the SSF. The goal of this and other chapters in this report is to identify the PLA units which will use counterspace weapons in a time of conflict; but in this chapter, the available information on these weapons points to SSF employed civil servant science and technology (S&T) experts and non-SSF services.

Another key point in this chapter is that the PLA does not maintain the same division between DE and electronic warfare (EW) counterspace weapons, as some western researchers presume. Even the DIA's report defines DE weapons as lasers, high-power microwaves, and "other types of radiofrequency weapons," but then proceeds to describe DE and EW weapons separately. The PLA regularly includes lasers as a type of EW and information warfare weapon. The PLA also regularly refers to DE counterspace weapons as "jamming" satellites, phraseology western researchers usually reserve for EW weapons. This chapter can however confirm that the PLA often describes the "electro-optic jamming" teams as separate from navigation and radar jamming teams. The PLA often refers to communications jamming teams as jamming satellite

communications, which would be in the microwave frequency band, and might be capable of HPM attacks.[xxii]

Towards better understanding the PLA's thinking on command and control for ground-based DE counterspace weapons, this chapter can provide clarity on the PLA's probably widely deployed mobile DE trucks for reversible satellite dazzling and space services jamming. The PLA Central Military Commission (CMC) seems to categorize destructive, non-reversible attacks with DE weapons as "strategic" and low-powered, reversible attacks with DE weapons as "campaign," and "tactical." This distinction indicates that Theater Commands (TCs) can probably decide to leverage the low-powered, reversible weapons without repetitive higher approval, coordinating instead with the TC Joint Operations Center. This research did not find evidence of a deployed high-powered laser capability.

PLA UNITS TESTING AND SUPPORTING TRAINING WITH DIRECTED ENERGY COUNTERSPACE WEAPONS

Former General Armaments Department (GAD), now probably SSF Base 33, in Luoyang City, Henan Province is one of three former GAD weapons testing and training bases, which supported the PLA services and former Second Artillery Force. Base 33 is also known as Unit 63880. The base has historically been responsible for testing and training PLA joint forces on electronic warfare equipment; its subordinate units have long worked on lasers and microwave weapons for multiple applications, including counterspace. As of early 2023, the SSF Base 33 described itself as an "engineering application and technology research composite unit [in] the work fields of electronics, communications, navigation, computers, optics and other fields."

Based on publicly available information, subordinate units 63891 and 63892 have done the most on counterspace applications. They have focused on supporting the now Rocket Force with laser dazzling early warning satellites, and training electronic warfare (EW) forces focused on satellite communications (SATCOM) jamming, with reversible and non-reversible microwave attack weapons. In early 2023, Unit 63891 was recruiting "engineering application and technology researchers for electronics, communications, radar, navigation, computer, optics, and other majors." In 2021, Unit 63892 was recruiting "information and communication engineering, optical engineering, aircraft design and other majors." Their more recent technical articles have increasingly been discussing "network-electronic" countermeasures, more information about which is in a separate Chapter titled Terrestrially-Based Satellite Electronic Jamming Weapons.

- Unit 63891, in 2022, wrote about preparing SATCOM jamming units for reversible and non-reversible attacks, to include with HPMs. The author repeated a decades long complaint about the actual EW troops not understanding the equipment, and there being a gap between the expertise of the technical forces and the actual troops. Unit 63891 with Unit 63886, also subordinate to Base 33, as early as in 2011, detailed the problem of the EW troops not understanding how to leverage the high technology equipment, leading to misuse, equipment failures, and non-realistic training practice.

[xxii] Determining when DE weapons are included in PLA references to EW forces is a challenge, so at this time, the information this report found on probable space-based laser and HPM weapon developments is not included in this nor the other space-based counterspace weapons chapters. It will be the topic of follow-up research.

- Unit 63891 in 2012 also authored a report on ground-to-space laser applications for infrared sensors.
- Unit 63892 with the Second Artillery in 2013 wrote a technical report on ground-to-space laser aiming precision to counter optical reconnaissance satellites. In 2023 Unit 63892 authored a report on the current status of GEO communications satellites jamming and countermeasures, to include the use of destructive HPM weapons.

While units subordinate to SSF Base 33 are most likely training with, or even potentially deploying with, EW troops who will use reversible, low-powered DE counterspace weapons, different SSF units seem focused on developing high-powered laser counterspace weapons. A review of technical articles indicates that a new SSF Unit 32026 and probably subordinate Unit 32027 are likely in charge of testing and supporting training with high-powered, ground-based counterspace lasers, though this is not their only responsibility. These units also publish on multiple other laser applications and space topics, which don't seem directly counterspace related. Unit 32027 has also published two other reports on intentional and unintentional satellite jamming, reports which seem to be discussing radio wave enabled jamming, not optical enabled jamming.[xxiii]

As of 2020, SSF unit 32026 was headquartered in Kaifeng City, Henan Province and had subordinate units located at least in Wulumuqi City, Xinjiang Province, Xi'an City, Sha'anxi Province, and Beijing and Tianjin Municipalities. SSF Unit 32026 is likely the unit number for a new SSF Base 36, which most probably absorbed former GAD units 63650 and 63655 and their work on lasers, including counterspace lasers in Xinjiang Province. While Base 36 seems to have absorbed the former GAD's high-powered laser work, amongst other units, it is highly unlikely that all the different locations of Unit 32026 are focused on counterspace lasers; they probably work on broader laser applications.

- A researcher from Unit 32026 in Wulumuqi City, Xinjiang Province published two relevant articles, one in English and a separate article in Mandarin, with the PLA National University of Defense Technology's School of Electronic Countermeasures in Hefei, Anhui Province. The first article in November 2018 simulated optical satellite damage with a ground-based laser applied at different angles. The second article in January 2019 reported a test on the thermal effect of a pulsed laser for satellite blinding and blinding detection. The authors are all the same, and the proximity of the publications indicates that these results may have been based on a single usage of the laser facilities in Xinjiang.
- Several researchers from unit 32027 out of Kaifeng City, Henan Province applied for invention patents from China's State Intellectual Property Office (SIPO). The first of which, in May 2019, was specifically for modeling laser intensity distribution on targets for high power and pulsed lasers. While there was no reference to space applications, the unit later applied for another invention patent from SIPO in June 2020 covering ground-to-space methods to characterize atmospheric interference at various sites in China.

[xxiii] Unit 32027's participating authors are all different across the two articles, but each of them states that communications countermeasures is their research focus.

The available information did not show units 32026 and 32027 writing on, or testing, HPM counterspace weapons. Rather a different PLA unit has published extensively on HPM and electromagnetic pulse (EP) technology, but not with a clear counterspace focus. Unit 63660 is not readily mentioned in Mandarin media until around 2019, around which time it has become clear that the unit is based out of Luoyang City, Henan Province, and maintains a testing facility in Xinjiang Province. Recent procurement announcements for the unit do indicate that some of the procured items would be used for satellite applications. The unit has rapidly received multiple HPM and EP related invention patents since it appeared. As of early 2023, online media referred to Unit 63660 as a general PLA unit, and not a SSF unit. A probably related unit, 63663, has existed since before the SSF's creation in late 2015, and Mandarin articles, as early as 2011, have referred to it as a vehicle service team, indicating that Unit 63660 may also have existed in that timeframe. Unit 63663 is still active as of 2023, based on procurement notices.

As discussed above, Luoyang City is the location of SSF Base 33, but this report could not determine if Unit 63660 was subordinate to the base. According to PLA numbering conventions, it does not seem that Unit 63660 would be under Base 33, the unit number for which is Unit 63880. However, Unit 63660 would be a former GAD unit, most of which have transferred to the SSF. The proximity of Unit 63660's facilities to both Base 33 and the new SSF Base 36 in Kaifeng justifies its inclusion in this report.

A 2023 recruitment notice for Unit 63660 stated it originated in the time of the "Two Bombs one Satellite Era" and embodies the "Malan Spirit," indicating its historical connection with former GAD Base 21 in Xinjiang Province, the unit number for which was Unit 63650. The recruitment notice also states that the unit is involved in leading edge weapons testing and evaluation in the fields of electronics and information technology, military weapons development, aerospace technology, and artificial intelligence unmanned systems.[xxiv] As of 2021, Unit 63660 maintained, or was expanding, two facilities. First, its facilities in Jiaozuo, Henan, which is approximately two hours northeast from Luoyang; and second, facilities in Hangzhou City, which is in the more coastal Zhejiang Province. Procurement announcements for Unit 63660's Jiaozuo and Hangzhou locations indicate that the equipment would be used for satellite applications,

[xxiv] In a November 2022 recruitment advertisement, recruited majors include: Electronic Science and Technology, Optical Engineering and Technology, Instrument Science and Technology, Information System Communication Engineering, Computer Science and Technology, Aerospace Science and Technology, Control Science and Technology, Software Engineering, Ordnance Science and Technology, Artificial Intelligence Science and Technology, Physics, Mathematics and other related majors.

amongst others.[xxv,xxvi] The procurement notices for the Luoyang facilities do not include satellite applications.[xxvii]

The below image is from Unit 63660's November 2021 recruitment advertisement, which shows mobile trucks with sliding roofs and antennas, which might be capable of housing the HPM and EP weapons.

THOUGHTS ON THE SSF'S ROLE IN WARTIME USAGE OF DIRECTED ENERGY COUNTERSPACE WEAPONS

The goal of this report is to identify PLA units which will use counterspace weapons in a time of conflict, but in this case, Chinese media refers to the relevant units involved in DE counterspace weapons as PLA employed civil servant science and technology (S&T) experts. Recent reports from Unit 63891 still expressing concerns of a disconnect between S&T units and the warfighting troops, together with even the new SSF units still being described as "science and technology research units, not regular troops," indicates that the PLA is still not satisfied with its command of DE counterspace weapons. While most western researchers discuss the SSF as having absorbed the previous GAD and General Staff Department (GSD) high technology units, engineering and logistics units have important battle-support roles. An informed Chinese blogger

[xxv] A notice out of Jiaozuo for a transverse electromagnetic wave chamber (TEM Chamber) indicated the relevant fields would be: Satellite Applications, Guidance and Control Technology, Electronic Components, Detection and Identification, Computers and Software, System Modeling, Simulation and Evaluation, Electronic Information, Network Communications, Power and Transmission, Advanced Materials and Manufacturing, Reliability/Testability/Maintenance, Others

[xxvi] A notice out of Hangzhou for an unmanned arial vehicle swarm (UAV swarm) system indicated the relevant fields would be: Satellite Applications, Guidance and Control Technology, Electronic Components, Computers and Software, Electronic Information, Network Communications, Power and Transmission, Reliability/Testability/Maintenance, Others

[xxvii] A notice out of Luoyang for radiation testing equipment indicated the relevant fields would be: Detection and Identification, Computers and Software, System Modeling, Simulation and Evaluation, Electronic Information, Reliability/Testability/Maintainability, among others.

analyzing various PLA SSF recruitment advertisements has stated that Unit 32027 is a scientific research organization from the former General Logistics Department, not former GAD or GSD.

Ultimately, even S&T and engineering units might deploy to support joint forces, or as some other recruitment advertisements have stated, they may convert to regular troops in wartime. One way to determine if the units included in this report will also be the units that will ultimately use these weapons in wartime is to research the role the SSF plays in joint national or regional military exercises. This research found one reference to Base 36's "combat company" participating in a 2018 counter-air operations exercise in Luoyang, Henan Province, which was probably hosted by Base 33. In another example, Base 36 subordinate Unit 32031 participated in a SSF hosted exercise in 2019, were participants exercised unscripted operations to "interfere with the enemy" and "prevent reconnaissance of important areas."

Yet another way to attempt to determine if the units that work on DE counterspace weapons do indeed deploy to operate these weapons in a time of conflict is to research if those units are stationed in multiple locations, which might make them more readily available to a Theater Commander. Under Base 36, this research found one unit, Unit 32033, which has multiple locations, but the unit did not have any obvious DE counterspace focus; it is rather a space information support unit deployed with EW and Rocket Force units. Base 36 subordinate Unit 32033, as of at least 2019, had units in several places: Jiaozuo, Henan Province; Fengtai District, Beijing; Sanya, Hainan Island; Shenzhen, Guangdong Province; Haikou, Hainan Island; Hangzhou, Zhejiang Province; and Ejina Banner, Inner Mongolia.

This research also found Unit 63891 maintains at least three locations and Unit 63892 maintains at least five locations, though they are not in as many PLA operationally useful locations like Unit 32033. Unit 63891 is in Luoyang City and Jiaozuo City, both in Henan Province, and Beijing. Unit 63892 is in Xian City, Sha'anxi Province, Jiaozuo, Luoyang, and Kaifeng, cities all in Henan Province, and Beijing.

HYPOTHESIS OF PLA COMMAND AND CONTROL (C2) FOR DIRECTED ENERGY COUNTERSPACE WEAPONS

In an attempt to bring more fidelity to China's counterspace C2, this section will attempt to answer two questions. First, "What is the most likely chain of command for the PLA to decide when to use DE counterspace weapons?" This question is related to the above section's question: "Who in the PLA will use DE counterspace weapons?" The second question in this section is, "In what way will the PLA be directed to use DE counterspace weapons?"

The PLA Central Military Commission's (CMC's) Joint Operations Command Center (JOCC) highly likely delegates deployment planning of counterspace DE weapons for low-powered, reversible attacks to Theater Command (TC) JOCCs. Many reasons support this assertion. First, the CMC has long intended wide PLA usage of DE technology through supporting development of "new concept weapons." Second, PLA media and textbooks refer to the reversible usage of DE counterspace weapons as a weapon used by electronic warfare troops, which are subordinate to TC JOCCs. For example, the 2018 PRC National Defense University (NDU) book called Mechanisms for Gaining Victory with Electronic Confrontation states that,

> *"Under informationized conditions, although electronic confrontations include electronic reconnaissance satellites, directed energy weapons, and other strategic- and*

campaign-level weapons and equipment…there has been no change yet in the basic position that electronic confrontation strengths are subordinate to joint operations strengths, and that the goals of electronic confrontation serve the goals of joint campaigns."

A third reason is based on evidence that TC units are developing methodologies to help TC commanders effectively use DE counterspace weapons, like mobile laser dazzling trucks. In one case, the PLA Central TC's Unit 66135 out of Beijing in 2020 published their technical study on how commanders should determine the effective suppression zone of ground-based, probably mobile counterspace laser dazzling stations when crafting deployment plans. The Central TC's focus was on interfering with early warning satellites like the U.S. SBIRS in geosynchronous Earth orbit (GEO) to slow the satellite's information acquisition time.

HPM counterspace weapons for reversible attacks are also probably delegated to the TCs. Based on Unit 63660's focus on testing and training other units in HPM weapons on mobile platforms, to include systems with satellite applications, it seems reasonable to assume that such mobile platforms support campaign and tactical level joint operations. In the 2016 PLA book called Perspectives of U.S. Military Space Operations Exercises, which analyzed the PRC perceived content of early U.S. Schriever and Space Flag exercises, the author stated that the United States assumed it and the Chinese would use ground-based HPM weapons for counterspace applications starting in 2021. The book also says the United States assumed it and the Chinese would have EP weapons in 2027 for counterspace operations. This might mean that the PLA assumes early U.S. references to these weapons imply the U.S. planned to widely deploy the weapons, and that the PLA must be prepared to as well.

Because the PLA regards DE weapons as one of the tools of its electronic warfare (EW) forces, and it does not yet appear that all PLA EW forces are, or will be, SSF units, TC's ability to task reversible counterspace DE weapons is important.[xxviii] Both early and more recent examples of non-SSF PLA services discussing how they use their unit's DE counterspace weapons implies TC command and control. For example, as early as 2007, the then Second Artillery was developing strategies to temporarily dazzle early warning satellites like the U.S. DSP satellites in GEO to decrease the United States ability to shoot down PLA ballistic missiles. The Second Artillery also wrote a similar article with Base 33 in 2012. The PLA Navy in 2018 discussed the use of lasers to protect PLA Navy communications satellites.

The last portion of this chapter attempts to answer the second question, "In what way will the PLA be directed to use DE counterspace weapons?" The evidence suggests that TC DE usage for reversible attacks is probably deeply integrated across the PLA for low Earth orbit (LEO) imagery and early warning satellites, higher orbit early warning satellites, and for satellite ground-based services. The 2013 Academy of Military Sciences (AMS) book titled The Lectures on the Science of Space Operations includes references to high and low power lasers as having "already demonstrated their operational effectiveness." The text further states that "the use of the means of soft kills…such as low power lasers… are an important means for seizing command of space" and that "low-powered ground-based lasers are a space-attack weapon with excellent performance."

[xxviii] See the chapter on ground-based satellite jamming for more information on the non-SSF units which will operate this EW equipment in wartime.

PLA media in January 2021 stated that "laser blinding weapons have entered the golden age," and included dazzling satellites as one of the many operationalized uses.

The same seems true for HPM weapons. The 2015 PRC National Defense University (NDU) book called Study on Asymmetric Operations refers to ground-based microwave weapons for countering communications and electronic equipment as being "mature," which probably includes jamming systems leveraging space information. In the 2018 PRC NDU book titled Mechanisms for Gaining Victory with Electronic Confrontation, the authors state that, "For example, carrying out a directed-energy attack against a communications satellite can do an effective job of paralyzing the normal operations of the entire satellite communications system," which may be a reference to ground-based HPM weapons to counter communications satellites transmitting in microwave frequencies.

Western analysts would typically categorize a destructive counterspace weapon as a strategic weapon, usage which they would now assume is under the purview of the SSF. Based on this research, PLA media does seem to use the word "strategic" more often when referencing destructive DE counterspace attacks, indicating such attacks might be approved with only cautious, centrally controlled direction. However, probably because the technology is not yet developed, this research did not find evidence that a destructive DE counterspace weapon would be operated exclusively by the SSF. Potentially complicating the CMC's central command of destructive DE weapons in wartime, the available PLA information indicates that many types of PLA units have other, non-counterspace related destructive DE weapon capabilities. For example, there is a body of Mandarin technical reports from non-SSF units on the use of lasers for destructive anti-ballistic missile operations, to include at mid-course range, technology which even advanced countries have not mastered yet.

The PLA's thinking on destructive DE counterspace weapons is probably evolving along with their technological developments. In a 2017 PLA media article, the authors stated that lasers are highly anticipated for intercepting intercontinental ballistic missiles, noting that while such anti-missile capabilities in space are under research, the most likely application will be on a ground-based truck. According to the 2020 NDU Science of Military Strategy (SMS), EW includes weapons capable of reversible and non-reversible attacks. The 2020 SMS states that EW "also has the use of anti-radiation missiles, strong laser weapons and electromagnetic pulse weapons… It not only involves electronic warfare forces, but also extensively involves various combat personnel and all combat forces that operate and use electronic equipment."

The PLA perceives that the U.S. and Russia have already achieved destructive counterspace capabilities with DE weapons, and is closely watching how the more advanced countries would deploy these weapons. In several recent PLA media articles, authors argued that multiple foreign countries were transitioning their laser counterspace weapons from soft to hard capabilities, implying the PLA should follow. The 2013 AMS book called The Lectures on the Science of Space Operations referenced the U.S. and Russia's strategy in deploying DE counterspace weapons in combat by saying, "[The U.S. and Russia] have adopted the stratagems of 'mastering capabilities and having cautious deployment,' and [the U.S. and Russia] have incrementally made breakthroughs in new-concept weapons for anti-satellites such as lasers and HPM, but they have not rushed to deploy these."

Chapter 6: Space-Based Grappling Counterspace Weapons

SUMMARY

There are two space-based capabilities most applicable to the People's Liberation Army's (PLA's) literature about on-orbit counterspace operations. This section covers maneuverable satellites in Earth orbits with at least one robotic arm. The PLA's space-based experimental electronic jamming system, which is more likely to be deployed as a counterspace weapon in wartime, is detailed in the Chapter titled Space-Based Satellite Electronic Jamming Weapons. The possibility for a PLA on-orbit grappling weapon to also have a jamming payload is very briefly discussed below.

The vast majority of the People's Republic of China's (PRC) government and PLA military documents have stated that its on-orbit movable systems with robotic arms are primarily for in-space servicing, and in support of what the PLA plans for "responsive space," a concept the PLA defines similarly to the early U.S. Operationally Responsive Space Office definitions.[xxix] The U.S. intelligence community agrees. The Defense Intelligence Agency (DIA) in 2022 stated that, "China is developing other sophisticated space-based capabilities, such as satellite inspection and repair. At least some of these capabilities could also function as a weapon." The Office of the Director of National Intelligence (ODNI) stated in its 2023 report that China's on-orbit technology demonstrations, "are not counterspace weapons tests, [but] prove China's ability to operate future space-based counterspace weapons." The DIA's report specifically lists the Shijian-17 (SJ-17) and Shijian-21 (SJ-21) satellites in geosynchronous Earth orbit (GEO) as examples. SJ-17 and SJ-21 have at least one robotic arm each and have conducted several rendezvous and proximity operations (RPOs) with other PRC satellites since their launch in 2016 and 2021, respectively.

However, two official PRC statements indicate that at least some in the PRC want internal and external audiences to interpret these systems as counterspace weapons, potentially for deterrence, or for positioning the PRC to shape international norms. First, the PRC's official submission in 2020 to the United Nations Resolution 75/36 stated that the PRC views U.S. systems like the Mission Extension Vehicle (MEV) as a threatening counterspace capability. Second, PRC government media in June 2021 publicized a PLA Northern Theater engineer's confirmation that the PRC had developed an experimental counterspace satellite with a robotic arm. He said it could change orbits and carry out detection of other satellites, but did not clarify which of the PRC's known systems he was confirming.[xxx] His statement may have been in response to the United States Space Commander General Dickinson's testimony in April 2021, which mentioned SJ-17. PLA media in early 2022 further stated that, "The U.S. Space Force plans to establish a space-based logistics on-orbit service system, provide on-orbit repair and maintenance, and small satellite recovery services for space carriers in peacetime… In wartime, they carry out space

[xxix] The U.S. Air Force Research Lab's (AFRL's) XSS-11 100kg satellite to perform on-orbit servicing was one of several satellites defined as "responsive satellites" under the Operationally Responsive Space Office's program in the early 2000s. Since then, the Chinese have pursued on-orbit servicing and rapid launch capabilities in tandem, as they perceived this was the U.S.'s plan at the time.

[xxx] The Shiyan-7 in low Earth orbit (LEO), the Aolong-1 in LEO, or the SJ-17 and SJ-21 in GEO.

combat missions such as approaching, seizing, and controlling the opponent's spacecraft." This topic is ripe for improved international messaging.

From a technical standpoint, Chinese on-orbit grappling satellites are currently large and detectable, and as such, in the near term, they are probably only capable of on-orbit servicing, not approaching undetected to grapple an adversary satellite.[xxxi] In the near-term, the PLA might be more likely to use these large satellites in what it calls a "space-blockade" to complicate adversary satellite communication links and ability to maneuver, simply by moving in the way, not by grappling nor electronically jamming adversary satellites. In the future, however, the PLA will probably miniaturize these systems and achieve what they call "stealth satellites" or "nano-spy satellites," concepts which the PLA primarily intends for intelligence, surveillance, and reconnaissance (ISR) missions, but which hypothetically could enable grappling of foreign satellites in GEO, with lower likelihood of immediate detection. This research did not find significant PLA discussion of "patrol satellite" concepts, though it is conceptually similar to what is discussed in the Chapter titled Space-based Satellite Electronic Jamming Weapons.

A new Strategic Support Force (SSF) Space Systems Department (SSD) unit out of Beijing, Unit 32032, has most likely absorbed the former General Armaments Department's (GAD's), and possibly other units' RPO missions, including planning for on-orbit servicing.[xxxii] The PLA's first maneuverable satellites, such as the SJ-15, were developed for and fielded to former GAD units; the PRC's first robotic arm systems, such as the Shiyan-7, were most likely later fielded to different GAD units working on the Chinese Space Station. This legacy leads this research to hypothesize that Unit 32032 probably plans the operations for SJ-17, a satellite which has been active in several approximately 1-kilometer (km) RPOs since its launch in March 2016, and probably SJ-21. The unit has a body of technical analysis on satellite operator training and wargaming for on-orbit servicing scenarios with uncooperative Chinese and foreign spacecraft in low Earth orbit (LEO) and GEO.

Historically, the PLA's on-orbit operations were primarily decided by the satellite owner, to include GAD, the General Staff Department (GSD), and the PLA services. PLA academy textbooks in the 2013 and 2014 timeframe describe Central Military Commission (CMC) approval for decentralized decision-making for emergency on-orbit maneuvers and other countermeasures in recognition that, at the time, the PLA could not get relevant information to the CMC in time for a useful maneuver. Based on the creation of Unit 32032, and several other indicators discussed below, this research hypothesizes that the PLA is working towards better centralization of on-orbit systems capable of RPOs, to include those for on-orbit servicing, in order to ensure resiliency of the PRC's space-based systems in wartime. This chapter will also discuss the findings indicating that the CMC Joint Operations Command Center (JOCC) is developing an on-orbit warfighting capability.

[xxxi] The SJ-17 weighs approximately 4,000 kilograms or 8,800 pounds, and launched on one of China's strongest rockets, the Long March-5. As will be discussed in the Chapter on Space-Based Satellite Jamming Weapons, these and other systems could have other counterspace payloads, for which the orbits and relative proximity to an adversary satellite could potentially enable less detectable operations.

[xxxii] This research has confirmed a Unit 32032 author to be a member of the SSD.

PLA UNIT OPERATING AND DEVELOPING TRAINING FOR SPACE-BASED GRAPPLING SYSTEMS

Unit 32032 is a new SSF SSD unit based in Beijing, Haidian District's Space City. The earliest recruitment notice for Unit 32032 is from 2019 and it solicited applicants with backgrounds in control science and engineering, computer science and technology, and software engineering for professional and technical positions. An April 2023 recruitment notice indicates a wider scope of applicants for civilian technical and PLA officer positions, including in fields of aerospace science and technology, control science and engineering, computer science and technology, information and communication engineering, optical engineering, cyberspace security, and electrical engineering.

Unit 32032 is highly likely subordinate to the new SSF Base 36, headquartered in Kaifeng City, Henan Province. A reputable Chinese netizen in 2018 assessed that some of the new SSF SSD bases such as the New Technology Base 36 and the Monitoring and Early Warning Base 37 were divided into units 32026-34 and 32035-40, respectively. This breakdown has mostly held true when researching individual unit's locations. For example, publicly available information shows that unit numbers between Unit 32026 and up to at least Unit 32030 are included under the new SSF Base 36. SSF Base 36 also has a location in the Haidian District of Beijing, consistent with at least Unit 32032. A 2018 recruitment notice for Base 36's Haidian location stated that they were looking for, "aerospace science and technology, information and communication engineering, computer science and technology, signal analysis, database construction, software engineering, simulation, guidance and navigation, pattern recognition, and power supply technology majors."

Prior to Unit 32032's recruitment of new personnel, it is likely that it was at least composed of select former GAD and General Staff Department (GSD) Units already located in Beijing's Haidian District. Unit 32032 may have also absorbed other PLA service units or at least their historical responsibility for determining their satellites' RPO and collision avoidance plans. Former GSD Unit 61541 was historically located in the Haidian District's Space City amongst several GAD units and since the establishment of the SSF, examples of its military unit number have largely disappeared. A member of Unit 61541 authored the PLA book called Perspectives on US Military Space Operations Exercises, published at the start of the SSF's creation in 2016. The book reviewed early U.S. Schriever and Space Flag wargames, to include what the PLA perceived was U.S. planning for microsatellite co-orbital counterspace weapons, a high-level review of which would have been an excellent basis for Unit 32032's later work on co-orbital operations.

Generally speaking, since its creation, Unit 32032's scientific and technical research demonstrates an expertise in algorithm development for simulating various technologies' performance and mission scenarios, not only possible grappling weapons. The technologies and mission scenarios the unit has reported on thus far, in chronological order, generally make up three phases: artificial intelligence enhanced electronic intelligence and countermeasures for terrestrial and in-orbit uses (2018-2019), hypersonic missile scenarios (2019), and on-orbit servicing and RPO scenarios with uncooperative spacecraft in LEO and GEO (2018-2021).

In December 2021, authors affiliated with Unit 32032 and the PLA Academy of Military Science (AMS) authored a book dedicated to the topic of on-orbit servicing, which could indicate a significant development in the PLA's planning and readiness for this emerging field. The title of the book is Research on Intelligent Planning for On-Orbit Service Tasks. Two of the authors, who

are elsewhere affiliated with Unit 32032, are described as on-orbit servicing experts. One of the experts is Gao Yong who is also described as being a Director of a department in the SSF's Space Systems Department (SSD). The author not affiliated with Unit 32032 is Ye Xiongbing, who at the time was the Deputy Director of the PLA AMS's Combat Experiment Center of the War Research Institute, and is described as an expert in military operations command and control.

A detailed review of Unit 32032's technical reports demonstrates their steady preparation for on-orbit servicing and RPOs with cooperative and "uncooperative" spacecraft in LEO and GEO, which the authors of one report define as defunct satellites, debris, active satellites, and space weapons. They did not define what they meant by the term "space weapon."

- Unit 32032 in 2018 wrote a technical analysis of how to build a simulator for an on-orbit service spacecraft to enhance operator training. The authors recommended that the simulator must be able to accommodate at least four on-orbit service satellites, because China's "on-orbit equipment had already passed tests in practice situations" and the authors expected the numbers to grow.
- Unit 32032 wrote about multi-orbit regime transfers for coplanar servicing missions to determine time and fuel requirements that met the team's standard for the remaining 50-kilogram (kg) of fuel. A specific orbit regime is not mentioned but the included image below indicates the scheme is to move from LEO to GEO or a highly elliptical orbit (HEO).

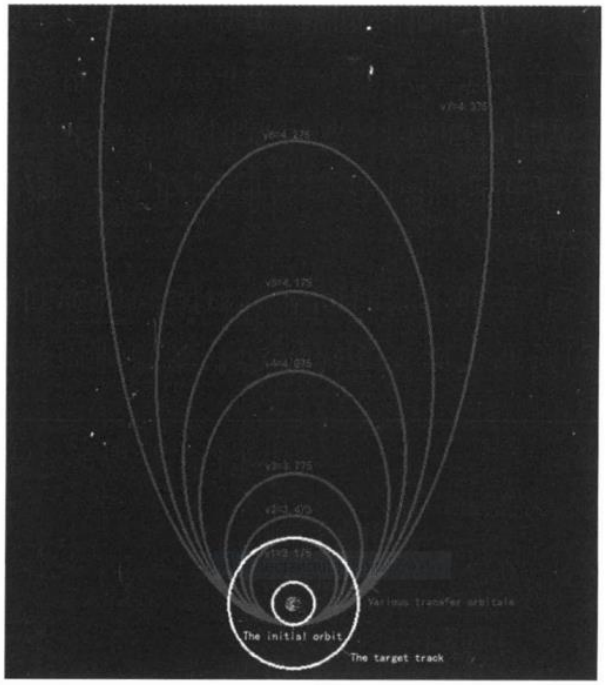


图2 不同速度下的转移轨道形态图

Fig.2 Transition orbit morphologies at different velocities

- Unit 32032 with the PLA AMS authored a report in 2020 on a simulated high orbit refueling mission that considered several foreign satellites, as in the image below. The

service vehicle started the mission from 39,164-kilometers (km), which would be the graveyard orbit above GEO.

表 1　GEO卫星的轨道根数

Table 1　Orbit elements of GEO satellite

序号	卫星名称	e	i/(°)	Ω/(°)	ω/(°)	τ/(°)
1	KAZSAT-2	0.0013	0.0068	82.8150	235.4080	65.5763
2	AZERSPACE 1	0.0021	0.0086	41.3642	228.1553	90.4703
3	INSAT-3D	0.0014	0.0170	251.0382	8.0294	100.9305
4	INTELSAT 907	0.0031	0.0081	34.8932	214.2637	110.8237
5	INTELSAT 16	0.0035	0.0085	88.0343	183.8587	117.0951
6	RADUGA-1M 2	0.0033	0.0089	320.7142	332.9825	126.5564
7	INTELSAT	0.0007	0.0034	294.4549	53.8833	138.0727
8	NSS-10	0.0031	0.0227	10.6796	246.4864	190.2729
9	VINASAT-2	0.0026	0.0087	2.2519	271.2912	210.3116
10	ZHONGXING-6B	0.0049	0.0095	328.0462	274.6047	236.4209

- Unit 32032 with the SSF Space Engineering University (SEU) and the PLA AMS authored a report in 2020 on their simulation of two satellites at 500km in LEO, each weighing 2,000kg, chasing and fleeing from each other.
- Unit 32032 and the PLA AMS updated their methodology on LEO chasing and fleeing in 2021.
- In December 2021, Unit 32032 coauthored with two universities and the China Aerospace Science and Industry Corporation (CASIC) a report on GEO space-based space situational awareness (SSA), with an optical camera, to image non-cooperative spacecraft, defined as default satellites, space debris, and space weapons. They evaluated imaging from GEO to LEO and vice versa. The authors stated that "in order to deal with the security threats of non-cooperative space targets all countries are vigorously developing space security technologies including space situational awareness and on-orbit services…"
- In April 2021 Unit 32032 with the PLA AMS, SSF SEU and the SSF Information Engineering University (IEU) evaluated fuel-optimal methods for transferring between orbits and avoiding space debris. The simulation example shows they focused on GEO from 36,000km to 36,300km, indicating a consideration with debris in the graveyard orbit.
- Unit 32032 and SEU in 2020 developed a method to identify LEO satellite optical scattering, also called satellite sails, to improve ground-based SSA. They verified their method at the Chinese Academy of Sciences Lijiang National Astronomical Observatory in south China's Yunnan Province.
- The Chinese State Intellectual Property Office (SIPO) awarded Unit 32032 an invention patent in 2022 for a system that can determine the status of a satellite's electronic reconnaissance or jamming payload, which most likely supports the PLA's decision-making on when to remove even an ISR or space-based jammer from orbit, or

hypothetically could indicate that the PLA's grappling-enabled satellites also have an ISR or jamming payload.

HYPOTHESIS OF PLA COMMAND AND CONTROL (C2) FOR SPACE-BASED GRAPPLING COUNTERSPACE WEAPONS

In an attempt to bring more fidelity to China's counterspace C2, this section will attempt to answer two questions. First, "What is the most likely chain of command for the PLA to decide when to use co-orbital grappling counterspace weapons?" This first question relates to the above section, which answers, "Who in the PLA will use them?" The second question is, "In what way will the PLA be directed to use co-orbital grappling counterspace weapons?"

Prior to PLA reform, there was evidence that some on-orbit operations, such as maneuvering tactical support satellites, were decentralized when necessary. In other words, GAD operators did not need to ask higher authorities in the CMC for approval. For example, the PLA's National Defense University (NDU) in 2014 published a textbook called Space Information Assisting-Support Operations, which detailed some aspects of C2. The authors described that the PRC would always prefer centralized decision-making, but in some battle scenarios, the technology had not yet advanced enough to enable fast centralized decision-making. In those cases, lower levels could make key decisions related to "protecting satellites" to ensure the successful completion of joint operations; in particular, lower-level commanders could decide when to maneuver a satellite when a threat was known. The book explains that even under a centralized command structure, unit commanders would still be in charge of submitting their satellite attack, defense, and information support plans for pre-approval.

Another example of lower-level commanders potentially previously being empowered to make on-orbit satellite protection decisions can be found in the PLA Academy of Military Sciences (AMS) 2013 Lectures on the Science of Space Operations in its discussion on on-orbit repairs. The text indicates that satellite protection measures include on-orbit repairs. The authors state,

> *"Two forms of maintenance will usually be used for space equipment that has been damaged: maintenance in orbit and maintenance on the ground. Regarding repairs in orbit, it will be necessary to establish technological support strengths that are extremely mobile and that can enter space at any time and carry out concomitant support for space equipment."*

While speculative, the AMS author's call for the creation of "technological support strengths" may have been one of the opinions that precipitated the creation of Unit 32032.

There are several indications that the SSF is working towards enabling centralized decision-making for on-orbit missions through the CMC JOCC. First, broadly speaking, over the last ten years, the PLA has been working to improve its ground and space-based SSA, and necessary inter-satellite relay capabilities, for quicker access to and command of their space systems. Even the U.S. ODNI has noted as recent as 2021 that without improvements to the PRC's data relay system, some of the PLA's space and counterspace planning would be delayed. However, recent PLA on-orbit servicing missions, RPOs, and uncoordinated engagements with U.S. satellites in GEO, since the establish of the SSF and Unit 32032, might indicate that the PLA has succeeded in at least some key data relay improvements.

Second, there is evidence that in addition to improving ground and space-based SSA, the SSF is working towards integrating formerly disparate, PRC funded small satellite technology test results, which could further strengthen centralized decision-making. For example, in mid-2021, Unit 63921, also known as the Beijing Institute of Tracking and Telecommunications Technology (BITTT) together with other technical Chinese Academy of Sciences (CAS) institutes wrote about a possible solution to integrating satellite test and evaluation data, which the authors said was formerly spread across various units and departments.

Most would agree that if the PLA used a large or small satellite grappling weapon against an adversary space system, this would be highly escalatory. This research could not find clear indications in PLA or other militaries' publications if grappling would be intended to enable permanent or reversible satellite interference, or if such activity would be debris generating. It is, however, safe to assume that such a decision in the PLA would be centralized. In a hypothetical scenario, even if a robotic-arm-equipped, maneuverable satellite also had a jamming payload, PLA usage would also require centralized decision-making. As discussed in this report's Chapter titled Terrestrially-Based Satellite Electronic Jamming Weapons, the PLA's usage of spectrum is centrally planned to ensure avoidance of a self-blockade.

The last portion of this chapter attempts to answer the question, "In what way will the PLA be directed to use co-orbital grappling counterspace weapons?" The PLA's methods will probably change over time, as they gradually miniaturize these systems. At present time, PLA textbooks provide examples of near-term scenarios for these systems that rely on their large size, not their grappling capability. These textbooks also provide insight into the likely scenarios in the future, probably once miniaturized.

The PLA AMS 2013 textbook called Lectures on the Science of Space Operations detailed a space blockade saying that,

> *"In space blockade operations, the main goal lies in blocking the enemy space forces from … conducting orbital maneuver, and not in seeking to thoroughly wipe out the enemy. As long as the enemy cannot timely and effectively carry out space launch and orbital maneuver, the blockade operations will directly achieve their goal."*

Importantly, all the PLA books reviewed in this research failed to mention "grappling" concepts as a type of space weapon. The type of "space blockade" with large spacecraft that is most often discussed is one where the PLA moves in the way of another country's satellite communications path, which would complicate its communication mission and could also challenge its ability to safely maneuver.

According to publicly available information, the PLA has not yet used one of its large, robotic arm equipped satellites to do RPOs with a foreign satellite, but it has with several of its own communications and navigation satellites. Taking SJ-17 as an example, it has conducted several, such as its within 1.65km RPO with Chinasat-6A in mid-2017 and its within 1 km RPO with Chinasat-20 in 2018. For context, western analysts state that approximately ninety percent of GEO satellites are separated by 25km, and ninety-six percent are separated by 10km. Also important to note is that even the Canadaarm on the International Space Station is only 15.2 meters long, so it would not be able to grapple a satellite 1km away. When the Chinese SJ-21 removed a defunct Chinese satellite from the GEO belt, its arm was much shorter than the Canadaarm, and

required getting much closer than 1km. SJ-17's RPOs are probably in preparation to conduct another on-orbit servicing mission because older Chinese communications satellites are known to be experiencing anomalies. However, while speculative, Unit 32032 has a 2022 invention patent for a way to determine if a satellite's electronic reconnaissance and jamming payloads are working, systems which they might have tested in their RPOs with Chinese communications satellites.

Further evidence that in the near-term the PLA does not plan to use systems like SJ-17 and SJ-21 as grappling counterspace weapons is that on-orbit servicing satellites are not included amongst the "new concept weapons," like nano-satellites and stealth satellites. The PLA's list of "new concept weapons" acts as a technology development plan and is a good indicator of the types of weapons receiving PLA development funding. Rather, in the 2020 Science of Military Strategy, the PLA NDU described on-orbit servicing as an emerging technology in a section separate from the one listing "offensive and defensive technologies."

The miniaturization of such systems, especially in GEO is the likely technology path which would be a hard to track co-orbital counterspace threat. PLA media in mid-2020 described that "the world's military powers," which would include China, "are investing in several space-based combat platforms which can capture and dismantle spacecraft with…robotic arms," which this research interprets as being an indicator of technologies the PLA intends to develop in the future, not a description of currently operating satellites.

Another indicator that the PLA is more likely interested in shrinking its robotic arm enabled satellites is its perception that several U.S. Schriever and Space Flag wargames have demonstrated the importance of microsatellites directly interfering with another satellites' signals, and even "attacking" satellites, based on the 2016 book called Perspectives of U.S. Military Space Operations Exercises. Additionally, PLA media in early 2022 referred to U.S. military small satellite and on-orbit servicing concepts in GEO, such as the Payload Orbital Delivery System (PODS) as "the U.S.'s orbital warfare technologies." U.S. military space on-orbit servicing experiments like the Defense Advanced Research Project Agency's (DARPA's) Phoenix program, which included PODS, and AFRL's XSS satellites have often appeared in PLA books and official media. The above 2022 reference likely indicates the PLA is still closely watching those programs, which have faced delays and been restructured, but seem to be ongoing.

Chapter 7: Space-Based Satellite Electronic Jamming Weapons

SUMMARY

Within the last ten years, the People's Liberation Army (PLA) has probably launched an experimental communications jamming satellite in geosynchronous Earth orbit (GEO) to practice space-based reversible satellite communications (SATCOM) jamming, based on limited, but recent, PLA technical report references, and an authoritative 2014 PLA academy book.[xxxiii] In 2023, the U.S. Office of the Director of National Intelligence (ODNI) stated that, "the PLA is fielding new destructive and nondestructive ground- and space-based antisatellite (ASAT) weapons." Regarding the space-based weapon reference, this report only found evidence of possible space-based reversible jamming. The U.S. Defense Intelligence Agency's (DIA's) 2022 report did not include kinetic or destructive space-based weapons references, so this research interprets ODNI's statement as potentially confirming only a PLA space-based nondestructive counterspace weapon capability.[xxxiv] The PLA units discussed below seem most interested in data relay satellites and space-to-ground communications links originating from GEO satellites.

It is important to note that even in the United States, there are multiple media references to U.S. space-based warfare training, and satellite jamming capabilities and training, so it is not surprising to find that in the few examples below, the PLA authors also casually discuss their own capabilities. In the best example, an author from a newly formed Strategic Support Force (SSF) unit said that the PLA's "existing jamming techniques and strategies don't work for GEO communications satellites using Ka-band [for data relay, and possibly crosslinks], so we need to research new techniques and strategies." The images in the paper are clearly exhibiting space-based capabilities, not ground-to-space capabilities. Consequently, this chapter hypothesizes that the PLA adopts the perspective reflected in U.S. policy circles that "jamming is a normal part of conflict," which the PLA interpret as including space-based jamming. Another important distinction is that the Ka-band is a part of the microwave portion of the electromagnetic spectrum, and PLA references to jamming it sometimes refer to electronic methods generally, or specifically "directed energy" weapons, which could confuse counterspace researchers looking for "high-powered microwave" weapons.[xxxv]

This area of the PLA's counterspace weapons command and control is still in transition, and multiple aspects need further research. For example, the PLA's space-based jamming capabilities have at least in part originated from units of the former General Armaments Department (GAD) and the General Staff Department (GSD) working on satellite communications and data relay. Since the establishment of the SSF in late 2015, there continues to be ongoing restructuring of these units. Based on current information on unit numbers and locations, the units that operate the probable experimental space-based jamming capability may now be organized

[xxxiii] This research did not try to determine a likely candidate satellite.

[xxxiv] See this report's Chapter titled Space-Based Grappling Weapons for more information on ODNI and DIA's comments on those systems.

[xxxv] For more information on high-power microwave weapons and how the PLA includes them in its discussions on electronic warfare, see this report's Chapter titled Directed Energy Counterspace Weapons and Chapter titled Terrestrially-Based Electronic Satellite Jamming Weapons.

under the SSF Space Systems Department's (SSD's) new Base 37, or the SSF SSD's new Base 36. Brief online references to Base 37 have called it the Monitoring and Early Warning Base and indicate it is headquartered, in Lintong City, Sha'anxi Province.[xxxvi] Alternatively, Base 36 is headquartered in Kaifeng City, Henan Province; brief online descriptions say it "undertakes weapons and equipment demand demonstration, testing, appraisal and evaluation tasks." Both bases have subordinate locations across China and it is not yet clear if the units discussed below, based in Henan and Beijing, are subordinate to Base 37 or Base 36.[xxxvii]

Another aspect that needs more research is if, and how, space-based jamming will be included in the PLA's drive for merging cyber and electromagnetic spectrum attack capabilities. Based on the research for this report, the PLA's electromagnetic spectrum jamming is pre-approved at the Central Military Commission (CMC) level, and on-orbit operations are executed by the SSF, which is also centralized under the CMC. More research is needed on this setup because it either could make on-orbit jamming burdened with bureaucracy or easily executable at the behest of Xi Jinping. At the same time, this research found that the CMC gives the orders for network-electromagnetic spectrum operations that would have effects outside of a theater command, whereas Theater Command Commanders give the orders to execute such attacks when effects are localized to a theater.[xxxviii]

HYPOTHESIS OF PLA UNITS OPERATING SPACE-BASED SATELLITE JAMMING WEAPONS

This section attempts to answer, "Who in the PLA will use space-based electronic satellite jamming weapons?" This chapter describes two PLA units which are highly likely operators of at least one satellite capable of conducting reversable jamming attacks. They are SSF Unit 32039 and SSF Unit 63923, with elements from the latter potentially being absorbed by the former. Two other PLA units have probably participated in testing on-orbit satellite jamming capabilities, specifically SSF Unit 32032, likely subordinate to new SSF Base 36 and SSF Unit 63888, previously subordinate to GAD Base 33.

Regarding Unit 32039 and Unit 63923, based on their publications and patents, they work primarily on managing the PRC national satellite communications network, including the relay satellites. Unit 63923 comes from a former GAD group that managed the daily orbital operations of the communications and data relay satellites. Unit 32039 comes from a group that managed the PLA's scheduling and optimization for users of strategic and tactical SATCOM. Unit 32039 may have absorbed at least a part of Unit 63923, based on the latter relocating to, or establishing, a second location in Mentougou District of Beijing in 2020, where Unit 32039 maintains a location. Unit 63923's online activities significantly decrease after 2021.

[xxxvi] The China Aerospace Studies Institute also published a report describing the implications of Base 37 in mid-2023.

[xxxvii] One list of Base 37's locations included Xi'an City in Sha'anxi Province, Jinan City in Shandong Province, Wulumuqi City in Xinjiang Province, Chuxiong City of Yunnan Province, Hangzhou City of Zhejiang Province, Chongqing Municipality, and Haidong City in Qinghai Province. A separate reference included Lichuan City, Hubei Province.

[xxxviii] For more information on the PLA's plans for network-electromagnetic spectrum operations see the Chapter titled Offensive Cyber Counterspace Weapons, the Chapter titled Terrestrially-Based Satellite Weapons, and the Chapter titled Directed Energy Counterspace Weapons.

Specific to Unit 32039, its first director nearly consecutively served in the GSD Satellite Communications Command, Unit 61096, and the GAD Data Relay Control and Management Center, probably units 63921-63923.[xxxix,xl] Unit 32039 also shares the exact same address as Unit 61096, based on their respective patent applications. Only select components of Unit 61096 may have merged with Unit 32039 because the original unit still appears to be active as of 2021. According to a 2017 study describing the PRC's national satellite communications network, the author indicated that the Central Military Commission (CMC) Joint Staff Department's (JSD's) Information and Communication Bureau assessed and approved frequency allocation of SATCOM for military end-users, and sent approved requests to the SSF's Satellite Communication Main Station for execution. Unit 32039 may have some relationship with the new SSF Satellite Communication Main Station. If Unit 32039 is under Base 37, a connection with SATCOM makes sense based on the base's technical reports that discuss ensuring PLA SATCOM from intentional and unintentional jamming. The remaining elements of Unit 61096, at least for now, may continue to fall under the JSD. As of May 2023, Unit 32039 had multiple locations in Henan Province (Sanmenxia, Xuchang, and Jiaozuo cities) and Beijing (Haidian and Mengtougou districts).

A reputable Chinese netizen in 2018 assessed that some of the new SSF SSD bases such as Base 36 and Base 37 were divided into units 32026-34 and 32035-40, respectively. This breakdown has mostly held true when researching individual unit's locations and would imply that Unit 32039 is under Base 37, the unit number for which is 32035, based on a review of technical reports.[xli] Unit 32035 is described as focusing on space target surveillance, distinguishing it from other Xi'an City based telemetry, tracking, and control (TT&C) functions at Base 26. A PRC government website has also described Base 37 as using national models for on-orbit radiation, which would be important for a SSA focused organization supporting reliable usage of SATCOM and data relay. A Base 37 component called the SSF Base 37 Third Monitoring and Early Warning Station, located near Beijing, in Lichuan City, Hubei Province, may be a new facility or one transferred to Base 37.

There are a few examples of 32039's technical papers and patents, which indicate its interest in space-based jamming as a countermeasure or as a preemptive jamming operation, probably for satellite crosslink and downlink.

- 32039 co-authored a technical study in 2020 with a Chinese Academy of Sciences group out of Hainan Province (Island) explaining a completed experiment on a new space-based satellite communications jamming method. The report cited other Chinese authors from PLA universities in the early 2000s who had described different methods, and said these previous methods no longer worked.

[xxxix] Units 63921-23 are subordinate to the Beijing Aerospace Flight Control Center (BACC), also known as Unit 63920.

[xl] Unit 61096 and Unit 63921 often work together, one instance of which is jointly authoring with State Owned Enterprises (SOEs) the national standard for in-orbit testing for GEO communications satellite payloads.

[xli] One list of Unit 32035's locations included Xi'an City in Sha'anxi Province, Jinan City in Shandong Province, Wulumuqi City in Xinjiang Province, Chuxiong City of Yunnan Province, Hangzhou City of Zhejiang Province, Chongqing Municipality, and Haidong City in Qinghai Province.

- Different authors from Unit 32039 also in 2020 discussed the implications of what they claimed are the U.S.'s ground, air, and space-based satellite communications jamming systems. They said that based on their review of the U.S. satellite jamming system, the Chinese "satellite communication countermeasures must realize the transition from signal layer countermeasures to information layer countermeasures as soon as possible, and focus on improving the internal countermeasure capability of the information network system. These determine the future development trend and direction of satellite communication jamming equipment and technology."[xlii]
- At a satellite communications conference in 2021, Unit 32039 presented a paper on an algorithm for determining how well a satellite is performing when it is getting jammed, which is most likely related to countermeasures for Chinese satellites experiencing jamming, but could be for assessing the successfulness of their own jamming of other satellites.
- The majority of 32039's patents are related to improving efficiency in the multiple user interface of the data relay satellite system. However, a different patent for testing on-orbit antennas tracking relay satellites could also enable flexibility in executing jamming.

Unit 63923, as mentioned above, is probably part of the former GAD Data Relay Control and Management Center, which had been subordinate to the Beijing Aerospace Flight Control Center (BACC), i.e. Unit 63920. Unit 63923 historically has focused on managing the human spaceflight program's access to Tianlian data relay satellites in GEO. Two of their patents are regarding GEO satellites near the end of their life, probably referring to the first Tianlian satellite launched in 2008. In 2020, Unit 63923 and parent Unit 63920 jointly authored a paper on their plan for ensuring consistent communications while one satellite was replaced. Another subordinate unit 63999, earlier in 2017, wrote on an orbital maneuver to remove the satellite to the graveyard orbit.[xliii]

Also as mentioned above, in January 2020, Unit 63923 renovated a location in Beijing's Mengtougou District, which could mean one of two things; they have merged with the new SSF Unit 32039 and somehow connected it to the new SSF Satellite Communications Main Station, or simply that they built a ground station at the newly renovated location. Alternatively, it is possible that Unit 63923 hasn't moved at all. Based on its 2021 patents, the unit continued to maintain its address in Haidian District with BACC.

This research found only one reason, but a seemingly significant reason, to include Unit 63923 in this report.

- Unit 63923, in 2021, received an invention patent for a method that could determine how "covert" satellite communications jamming attempts are discovered, attempts made by

[xlii] The exact Mandarin used is, "因此，卫星通信对抗必须及早实现从信号层对抗为主向信息层对抗为主的过渡转型，注重提高信息网络体系的内质对抗能力，这些决定了未来卫星通信干扰装备和技术的发展趋势和走向."

[xliii] Units 63921-23 are subordinate to the Beijing Aerospace Flight Control Center (BACC) with the unit number 63920.

either by the PLA or another country, so that the PLA can remediate the problem. [xliv] Technical experts are better placed to evaluate this patent's contents; this may be about countermeasures if the Chinese Space Station is jammed.

- As possible useful context, in 2021, Unit 63923 received a different invention patent for a system enabling a communications satellite to identify the ground location from which it was detecting interference. Importantly, the patent specifically referenced a ground station with aging equipment experiencing anomalies, not intentional jamming.

This single example of Unit 63923 should be viewed cautiously, but this report included it, as it may be related to earlier speculation that Shenzhou 6 tested a military reconnaissance payload in the early 2000s.

PLA SSF Units which have probably tested and participated in training with the PLA's experimental space-based satellite jamming satellite could include Unit 32032 and Unit 63888. Unit 32032 is subordinate to Base 36 in Kaifeng City, Henan Province.

- Unit 32032 received an invention patent in 2022 for assessing whether a satellite's electronic countermeasures functions were working and described these functions as orbital maneuvers, jamming, and electronic reconnaissance.
- Unit 32032 wrote on PLA lessons learned from the Russian LUCH-Olymp satellite in 2019, a satellite which is believed to be a strategic communications satellite with an electronic intelligence payload, according to western analysts.
- Unit 32032 wrote a detailed review of U.S. military satellites in 2019.
- Unit 32032 authored a study on natural and manmade causes of space-based electronic interference in 2019.

Unit 63888 is now under SSF Base 33 in Luoyang City, Henan Province, an important location for PLA joint electronic warfare weapons testing and training.[xlv] Unit 63888 in the early 2000s authored reports on not only ground-to-space satellite jamming, but also papers on space-based jamming and unmanned aerial vehicle-to-ground SATCOM jamming.

HYPOTHESIS OF PLA COMMAND AND CONTROL (C2) FOR SPACE-BASED REVERSIBLE ELECTRONIC JAMMING WEAPONS

In an attempt to bring more fidelity to China's counterspace C2, this section will attempt to answer two questions. First, "What is the most likely chain of command for the PLA to decide when to use space-based electronic satellite jamming weapons?" This first question relates to the above section, which attempts to answer, "Who in the PLA will use space-based electronic satellite jamming weapons?" The second question is, "In what way will the PLA be directed to use space-based electronic satellite jamming weapons?"

[xliv] The Mandarin characters used are "隐蔽."

[xlv] See this report's Chapter titled Directed Energy Counterspace Weapons and Chapter titled Terrestrially-Based Satellite Electronic Jamming Weapons for more information on SSF Base 33.

References to space-based satellite jamming were most common in a PLA text published just prior to the establishment of the SSF. The 2014 PLA National Defense University (NDU) Space Information Assisting-Support Operations text clarified that the CMC's Joint Operations Command Center (JOCC) decided space-based jamming operations at the time, and indicated that the weapon was primarily for a counterattack, not a preemptive attack. Based on the PLA unit numbers discussed above, the CMC JOCC would likely task the SSF's Space Systems Department (SSD) with carrying out related operations. A reputable netizen in 2018 judged that new SSF units in the 320XX block up to 32040 were probably SSD, with Network Systems Department (NSD) units starting at 32040. This assessment has largely held up.

Though it has been nearly a decade since the establishment of the SSF, the restructuring of space-based electronic intelligence, attack, and countermeasures under the SSD is probably still in transition, and may be riddled with challenges. Prior to the PLA's 2015 reform, electronic intelligence satellites were probably funded, tasked, and utilized by General Staff Department (GSD) units and the PLA services, while the functional orbital management was performed by General Armaments Department (GAD) units. Another complication is probably that the broad PLA attempt to emphasize network-electromagnetic warfare was originally led by the GSD.

This transition together with significant improvements in the People's Republic of China's (PRC's) data relay system indicates that the CMC is probably now more capable of quicker decision-making for orbital warfare like space-based jamming. However, it is worth noting that the 2014 PLA NDU Space Information Assisting-Support Operations book stated that, at the time, under special circumstances determined by the JOCC, space-based satellite jamming operators could take the initiative in an attack, if commanders determined that there was a large threat, defined as one that would "bear on the results of the entire joint IO [Information Operation], or when [we] are about to lose information dominance." This could hypothetically indicate the PLA would restructure their forces to protect SATCOM and empower the operators to counter jam, if they concluded the interference was intentional.

The remaining paragraphs of this chapter will attempt to answer the second question, "In what way will the PLA be directed to use space-based electronic satellite jamming weapons?" The 2014 PLA NDU Space Information Assisting-Support Operations book refers to multiple types of dedicated communications, radar, electro-optical, and navigation space-based jammers, but according to the information in this chapter, reversible SATCOM jamming is probably the most likely on-orbit weapon. The text states that,

> *"Under unified command by the Joint Operations Command's Information Operations Center… with the communication jamming satellites and the enemy communication satellites flying in the same orbits or different orbits, having the communication jamming satellites at proper time opportunities or in proper zones emit broadband electromagnetic jamming signals, to carry out blanket jamming of multiple channels of the enemy's spectrum."*

In fact, a joint GAD and GSD study in 2014 surveyed top PLA leaders, asking their opinion regarding the "most threatening military satellite," and the majority of them chose military communications satellites, probably for their fundamental role in enabling clarity of the mission.

Summary

In an effort to provide a benchmark on PLA counterspace weapons command and control (C2), this report established tailored research questions to re-examine the publicly available information. Each of the six chapters on a counterspace weapon attempts to answer these questions:

1. Who in the PLA will operate counterspace weapons in wartime?
2. Who will task the operators and how will the operators use counterspace weapons in wartime?

At a high level, this approach demonstrates the power of asking specific questions, and researching across the traditionally siloed space, PLA, and cybersecurity communities. This research approach further demonstrates the extent to which PLA counterspace C2 can be examined, modeled, and gamed at an unclassified level. More research is needed to further test the hypotheses in this report, as well as to provide continued updates on this evolving topic.

The dedicated chapters for each counterspace weapon should enable military planners, policy makers, and researchers to answer key questions for their respective professions. Military planners can use the discussion on counterspace weapon operators and rules of engagement to better collaborate with partners at an unclassified level for war games. Policymakers can better understand uncertainties regarding each weapon class to develop internal and external messaging and frameworks that position the U.S. for sustained leadership. Researchers can see where they can contribute to the discussion.

Re-examining publicly available information on the PLA's pre-reform debates regarding the organization of its space capabilities, illustrates that those debates were primarily about improving the PLA warfighters' access to a variety of space information, not about centralizing counterspace weapons. Given that the People's Republic of China (PRC) planned for the PLA reform, which included the establishment of the Strategic Support Force (SSF), to be completed by 2020, and it is nearly the end of yet another five-year plan in 2025, counterspace weapons might continue to be operated by multiple PLA services. Accepting this as true could enable many possible mental shifts, such as to consider what the SSF is freed up to do better, if they are not strapped will all counterspace operations.

As shown in each of the six chapters on counterspace weapons, while the operators are currently spread across the PLA, there is a consistent PLA message on rules of engagement for most weapons. The operators of ground-to-space satellite electronic jammers and DA-ASAT missiles are most likely spread across PLA services, but these weapons are tasked by the Central Military Commission (CMC), even though one is reversible and one is destructive. PLA decisions about the operators of directed energy counterspace weapons are ongoing because correct technology operation currently requires close collaboration with the developers; however, PLA books repeat that there will be at least mobile, reversible capabilities deployed to the Theater Commands (TCs). The SSF operates space-based experimental counterspace capabilities for reversible effects, which are centrally directed by the CMC. The operators and rules of engagement for offensive cyberattack counterspace weapons are the most uncertain, especially the role of merged electromagnetic spectrum and cyber capabilities. Noteworthy is that the PLA term for "network-electromagnetic spectrum" operations is in fact similar to some U.S. concepts, so

researchers can contribute more, to ease this uncertainty, in the future. Either the CMC or TCs can direct network-electromagnetic spectrum weapons, probably depending on if the effects can be limited to a target in theater.