Mitchell Institute for
Aerospace Studies
1501 Langston Blvd
Arlington, VA 22209
www.mitchellaerospacepower.org

March 21, 2024

Testimony before the U.S.-China Economic and Security Review Commission

Hearing on China's Evolving Counter Intervention Capabilities
and Implications for the U.S. and Indo-Pacific Allies and Partners

China C4ISR and Counter-Intervention

J. Michael Dahm
Senior Resident Fellow for Aerospace and China Studies
The Mitchell Institute for Aerospace Studies

Introduction

I appreciate the opportunity to speak to the Commission and provide this written testimony on what is perhaps the most consequential aspect of U.S. security competition with the People's Republic of China (PRC)—how the People's Liberation Army (PLA) seeks to control battlespace information to deter and potentially defeat a U.S. military intervention in a conflict. My assessment draws on published and previously unpublished independent, open-source research that I have conducted on China's C4ISR and counter-C4ISR strategies and capabilities.[a] This is not an exhaustive net assessment of U.S. and PRC capabilities but does highlight significant developments, illustrating trends I have observed over the two decades I have been examining the PLA and its warfighting capabilities. The analysis and opinions expressed in this testimony are my own—they do not necessarily reflect the views of the Mitchell Institute for Aerospace Studies, its sponsors, or any previous employer.

Executive Summary

- The PLA will likely initiate counter-intervention operations by conducting overwhelming kinetic and non-kinetic strikes on the sprawling C4ISR system-of-systems of the U.S. and its allies in order to achieve battlespace information dominance.

[a] "C4ISR" – command, control, communications, computers, intelligence, surveillance, and reconnaissance.

- Seizing battlespace information dominance will be one of, if not *the* most consequential struggles in any scenario where the PRC seeks to prevent the intervention of U.S. and allied military forces. In the minds of PLA decisionmakers, possessing superior C4ISR and counter-C4ISR capabilities to achieve information dominance early and throughout a conflict will be critical to combat success.

- The PLA's overarching design to achieve information dominance—informationized warfare—is not asymmetric nor is it uniquely Chinese. The PLA approach copies a well-established U.S. military playbook: Render enemies deaf, dumb, and blind, and then pick off disconnected enemy forces with long-range precision fires.

- The PLA has been reorganizing itself around its informationized warfare principles. The creation of operationally oriented theater commands, the joint operational command system, and the Strategic Support Force (SSF) among other C4ISR investments have significantly increased the PLA's ability to achieve battlespace information dominance and support counter-intervention operations.

- For the past quarter-century, the PLA has made substantial investments in diverse and resilient "information power" capabilities that will allow it to create important synergies among different C4ISR and counter-C4ISR capabilities. The cascading effects created by these capabilities will likely play a significant and potentially decisive role in counter-intervention.

- Within the Yellow Sea, East China Sea, and most of the South China Sea, the PLA probably begins a counter-intervention operation with information dominance and enjoys distinct advantages that may quickly translate into initial air and maritime dominance. In the initial stages of a counter-intervention operation, the PLA may be able to establish localized information, air, and maritime dominance in areas out to the Second Island Chain that would, if necessary, allow the PLA to launch strikes on U.S. bases and deployed forces.
    - The PLA enjoys a "home field advantage" in counter-intervention operations. These advantages extend beyond basing and logistics to its fortress-like C4ISR.

- The PLA has seen significant growth in space based C4ISR capabilities that will likely create pronounced challenges for U.S. and allied forces attempting to avoid detection and targeting in a PLA counter-intervention operation.
    - Over the past five years, the number of PLA ISR satellites in geostationary orbit (GEO) has doubled while the number of PLA ISR satellites in low Earth orbit (LEO) has tripled.

- The PLA is an electronic warfare juggernaut. The PLA possesses both the technological capabilities and significant electronic warfare capacities to conduct significant offensive and defensive electromagnetic spectrum operations that will enable, if not ensure initial PLA information dominance in a counter-intervention operation.

Summary of Recommendations

U.S. policymakers may wish to consider the following recommendations, which are explained in detail at the end of this report.

- Conduct a comprehensive net assessment of U.S. and allied C4ISR and counter-C4ISR capabilities in a large-scale conflict with the PLA.
- Engage the U.S. military regarding future C4ISR strategies and the need to emphasize more defensive capabilities including significant redundancy within the U.S. C4ISR system-of-systems.
- Invest in significant counter-reconnaissance capabilities to defeat PLA ISR that includes physical, virtual, and electromagnetic camouflage, concealment, and deception measures.
- Invest in robust, redundant, and resilient coalition C4ISR links and networks to increase combat interoperability among critical allies and partners, denying the PLA battlespace information dominance that might separate the U.S. from a coalition.
- Fund additional U.S. Intelligence Community capabilities to analyze current and future PLA counter-C4ISR capabilities and strategies.
- Publish a detailed open-source assessment of PLA C4ISR and counter-C4ISR threats to U.S. and allied military forces to increase public and policymaker awareness of these challenges.
- Fund additional U.S. Intelligence Community capabilities to analyze current and future PLA electromagnetic spectrum operations capabilities and strategies.
- Publish a detailed open-source assessment of PLA electronic warfare capabilities and threats to U.S. and allied military forces, again, to increase public and policymaker awareness of these challenges.

This report begins with a description of PLA informationized warfare concepts and principles and how they apply to counter-intervention operations. This is followed by an examination of recent organizational reforms in PLA command structure and their implications for counter-intervention. There is also a brief discussion of how C4ISR and counter-C4ISR elements may interact to create information dominance through synergistic effects. Several examples of PLA C4ISR capabilities illustrate the PLA's ability to combine different intelligence sources to locate, track, and target U.S. and allied military forces in different domains. Examples of counter-C4ISR capabilities with special attention to electronic warfare capabilities demonstrate direct challenges to U.S. and allied C4ISR. Finally, a number of recommendations are offered for the Commission's consideration.

Informationized Warfare and Counter-Intervention

- **The PLA will likely initiate counter-intervention operations by conducting overwhelming kinetic and non-kinetic strikes on the sprawling C4ISR system-of-systems of the U.S. and its allies in order to achieve battlespace information dominance.**
- **Seizing battlespace information dominance will be one of, if not *the* most consequential struggles in any scenario where the PRC seeks to prevent the intervention of U.S. and allied military forces. In the minds of PLA decisionmakers, possessing superior C4ISR and counter-C4ISR capabilities to achieve information dominance early and throughout a conflict will be critical to combat success.**

The PLA has explicitly described their designs to defeat a "strong enemy" like the United States military and counter U.S. intervention in a conflict—attack the C4ISR system-of-systems of the U.S. and its allies in order to achieve battlespace information dominance. With the PLA's redundant and resilient C4ISR still functional, battlespace information dominance enables the PLA to then achieve air and maritime dominance, potentially paralyzing a U.S. and allied advance. This overarching strategy is not asymmetric nor is it uniquely Chinese. The PLA approach copies a well-established U.S. military playbook: Render enemies deaf, dumb, and blind, and then pick off disconnected enemy forces with long-range precision fires.

The PLA's priority to achieve and sustain battlespace information dominance as a tactical, operational, and strategic imperative cannot be overstated. Any force that engages in a conflict with the PLA that fails to recognize and understand the central role of battlespace information dominance to PLA operational design risks a potentially disastrous outcome.

What is C4ISR?

C4ISR is an acronym that has traditionally referred to "command, control, communications, computers, intelligence, surveillance, and reconnaissance."[1] C4ISR may be thought of as a collection of individual systems that align to the seven named categories. This leads to any number of variations of "C4ISR" as different institutional champions append additional categories to the original seven (e.g. C5ISR-T adding another 'C' for "cyber" or "cyber-defense," and a 'T' for "targeting").[2] However, C4ISR is more than simply a description of different categories of systems. C4ISR should be considered an amalgamation of systems—a complex system-of-systems that enables an information-related purpose—military decision advantage.[3]

For the purposes of this report, C4ISR refers generally to a complex battlespace information system-of-systems that provides relevant information to a commander or weapons system operator, affords decision advantage, and enables military action. A C4ISR system-of-systems consists of command-and-control organizations and systems, communications and computer networks, and intelligence collection systems. Counter-C4ISR refers to a system-of-systems designed to confuse, disrupt, or destroy adversary C4ISR and deny an adversary commander decision advantage thereby inhibiting or preventing adversary action. A counter-C4ISR system-of-systems may include camouflage, denial, and deception activities, as well as electronic warfare, cyber-attack and defense, and the physical destruction of adversary networks, ISR platforms, and command nodes.

This analysis is scoped to battlespace information dominance and C4ISR. Western assessments of all things "information" and "military" too often confuse PLA informationized warfare concepts with what the PLA might term "political warfare" or "three warfares"—public opinion warfare, psychological warfare, and legal warfare. Assessments that indiscriminately mix everything from electronic warfare to malign influence on social media obscure PLA efforts to generate information power in the operational battlespace. Informationized warfare is about what a commander or weapons system operator sees, hears, and perceives in combat. It is about how battlespace data is collected and processed, how decisions are made, how actions are directed, and how data passes from "sensor-to-shooter."

Informationized Warfare and Force Employment

How the PLA will employ military force against an adversary in a counter-intervention scenario may be understood by examining the PLA's overarching approach to multidomain integrated joint operations and how their forces will likely employ different elements of combat power in any given large-scale military operation.

PLA strategic doctrine and other writings consider information power (信息力) or information dominance (制信息权)[b] as the key to controlling the battlespace and operational initiative. As early as 2002, Central Military Commission (CMC), Chairman Jiang Zemin observed:

> *"Informationization is the core of a new military transformation… information warfare links all combat processes and permeates each warfare domain. Competition for information superiority has become the focus of war. Information dominance is the key to seizing air and maritime dominance and control in other combat domains."*[4]

For over twenty years, the PLA has built upon this tenet—developing and refining ideas about informationized warfare.[5] Information power (信息力) is the operational expression of informationized warfare. It is the first among the five "Basic Elements of Campaign Power," in the seminal PLA doctrinal text, *Science of Campaigns*. Table 1 lists information power and the other elements of campaign power in priority order.

Table 1. Basic Elements of Campaign Power[6]

English Term	Chinese Term
Basic elements of campaign power	战役力量的基本要素
1. Information power	信息力
2. Firepower	火力
3. Maneuver power	机动力
4. Assault power	突击力
5. Protection power	防护力

[b] 制信息权 is translated in this report as "information dominance" but could also be translated as "information control." The characters might be translated more literally as "the power or authority to control information."

The 2006 *Science of Campaigns* and other more recent PLA writings note that information power does not stand alone; all the elements are necessary and complementary, applied in varying proportions depending on particular objectives. However, Chinese military doctrine and writings up to the present day indicate that that *all* the resources of war—that is, all the capabilities and materiel represented by the other elements—rely, first and foremost, on information power.[7]

The 2013 *Science of Military Strategy* introduced the concept of the "three dominances" (三权) – information, air, and maritime dominance. PLA theory holds that information dominance is critical to success in the modern battlespace. Air and maritime dominance cannot be achieved without first achieving battlespace information dominance according to PLA military doctrine.[8]

Current guidance from China's CMC in its Military Strategic Guidelines identifies informationized warfare as the prevailing "form of war" (战争形态). Just as the basic elements of campaign power are considered an objective list, the PLA's "form of war" is an objective assessment of the character of warfare in any given period that applies to all military operations, both friendly and enemy.

It is important not to confuse informationized warfare with the *process* of informationization, which is the transformation of any endeavor, from accounting to war, through the application of information technology. Informationized warfare, on the other hand, addresses the character of war and how wars are fought and won. The U.S. Department of Defense (DoD) annual report to Congress on the PLA, the 2023 *China Military Power Report*, states:

> *"PRC military writings describe informatized warfare as the use of information technology to create an operational system-of-systems, which would enable the PLA to acquire, transmit, process and use information during a conflict to conduct integrated joint military operations across the ground, maritime, air, space, cyberspace, and electromagnetic spectrum domains."*[9]

This statement is somewhat misleading. It accurately describes the *process* of informationization and the transformational goals for PLA C4ISR using information technology. It does not, however, accurately describe how the PLA believes informationized warfare has transformed warfighting or capture the depth and breadth of PLA informationized warfare concepts.

PLA ideas about informationized warfare were born out of PLA observations of modern wars, especially the 1991 Gulf War. PLA scholars drew heavily on concepts like "net-centric warfare" advanced by the U.S. military in the 1990s. The views of PLA authors writing on informationized warfare in the early 2000s were not entirely derivative of U.S. military doctrine. They incorporated many Western, Soviet, and Chinese information warfare concepts and ideas.

In the late-1990s and early-2000s, prominent Chinese military figures emerged to assess and define the new informationized form of war. One such figure was Major General Dai Qingmin (戴清民).[10] Often credited as the father of a core Chinese operational concept, "integrated

network electronic warfare (INEW)," Dai Qingmin's role in the development of informationized warfare is often overlooked. Beginning in the late 1990s, Dai wrote over sixty articles on informationized warfare and authored or coauthored a dozen books on the subject. Over two decades later, Chinese informationized warfare principles still clearly reflect the writings of Dai and his contemporaries.

Informationized warfare principles that are integral to current Chinese military doctrine, strategy, and operations include the following broad concepts:

- Information dominance is necessary to seize and maintain battlefield initiative.[11]
- "Active offense" is the key to seizing information dominance and the initiative in battle.[12]
- Information dominance is a prerequisite for air and maritime dominance.[13]
- Informationized warfare concepts are essential for success in large-scale joint operations.
- Individual elements of a combat system are networked and linked as an organic whole—a system-of-systems—through multidomain information perception, real-time information transmission, and intelligent information processing.[14]
    - Therefore, informationized warfare is inherently system-of-systems versus system-of-systems confrontation (体系与体系的对抗).[15]
- C4ISR systems-of-systems are critical friendly and enemy centers of gravity.[16]
    - C4ISR must be diverse and redundant since networks and myriad linked elements will be targeted for interference and destruction.
    - In the defense, diversity and redundancy in one's own C4ISR network is necessary to preserve friendly access to information.
    - In the attack, no single combat measure will paralyze an informationized system-of-systems; coordinated strikes must take place across adversary C4ISR.[17]

"Informationized warfare" (信息化作战) may be translated literally as "warfare transformed by information."[c] If the industrial age resulted in warfare transformed by machines (mechanized warfare), the information age yields warfare transformed by information (informationized warfare). Future warfare may be transformed further by artificial intelligence and intelligent systems (intelligentized warfare, 智能化作战).

Informationized warfare does not exclude contests of materiel power. The authoritative 2020 PRC National Defense University text, *Science of Military Strategy*, observes that information dominance is facilitated through electronic warfare, network warfare, *and* physical destruction. Informationized warfare principles manifest information-centric operations in which both non-kinetic *and* kinetic strikes are used to ensure friendly control of battlespace information while

[c] 信息化作战 may also be rendered "informatized warfare."

targeting, destroying, and paralyzing an enemy combat information system.[18] The ultimate goal is to ensure PLA decision-making advantages and operational advantages through information dominance in a paradigm where "information flow dominates materiel and energy flows."[19]

Information dominance remains a central feature of PLA operational concepts.[20] Even as the PLA's "basic form of operations" (基本作战形式) has evolved over the past quarter-century from "joint operations" (联合作战) to "integrated joint operations" (一体化联合作战) to "multi-domain integrated joint operations" (多域一体化联合作战), the overarching principles of informationized warfare have prevailed. The C4ISR system-of-systems—fusing command and control, sensing, communication, precision strikes, support systems, and other capabilities into a coherent combat system—is the core of multi-domain integrated joint operations.[21]

Emerging PLA concepts of intelligentized warfare—the transformation of warfare by artificial intelligence (AI) and intelligent systems—is still fundamentally rooted in informationized warfare principles and battlespace information control. Some PLA sources are beginning to discuss intelligentized warfare as an independent, aspirational stage of future military development. Top-level PRC government guidance directs the PLA to simultaneously pursue the integrated development of mechanized, informationized, and intelligentized capabilities.[22]

That said, many Chinese military scholars regard intelligentized warfare as highly evolved informationized warfare and acknowledge the inextricable link between the two epochs of military development.[23] The reality is that AI will have significant impacts on *all* elements of combat power and military capabilities from C4ISR to firepower to maneuver to logistics. AI will enhance or, perhaps, even revolutionize the speed, accuracy, and volume of military actions and decision making. However, retaining friendly access to battlespace information while denying battlespace information to enemy forces will remain central to decision advantage even as AI-enabled networks and weapons systems become ascendant.

PLA Organizational C2 for Counter-Intervention

- **Since 2015, the PLA has been reorganizing around its informationized warfare principles. The creation of operationally oriented theater commands, the joint operational command system, and the Strategic Support Force (SSF) among other C4ISR investments have significantly increased the PLA's ability to achieve battlespace information dominance and support counter-intervention operations.**

Understanding the underlying organization of PLA command-and-control (C2) provides a foundation upon which to assess the PLA's expansive C4ISR system-of-systems. In 2015, the PLA created the Strategic Support Force, a military service-level organization that has overarching responsibility for PLA C4ISR. The PLA took several other significant steps to reorganize and streamline national- and theater-level C2 to facilitate integrated joint operations. This reorganization has also enabled more effective counter-intervention operations.

The PRC's 2015 military reforms, commonly referred to as "above-the-neck" reforms, fundamentally reoriented the PLA toward more joint, offensive capabilities.[d] The reforms enable the PLA to engage in the types of "active offense" (积极进攻) necessary to seize information dominance and gain operational initiative in military conflicts, including counter-intervention operations. The above-the-neck reforms replaced Military Regions (MRs), which were optimized to defend the PRC from attack and invasion, with five geographically oriented Theater Commands (TCs) that will allow for more focus on PLA offensive operations.

Joint Operational Command System Development

- **The PLA's joint operational command system was a significant reform that should improve the PLA's ability to conduct offensively oriented integrated joint operations and enable more effective counter-intervention operations.**

The 2015 reforms subordinated operational forces that might engage in counter-intervention against the U.S. or its allies to the PLA's "joint operational command system" (联合作战指挥体系).[24] Operational forces were previously under the control of PLA military service commanders. The PRC's Central Military Commission (CMC) also abolished the PLA General Staff Department, established a CMC Joint Staff Department, and created a national-level joint operations command center (JOCC) (联合作战指挥中心) to oversee theater operations as well as national-level, strategic operations. The CMC JOCC supervises five "theater joint operations command centers" (T-JOCC) (战区联合作战指挥中心) that are responsible for commanding operations in each of the TCs.[25]

What is not clear from available open-sources is how far from the Chinese mainland a TC's responsibility for counter-intervention operations might extend. In 2019, the Southern Theater Command T-JOCC probably controlled a PLA Navy surface ship task force far into the Central Pacific Ocean, beyond Guam and the Second Island Chain.[26] While this was ostensibly a training exercise, a T-JOCC controlling military forces so far from China's shores may indicate T-JOCC responsibility for coordinating counter-intervention operations at extended ranges. Over the past several years, PLA navy and air forces have operated with some frequency outside the First Island Chain in the Philippine Sea. In 2023, PLA Navy carrier strike groups operated within several hundred miles of Guam. There are no outward indications in open-source reporting that these operations were controlled directly by the CMC JOCC. These naval formations were probably controlled by the Northern, Eastern, or Southern Theater T-JOCCs.[27]

Within the T-JOCCs, different warfighting domain functions are organized into "command sub-centers" (指挥分中心), also referred to as "operational sub-centers" (作战分中心). The T-JOCC operational sub-centers are the "land operations sub-center" (LOSC) (陆上作战分中心), "maritime operations sub-center" (MOSC) (海上作战分中心), "air operations sub-center"

[d] The 2015-16 "Above-the-neck" reforms focused on top-level command reorganization, the "head" of the PLA. 2017-2019 "below-the-neck" reforms focused on reorganization within the "body" of the PLA.

(AOSC) (空中作战分中心), and "conventional missile operations sub-center" (CMOSC) (常导作战分中心).[28] The top-level theater command organization is depicted in Figure 1.

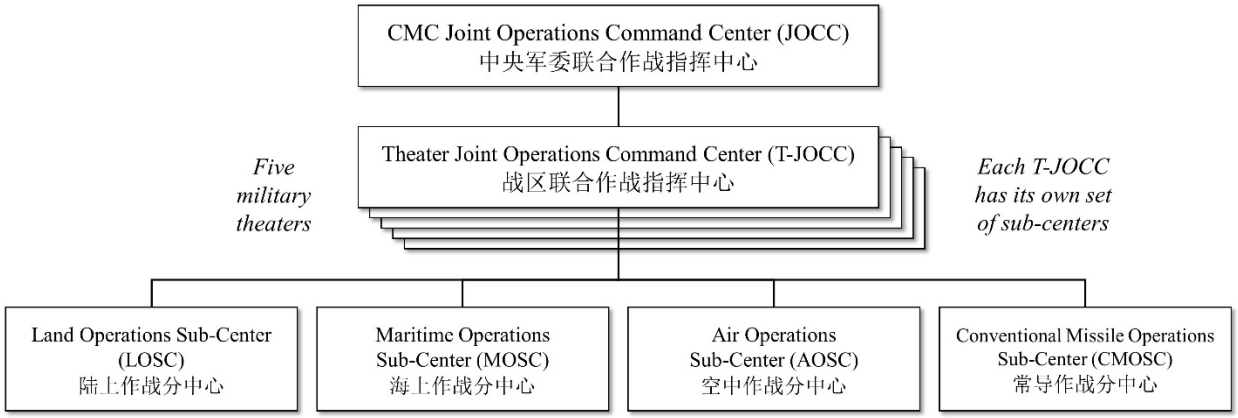

Figure 1. Theater Joint Operations Command System Organization.[29]

The sub-centers clearly align to the PLA military services—the PLA Army (PLAA), PLA Navy (PLAN), PLA Air Force (PLAAF) and the PLA Rocket Force (PLARF) respectively. The MOSC and the AOSC probably perform functions similar to the U.S. Navy's maritime operations centers (MOCs) and the U.S. Air Force's air operations centers (AOCs). Within each theater, the LOSC is probably led and managed by the TC Army commander, the MOSC is led by the TC Navy commander (for those coastal TCs with PLAN fleets), and the AOSC is led by the TC Air Force commander. It is not clear which PLARF senior officer might lead the theater Conventional Missile Operations Sub-Center since PLARF bases do not align with theater command boundaries.[30] "Dual-hatting" the theater service commander as both a "force provider" and "operational commander" again appears similar to U.S. military organization. For example, the commander, U.S. Pacific Air Forces is a U.S. Air Force major command and force provider while simultaneously serving as the air component commander for the U.S. Indo-Pacific Command theater.

The T-JOCCs are currently untested in real-world operations and would probably face significant challenges in conducting offensive action against a neighboring country while simultaneously coordinating and conducting counter-intervention operations against the U.S. and its allies. Open-source information does not currently provide many insights about how well the PLA's new C2 system is functioning or whether it has met with success or significant challenges in large-scale PLA exercises.

PLA Air & Air Defense Reorganization

- **A recent reorganization of PLA command has probably closed significant gaps and seams in air and air defense coverage but may have created new challenges and vulnerabilities related to counter-intervention.**

In 2023, the PLA took a major step to streamline and improve PLA air and air defense capabilities that might be applied in counter-intervention operations. Most land-based combat aircraft and air defense systems have apparently been consolidated under PLAAF command. More significantly, the consolidation improves the T-JOCC AOSC's ability to command operations in the air domain. The reorganization also probably improves the PLAAF's ability to support the PLA joint force and project airpower within East Asia.

Since the 1950s, the PLAN had always maintained a separate naval air force, the PLA Naval Aviation Force (PLANAF). The PLANAF was responsible for overwater intercepts, maritime strikes with bombers or fighter-bombers, and air defense of PLAN fleet concentration areas. Air defense forces included PLAN-owned and operated land-based radars and long-range surface-to-air missile systems like the HQ-9. The PLAAF was historically responsible for intercepts over the Chinese mainland (or just off the coast), air-to-ground strikes, as well as air and missile defense in parts of China not covered by PLAN air defense.

In early 2023, the PLAN transferred over 150 combat aircraft, ten airfields, three land-based air defense battalions, and several radar brigades to the PLAAF. The move consolidates virtually all PLA land-based combat airpower—fighters, bombers, air defense radars, and surface-to-air missile systems—under the control of the PLAAF. Moving PLAN combat aircraft to the PLAAF also means the PLAAF has assumed responsibility for airborne maritime strike operations with control of all land-based H-6 bombers and fighter-bombers like the JH-7 and J-16.[31]

The 2023 transfers from the PLAN to the PLAAF were likely inspired by the concentration of air operations command and control in the T-JOCC Air Operations Sub-Center. Consolidating land-based air defenses under PLAAF/AOSC command effectively closed any seams and vulnerabilities that had previously existed between PLAAF and PLAN areas of air defense responsibility. The consolidation potentially creates new seams and vulnerabilities. The PLAN and the MOSC must now rely almost entirely on the PLAAF and the AOSC to meet its air defense and air strike requirements. This dependency will persist at least for the next decade until the PLAN can generate sufficient airpower from its aircraft carriers.

PLA Strategic Support Force Development

- **The creation of the PLA Strategic Support Force appears to have had a seismic impact on the development of PLA C4ISR and electronic warfare capabilities. The SSF is now responsible for the majority of the PLA's joint C4ISR architecture as well as several counter-C4ISR capabilities.**

The 2015 "above-the-neck" reforms created the Strategic Support Force (SSF) (战略支援部队) from elements of the former PLA General Staff Department (GSD) and General Armaments Department (GAD). The SSF controls and manages joint military communications and computer systems, offensive and defensive military cyber operations, electronic warfare, space-based ISR,

and both terrestrial and on-orbit counter-space capabilities. The SSF also appears to have a limited role in military psychological operations against Taiwan.

The scale of PLA's SSF experiment has been massive. One public U.S. estimate in 2009 put the size of the former GSD 3rd Department (3PLA) at over 130,000 personnel.[32] The SSF combined personnel from 3PLA as well as the GSD 4th Department (4PLA) and some elements of the 2nd Department (2PLA), space-related forces, and communications troops. Accounting for some growth, the SSF may currently have between 200,000 and 250,000 personnel. Given the two-million PLA personnel, the SSF only represents between 10-12 percent of the force. Still, if the numbers are accurate, it means the SSF by itself is larger than almost every NATO military and close to the size of the entire Japan Self Defense Force. However, simply reorganizing personnel—even hundreds of thousands of personnel—into a single organization does not necessarily translate into operational proficiency or an ability to overcome institutional rivalries from the other military services.

Many popular assessments of the SSF tend to focus almost exclusively on the SSF's role in offensive cyber activity for both espionage and attack. Outsized interest in narrow SSF cyber capabilities has served to undermine a broader understanding of the SSF's fundamental responsibilities for developing and operating the PLA's extensive C4ISR system-of-systems and attendant counter-C4ISR capabilities, which includes offensive and defensive cyber capabilities.

The creation of the SSF consolidated many military information power capabilities and reflects the PLA's focus on informationized warfare and its strategic and operational imperative to achieve battlespace information dominance. The SSF is directly subordinate to the CMC Joint Staff with the same command grade as the TCs and military services (PLAA, PLAN, PLAAF, and PLARF). The SSF appears to be a "force provider" of information power capabilities for the theaters, but also appears to retain direct operational control of certain cross-cutting and strategic capabilities under the supervision of the Joint Staff.

Space Systems Department (SSD). The SSF Space Systems Department (航天系统部) is responsible for virtually all PLA space operations including space launch operations; telemetry, tracking, and control (TT&C) of satellites and other space vehicles; space-based management and control of PLA C4ISR; and select counterspace capabilities, especially on-orbit capabilities. Relative to PLA C4ISR, counter-C4ISR and counter-intervention operations, the most important SSD organizations are probably the 26th Base and the 37th Base, as well as several independent SSD Bureaus.

The 26th Testing and Training Base (第 26 试验训练基地), also known as the Xi'an Satellite Control Center (XSCC) (西安卫星测控中心), is the core of China's space TT&C network. Tasking for an ISR satellite to locate and track mobile or fixed targets very likely runs through the XSCC. Although the XSCC hub is in Xi'an, the XSCC is not a "center" as much as a nation-wide network of TT&C stations.[33] If the 26th base is responsible for C3 and tasking of PLA space assets, the 37th Base is responsible for space situational awareness (SSA) and ISR of adversary

space assets. The 37th Base, possibly known as the Monitoring and Early Warning Base, probably has responsibility for foreign space object identification, tracking, and analysis.[34]

The SSD Aerospace Reconnaissance Bureau (ARB) (航天侦察局) is responsible for analysis of space-based ISR.[35] The ARB was apparently moved to the SSF from GSD military intelligence (2PLA) indicating the ARB may focus on imagery intelligence. Space-based signals intelligence (SIGINT) may flow to the NSF's technical reconnaissance bureaus (TRBs) to be fused with other, terrestrial SIGINT sources for analysis. It is possible the ARB also acts as that fusion center for the different intelligence feeds.

The SSD's Satellite Communications Main Station (卫星通信总站) is responsible for space-based communications and data relay.[36] The SSD's space communications architecture would necessarily need to work closely with the SSF Information Communication Base (ICB) and its management of terrestrial communications. The SSD's Satellite Positioning Main Station (卫星定位总站) is responsible for the military operation and use of China's *Beidou* global positioning satellite system.[37]

Network Systems Department (NSD). The SSF Network Systems Department (网络系统部) is responsible for PLA strategic and joint SIGINT capabilities, which includes military cyber capabilities. The NSD is also responsible for strategic and joint electromagnetic spectrum operations (EMSO). The NSD reportedly inherited the PLA's 311 Base, which is responsible for psychological operations against Taiwan and generating propaganda, influencing public opinion on the island to support PLA objectives.[38]

Virtually every organizational element of the NSD likely plays an important role in counter-intervention operations against the U.S., its allies, and partners. The NSD's extensive SIGINT capabilities likely include signals intelligence (SIGINT)—electronic intelligence (ELINT) and communications intelligence (COMINT)—to monitor and intercept signals both terrestrially and in space. There are also indications that the NSD may be responsible for monitoring activity on international submarine fiber-optic cables where they land in China.[39]

SSF NSD inherited its SIGINT capabilities from the former 3PLA. 3PLA had been organized into twelve technical reconnaissance bureaus (TRB), a structure that most open-source analysts suspect was exported to the SSF intact. The most infamous of these TRBs was the 2nd Bureau that has been identified as responsible for a large share of PLA cyber hacking and espionage.

There is ample evidence that the twelve TRBs, including the 2nd Bureau, were responsible for SIGINT missions and capabilities well beyond computer network operations (CNO). A report prepared for the USCC in 2009 stated:

> *"While the TRB appear largely focused on traditional SIGINT missions, oblique references to staff from these units conducting advanced research on information security*

or possibly related topics suggests a possible CNO or EW role that augments their SIGINT collection mission."[40]

The SSF NSD operates a number of independent electronic warfare (EW) units, often identified as electromagnetic countermeasures (ECM) units. The PLAN, PLAAF, and PLARF all operate ECM brigades that support their respective service forces while PLAA ECM is incorporated within PLAA maneuver elements. NSD ECM brigades, inherited from the former 4PLA, are probably responsible for strategic air defense and counter-space electronic warfare (principally ground-based monitoring and jamming of satellite communications).

Information Communication Base (ICB). The PLA 2017-2019 "below-the-neck" reforms transferred what is now known as the "Information Communication Base" (ICB) (信息通信基地) to the SSF.[e] The move further consolidates the SSF's responsibility for PLA C4ISR. The ICB is responsible for national and joint military communication networks. The ICB is also probably responsible for the PLA's enterprise-level computer architecture, the integrated command platform (一体化指挥平台). The ICB may also hold overall responsibility for cyber defense and information security of PLA networks through its Network Security and Defense Center (网络安防中心).[41] ICB units appear to be responsible for maintaining and repairing the National Defense Communication Network (NDCN) (国防通讯网) built on the PRC's defense fiber-optic cable (国防光缆) backbone network.[42]

Immediately following the 2015 "above-the-neck" reorganization, the ICB, also known as the 61001 Unit (61001 部队), was subordinated to the CMC Joint Staff Department. At that time, the organization was known as the Information Assurance Base (IAB) (信息保障基地), also translated as the "Information Support Base."[43] Probably in 2017 or 2018, as part of the PLA's "below-the-neck" reforms, the IAB was transferred to the SSF and renamed the Information Communication Base.[44] The ICB appears to control a number of information communication brigades (信息通信旅) (possibly also referred to as local "information communication bases") that are geographically distributed and assigned to support individual theater commands. ICB information communication brigades appear to be further organized into battalions and then companies mirroring PLA ground forces organization.[45]

The Information Communication Base joins the SSF SSD and NSD possibly as the third branch of the Strategic Support Force.[46] This preliminary assessment is based on the ICB retaining its "61001" military unit cover designator (MUCD) and the somewhat tenuous observation that no interim command organization is ever mentioned in official PLA media that highlights ICBs subordination to the SSF.[47] That said, it is certainly possible that the ICB belongs to the SSF Network Systems Department.[48] In any case, it is unlikely that the ICB is co-equal with the SSD

[e] "Base" (基地) in "Information Communication Base" may synonymously be thought of as an organization – ***the*** Information Communication Base (organization) or, in some contexts, a place – ***an*** information communication base (a communication base subordinate to the ICB or one of the services).

or NSD. The SSF departments have been assessed to be deputy theater grade commands with their own subordinate bases. According to PLA organizational convention, a “base" (基地), is normally a corps grade or deputy corps grade command. An assessed SSF organizational chart appears in Figure 2. The working relationship between NSD theater bases and ICB theater information communications brigades/bases is currently unclear.

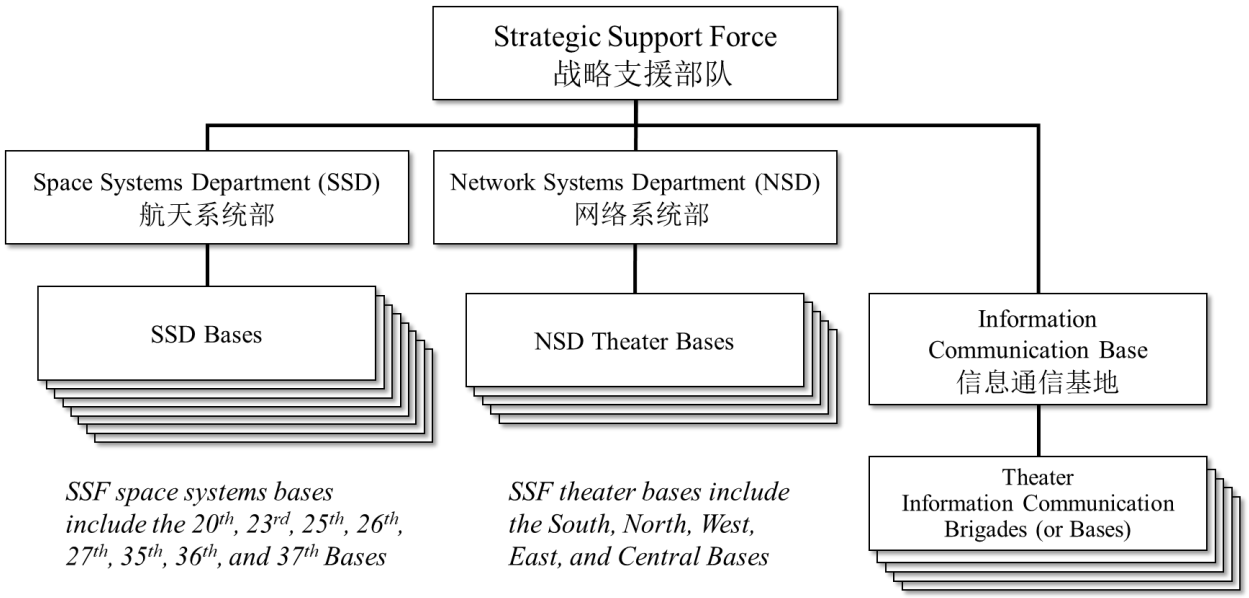

Figure 2. Assessed 2024 Strategic Support Force Organization.

SSF Support to Theater Operations. Theater-aligned SSF bases, possibly called “Technical Reconnaissance Bases,” may be subordinate to NSD or SSF headquarters. These SSF bases probably provide direct operational support to the five TCs and their T-JOCCs. Public references to SSF theater bases are normally prefaced with “Strategic Support Force” (战略支援部队) adding the term Eastern Base (东部基地), Southern Base (南部基地), Western Base (西部基地), Northern Base (北部基地), and Central Base (中部基地) aligning to their respective theater command.[49]

Figure 3 depicts a notional SSF theater support arrangement in which the SSF theater bases act as hubs for intelligence, cyber, and ECM. In this construct, the SSF theater bases draw information out of the SSF SIGINT and space ISR architecture and, conversely, convey theater tasking and requests for support back to the SSF. This diagram postulates either an administrative or operational relationship between the SSF theater bases and the theater information communication brigades. In any case, this arrangement is simply a logical extrapolation and would require research and further analysis to confirm.

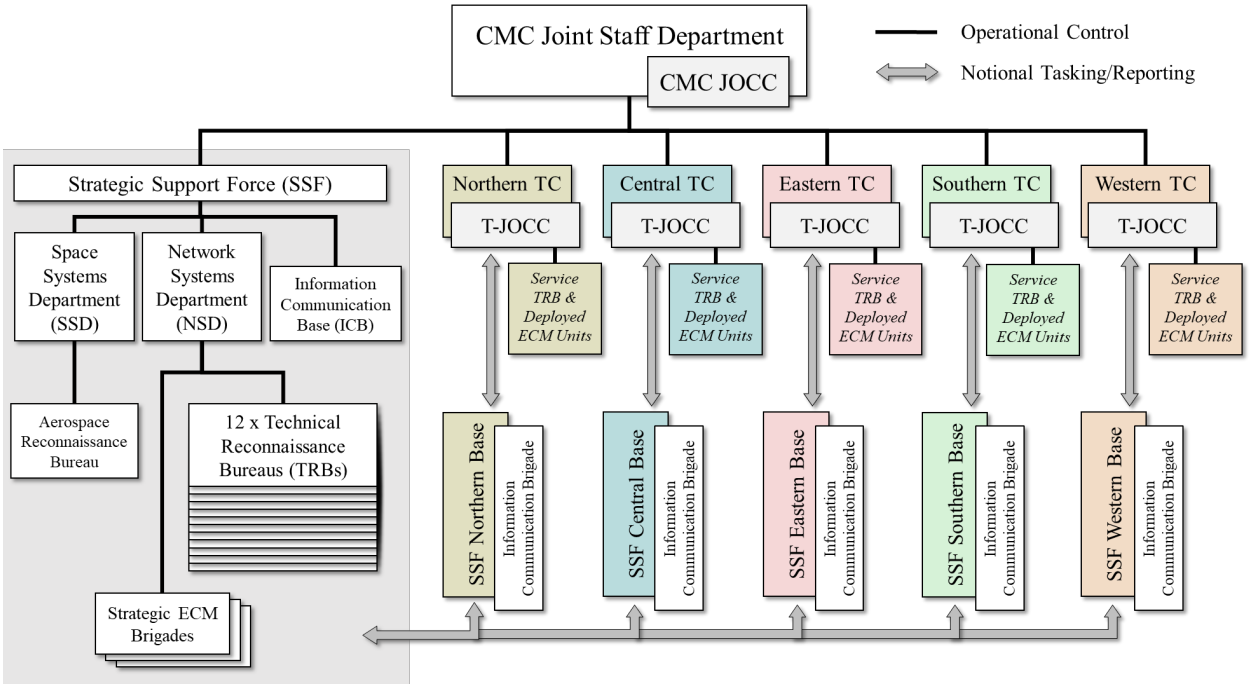

Figure 3. Notional Organization for SSF Theater Support.[50]

This notional SSF theater support arrangement raises questions about roles the SSF may play in the T-JOCC. How, for example, does the T-JOCC deconflict tasking and actions of service TRB and ECM forces with those of the SSF? There is a possibility that the SSF theater base or other SSF staff might be integrated into the T-JOCC to command an independent information operations sub-center (IOSC) alongside the land, maritime, air, and conventional missile operations sub-centers. The presence of an IOSC is purely speculative. How the PLA manages information warfare within the T-JOCC would also require further research and analysis.

Eight years after the creation of the SSF, the organization is probably just beginning to realize many of the information power goals it was given. The Strategic Support Force, as managers and operators of core components of the PLA C4ISR system-of-systems will have a key role in generating battlespace information dominance and will have a significant impact on any PLA counter-intervention operation.

C4ISR & Counter-C4ISR Synergies

- **For the past quarter-century, the PLA has made substantial investments in diverse and resilient "information power" capabilities that will allow it to create important synergies among different C4ISR and counter-C4ISR capabilities. The cascading effects created by these capabilities will likely play a significant and potentially decisive role in counter-intervention.**

Figure 4 offers a framework that demonstrates how different C4ISR and counter-C4ISR information power elements may interact to create information dominance through synergistic effects.

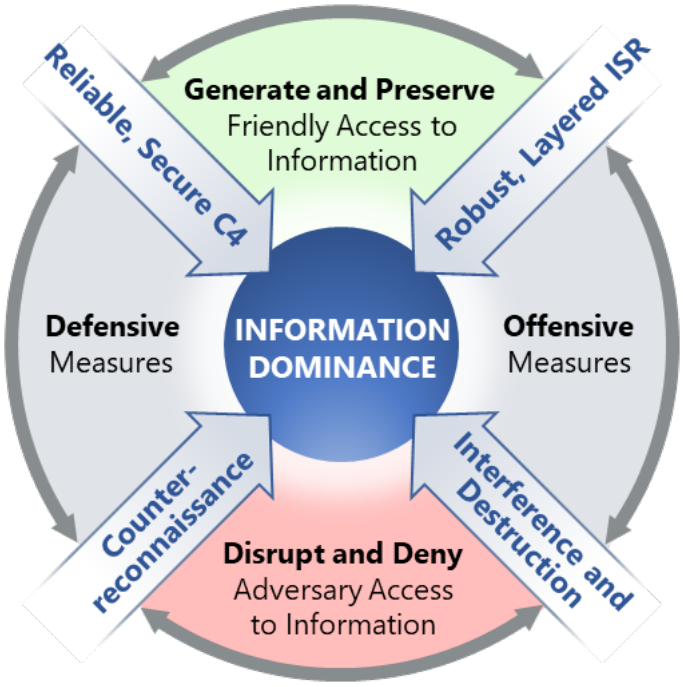

Figure 4. Information Power Capabilities Conceptual Framework.[51]

The diagram shows four information power categories—C4, ISR, interference and destruction, and counter-reconnaissance oriented toward information dominance. Interference and destruction may include kinetic actions, such as airstrikes, or non-kinetic actions that might be reversible or destructive such as temporary electronic interference or a cyber-attack that disables a system. Counter-reconnaissance may include camouflage, concealment, deception, decoys, and other measures to defeat adversary ISR. These categories are arranged into offensive or defensive measures that either preserve friendly access to information or deny an adversary access to information. The combination of different types of capabilities and the synergistic effects they generate will yield greater battlespace information dominance than any one capability employed in isolation. In an operational battlespace, the different categories of capabilities work together to achieve information dominance and deliver combat effects.

In the absence of counter-reconnaissance, interference, and destruction, two opposing C4ISR system-of-systems might compete with one another in terms of how fast one or the other system enables decisions or closes a kill chain. That is, the advantage may go to the C4ISR system that can spin the "OODA loop" faster than one's adversary.[f]

[f] OODA – Observe, orient, decide, act.

In any confrontation between the U.S. military and PLA, there are challenges comprehending how complex interactions and cascading effects across the respective C4ISR systems-of-systems may play out in multiple domains. For example, if the PLA sought to prevent a U.S. Navy ship from using satellite communications (SATCOM), a simple interaction might be for a PLA EW system to jam the communication satellite's receiver (PLA interference versus U.S. C4).

A more complex, and realistic scenario might combine PLA ISR with the risk of a missile strike against the ship. If PLA ISR can detect and geolocate the U.S. ship's SATCOM, the PLA *might* attack the ship. The U.S. ship recognizes the threat, so it does not transmit using SATCOM to evade PLA ISR. In this example, the ship turned off its own SATCOM and the PLA achieved its goal, but no actual jamming or missile strike took place (ISR and destruction versus C4). This scenario could continue to play out if the U.S. ship continued to use SATCOM by deceiving PLA ISR with SATCOM signals in false locations (counter-reconnaissance) or using interference and destruction to directly disrupt PLA ISR or defeat the threat of missile attack. The PLA could (and does) compensate for these types of countermeasures by having multiple types of ISR systems and missiles that an adversary must defeat simultaneously.

Walking through every permutation of complex C4ISR system-of-systems confrontation would be impractical. However, over the past thirty-five years, the U.S. military has not had to think in terms of systems-of-systems confrontation. U.S. military C4ISR in the post-Cold War era has been confronted by either a few individual adversary systems or a wholly unsophisticated and primitive C4ISR such as those employed by terrorist organizations that created its own sets of challenges.[52]

There is an argument to be made that neither the U.S. military, nor any military, has faced the challenges that may emerge from military competition or confrontation with the PRC. Toward the end of the Cold War U.S. and Soviet military leaders were heralding a "revolution in military affairs" brought on by new technologies that connected sensors to shooters. However, kill chains in the 1980s were still fairly linear, and network technology was rudimentary by today's standards. Now, for the first time, the U.S. military faces a near-peer competitor with an extraordinarily complex C4ISR systems-of-systems and counter-C4ISR capabilities with a vision to defeat the U.S. at its own game – to achieve battlespace information dominance at in the early stages of hostilities.

The PLA has fully embraced system-of-systems confrontation concepts.[53] Informationized warfare is inherently system-of-systems versus system-of-systems confrontation—information and information technology are what binds a joint force together in a networked system-of-systems. As early as 2001, PRC National Defense University scholars observed, "[Modern warfare] is a confrontation between a system-of-systems and a system-of-systems. In informationized warfare, the degree of 'systemized confrontation' (体系化对抗) will be even more extreme."[54] By 2005, the CMC began emphasizing proficiency in system-of-systems confrontation as a specific goal for the PLA.[55]

This is not to say that the PLA has fully realized its C4ISR goals over the past two decades, nor has PLA necessarily exceeded the C4ISR capabilities of the U.S. military. However, the PLA is clearly working to build a world-class C4ISR and counter-C4ISR system-of-systems—all the offensive and defensive capabilities necessary to generate and preserve PLA access to information while disrupting and denying access to information for the PLA's adversaries.

PLA C4ISR in Counter-Intervention Operations

PLA C4ISR will have a critical role in establishing information dominance in a PLA counter-intervention operation. Robust, redundant, and resilient PLA C4ISR was principally designed to preserve PLA access to battlespace information in a defensive fight—to continue functioning in the face of anticipated attacks against the PLA C4ISR by U.S. and allied forces. However, PLA C4ISR also serves an important counter-C4ISR function through synergistic effects, as was described earlier in this report. Beyond direct damage and disruption to U.S. and allied C4ISR caused by PLA attacks, U.S. and allied active emitters may need to shut down to hide and prevent targeting by dense, layered PLA ISR. The PLA anticipates these synergies will yield potentially decisive information dominance for the PLA in a counter-intervention fight.

PLA Operational Reach

- **Within the Yellow Sea, East China Sea, and most of the South China Sea, the PLA probably begins a counter-intervention operation with information dominance and enjoys distinct advantages that may quickly translate into initial air and maritime dominance. In these initial stages of counter-intervention operations, the PLA may be able to establish localized information, air, and maritime dominance in areas out to the Second Island Chain that would, if necessary, allow the PLA to launch strikes on U.S. bases and deployed forces.**

C4ISR architecture largely defines the limits of PLA operational reach, especially in a large-scale operation like counter-intervention against the U.S. military. In 2024, PLA C4ISR and its ability to command and operate its joint force probably defines PLA conventional military power projection to the Western Pacific and Southeast Asia in a real-world combat scenario. In a counter-intervention operation, PLA kinetic strikes would probably be effective within 1500-2000 nautical miles of the Chinese mainland. Such strike capabilities, if realized in sufficient volume, may seriously impede, if not stop, a U.S. military intervention.

The PLA has certainly demonstrated global C4ISR capabilities in limited military operations that include peacekeeping operations in Africa, military diplomacy deployments, counterpiracy operations, and permissive non-combatant evacuation operations. What the PLA Navy calls "far seas" operations, even if limited, are a relatively recent development and generally have not involved large-scale joint military operations. The PLA Navy conducted its first substantial exercises in the Philippine Sea beginning in 2012.[56] The first circumnavigation of the Japanese archipelago by a formation of PLA Navy ships first occurred in 2013.[57] It is only within the past

few years that substantial joint formations of PLA ships and aircraft have exercised and operated together beyond the First Island Chain.[58] Even as the PLA stretches into global operations, it is important to recall that until very recently, PLA C4ISR was designed for the defense of China. The PLA's current C4ISR architecture is built upon those legacy C4ISR capabilities that are largely concentrated in mainland China.

Terrestrial C4ISR

- **The PLA enjoys a "home field advantage" in an East Asian conflict or counter-intervention operations. These advantages extend beyond basing and logistics to its fortress-like C4ISR.**

Over the past thirty years, the PLA leveraged growing defense budgets to create survivable and informationized warfare capable C4ISR. PLA leaders were impressed and extremely concerned by the devastating U.S. air strikes against Iraqi C4ISR in the 1991 Gulf War. Beginning in 1994, the PLA began to completely overhaul its National Defense Communications Network (NDCN), upgrading the entire system to high-speed fiber-optic cable.[59] The NDCN is almost entirely segregated from the PRC's civilian telecommunications network. NDCN fiber-optic cable may travel in the same cable trenches as civilian fiber, but the two systems have limited connectivity. However, as part of the PRC's civil-military fusion initiative, there have been exercises in which the civil network serves as a backup for the NDCN if it suffers damage.[60] The PLA's fiber-optic cable network also extends from the Chinese mainland to the PLA's artificial island-reefs in the South China Sea.[61]

Following embarrassment at the hands of the U.S. military in the 1995-1996 Taiwan Strait Crisis, the PLA began installing a "theater electronic information system" in southeast China.[62] It was known by the Chinese abbreviation "Qu Dian."[63] The Qu Dian theater system reportedly covered all of China's military regions by 2008 and offered high-speed communications and automated C2 of China's defenses for the first time.[64] Also in the early 2000s, the PLA developed an "integrated command platform" (ICP) (一体化指挥平台) an enterprise architecture to ingest and process large amounts of information, aid in command decision-making, and enable an interoperable joint force.[65] The PLA SSF's Information Communication Base is now probably responsible for the upkeep and maintenance of the ICP and its supporting networks.

PRC terrestrial C4ISR networks are the core of the architecture upon which the broader PLA C4ISR system-of-systems is built. PLA space-based communications capabilities have grown significantly in the past several years, but the "hard-wired" connectivity of the NDCN provides PLA command centers as well as units in the field with secure, reliable communications that are difficult for an attacker to disrupt or destroy.

Cyber ISR. PLA cyber ISR conducted by the SSF NSD will be an integral part of PLA counter-intervention operations, but these ISR capabilities are difficult to quantify. Cyber will certainly be used to launch computer network attacks against U.S. and allied C4ISR, platforms, and

weapon systems. However, the PLA will need to consider what intelligence might be lost if those networks are attacked and disabled. In a counter-intervention operation, cyber ISR will be employed to collect intelligence for indications and warning of intervention, intended movements, and the real-time location of U.S. and allied forces for targeting.

One area of concern for U.S. and allied forces should be an understanding of the "cyber terrain" and vulnerabilities in third countries where the U.S. or its allies may be operating. That is, U.S. networks may be protected and completely segregated from a telecommunications network where U.S. forces are based (e.g. the Philippines). However, if those national networks were constructed by PRC companies or are built on PRC network hardware, the PLA may be able to exploit those networks for ISR. (e.g. Surveilling Philippine networks for intelligence divulged by otherwise well-meaning locals such as a text messages or social media posts about the location of dispersed U.S. forces.)

Skywave Over-the-Horizon Radar. One notable land-based PLA ISR system that may be particularly relevant to counter-intervention operations is one or more sky-wave over-the-horizon (OTH) radars operated by the PLAAF. These OTH radars transmit high-frequency (HF) radar waves from huge land-based arrays that then bounce off the ionosphere and reflect back to Earth. Depending on the height of the ionosphere, China's skywave OTH radar may be able to detect ships and aircraft to ranges up to 3000 kilometers (1600 nautical miles) from the Chinese coast. The known skywave OTH radar transmitter and receiver sites are located 1000 kilometers inland and can probably detect ships and aircraft between the First and Second Island Chains.[66] China is also believed to operate several surface wave over-the-horizon radars which probably only provide detection and tracking capabilities a few hundred miles offshore and would not play a significant role in counter-intervention.

Air and Maritime C4ISR

- **Over the past several years, there has been a significant increase in the number of PLA C4ISR special mission aircraft. These aircraft, as well as uncrewed aerial vehicles (UAV) are flying with increasing frequency in the southern reaches of the South China Sea and beyond the First Island Chain. PLA improvements in airborne anti-submarine warfare as well as surface ship anti-submarine warfare has likely increased detection threats to U.S. and allied submarines.**

Special mission aircraft operated by the PLA have capabilities that include airborne early warning and control (AEW&C), signals intelligence/electronic intelligence (SIGINT/ELINT), electronic attack (EA) (i.e., jamming), as well as anti-submarine warfare (ASW) and maritime patrol (MARPAT). A list of PLAAF and PLANAF special mission aircraft appears in Appendix A. These aircraft elevate communications as well as active and passive sensors, allowing them to look down on the battlespace and extend line-of-sight ranges over the curve of the Earth. An example of the types of coverage that can be achieved by special mission aircraft flying at different altitudes is shown in Figure 5.

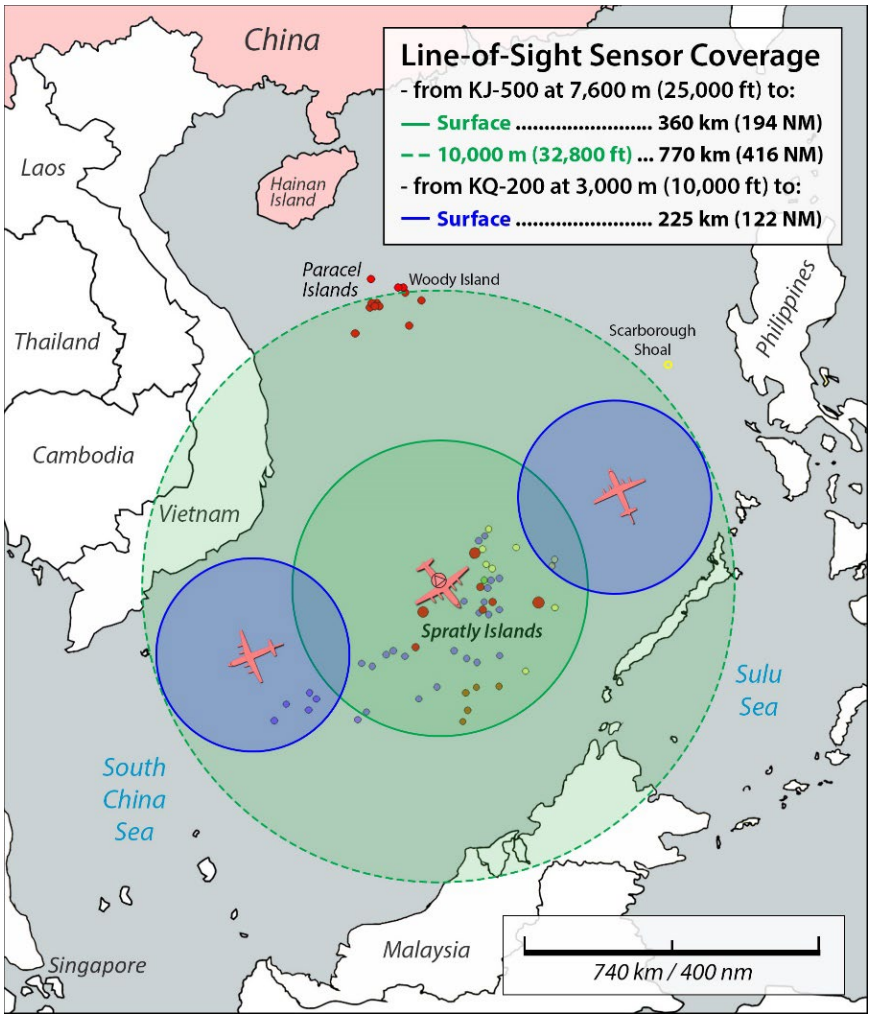

Figure 5. Example of Line-of-Sight Radar Coverage from PLA Aircraft [67]

Newer PLA special mission aircraft are based on the PRC's domestically designed and produced Y-9 transport aircraft. The Y-9 offers significant improvements in reliability and a 60 percent range increase over the Y-8, the airframe used for older PLA special mission aircraft. The Y-9 has a reported range of over 5,000 kilometers (~2,700 nautical miles) that translates to approximately ten hours of mission endurance.[68]

In 2019, the Shaanxi Aircraft Corporation, which produces Y-9 airframes, reportedly began mass producing special mission aircraft for the PLA.[69] A cursory examination of commercial satellite imagery reveals dozens of new special mission aircraft have appeared at PLA airfields over the past several years. Recognizable aircraft noted in commercial satellite imagery include KJ-500 AEW&C aircraft, KQ-200 ASW/MARPAT aircraft, and Y-9JB SIGINT/ELINT aircraft. More recently, the PLA has made significant improvements to infrastructure at several special mission aircraft airfields in the Northern, Eastern, and Southern TCs.[70]

Special mission aircraft have been noted flying beyond Japan's Ryukyu Islands and the First Island Chain with increasing frequency over the past several years.[71] Since at least 2021, special

mission aircraft have also been noted operating from PRC artificial island-reef air bases in the South China Sea.[72] In peacetime, these aircraft collect intelligence against U.S. and regional militaries. They also provide airborne C4ISR in support of PLAAF fighters and bombers or PLAN surface formations conducting routine operations and exercises.

UAVs would likely play a key role in providing ISR, communications relay, and possibly electronic warfare capabilities, especially in areas with a high threat of U.S. or allied air attack during counter-intervention operations. Occasionally, PLA UAVs have operated beyond the First Island Chain while accompanying special mission aircraft.[73] More typically, PLA UAVs have operated alone or in tandem with another UAV. Long-range UAVs that have been sighted flying into the Philippine Sea by the Japan Self Defense Force include the medium-altitude, long-endurance (MALE) Harbin BZK-005 and Tengden TB-001 as well as the high-altitude, long-endurance (HALE) Guizhou WZ-7 "Soaring Dragon." Figure 6 shows the recent flightpath of a BZK-005 and unidentified UAV operating east of Taiwan.

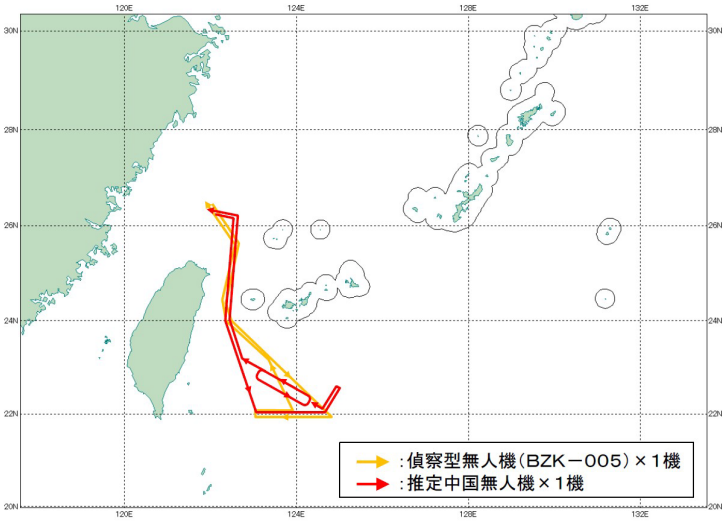

Figure 6. PLA UAV Out-of-Area Activity, August 25, 2023 [74]

Airborne C4ISR missions in the Philippine Sea and farther south into the South China Sea combined with increased PLAN ship presence has significantly improved PLA maritime domain awareness in these areas, especially against surface targets. It is important to note that PLAN and PLAAF presence in these areas only affords the PLA persistent C4ISR while they are deployed. Air and maritime domain awareness and C3 for forces operating far from the Chinese coast is largely enabled by rapidly developing space-based capabilities, discussed in the next section.

Long-range maritime ISR for counter-intervention is enabled by the SIGINT and radar information collected by PLAN ship patrols that venture beyond the First Island Chain and deep into the South China Sea. The three ship PLAN formation that conducts counter-piracy patrols in the Gulf of Aden as well at the PLAN base in Djibouti probably provide ISR of U.S. forces in Southwest Asia and would also provide indications and warning of a U.S. or allied move to intervene in an East Asian conflict from the Persian Gulf or through the Suez Canal and Red Sea.

Maritime ISR near and far from the PRC coast is also enabled by the PLA's maritime militia and PRC state-owned shipping. The PRC's maritime militia is most often associated with its fishing fleet but could conceivably include any PRC-flagged vessel. PRC mariners may be deployed to surveil U.S. and allied naval forces entering or operating in theater. C3 for these civilian vessels may include *Tiantong* communications. (*Tiantong* is a PRC version of IMARSAT.) Milita forces may also use the PLA-managed *Beidou* satellite navigation system, which has an integrated two-way text messaging capability.[75]

In the undersea domain, the PLA continues to make progress in improving its ASW technology, operational proficiencies, and capacities. Based on open-source assessments, PLA improvements in ASW technologies and operational proficiency are unlikely to shift the undersea advantage away from U.S. Navy submarines in the near term.[76] The PLA probably remains years away from having a submarine ASW capability. There is also very little open-source evidence to suggest that the PRC has developed and deployed a large-scale undersea acoustic array for ISR similar to the U.S. Navy SOSUS. However, the one area where the PLAN has made gains is in ASW capacity. Over the past several years, the PLA has fielded the new Z-20 shipborne ASW helicopter, dozens of KQ-200 ASW/MARPAT aircraft, and many more surface combatants equipped with both variable depth sonars (VDS) and towed array sonar systems (TASS).[77] Even if PLA ASW technology is not on par with that of the U.S. or Russia, some PLA undersea challenges may be addressed with the sheer volume of PLA ASW platforms available.

Space-based C4ISR

- **The PLA has seen significant growth in space based C4ISR capabilities. The number of PLA ISR satellites in geostationary orbit (GEO) has doubled in the past several years, while the number of PLA ISR satellites in low Earth orbit (LEO) has tripled. The PLA is also investigating and fielding new and novel technologies including a persistent imaging capability from GEO and automated detection and tracking from LEO satellites. These capabilities will likely create pronounced challenges for U.S. and allied forces attempting to avoid detection and targeting in a PLA counter-intervention operation.**

On February 29, 2024, General Stephen Whiting, Commander, U.S. Space Command, stated that the PRC is aggressively pursuing advances in military space capabilities. According to General Whiting's written testimony for the U.S. Senate Armed Services Committee,

> *"As of January 2024, the PRC's Intelligence, Surveillance, and Reconnaissance (ISR) satellite fleet contained more than 359 systems, more than tripling its on-orbit collection presence since 2018. The PRC has also dramatically increased its ability to monitor, track, and target US and Allied forces, both terrestrially and on orbit."*[78]

PRC development of military space capabilities has been stunning considering that the PLA only launched its first dedicated miliary communication satellite, its first real-time imaging satellite, and its first *Beidou* navigation satellite in 2000.[79] Even then, the PLA's on-orbit presence did not

see significant growth until after 2010. Now, the PLA launches dozens of satellites each year and appears to be heavily leveraging civil space capabilities. In 2023, PRC military and civil space launches totaled 67, putting over 200 satellites and other spacecraft into orbit. The record number of 2023 launches exceeded the previous PRC record, 64 launches 2022.[80]

PRC's Xi Jinping has described space as the "strategic high ground." The PLA clearly intends to occupy as much of that high ground as possible. An examination of PLA satellite constellations and their orbits reveals many PLA space priorities and counter-intervention capabilities.

Space Ground Segment. As previously outlined in the section on the Strategic Support Force (SSF) Space Systems Department (SSD), the 26th Testing and Training Base, also known as the Xi'an Satellite Control Center (XSCC), is the core of China's space telemetry, tracking, and control (TT&C) network. In a counter-intervention scenario, tasking for an ISR satellite to locate and track potential targets very likely runs through the XSCC and its nation-wide network of TT&C stations. The SSF SSD Aerospace Reconnaissance Bureau (ARB) is probably responsible for analysis of space-based ISR. These two key organizations will likely be directly involved in detecting and tracking U.S. and allied forces in a PLA counter-intervention operation. The PLA's space ground segment is extensive and may also include a handful of international ground stations. Further research would be required to offer a more comprehensive picture of the SSF SSD ground segment and processes for tracking and targeting foreign military forces.

Between 2019 and 2022, the PRC launched its second-generation of *Tianlian* data relay satellites. These relay satellites are critical enablers for the PLA space ground segment that pass tasking and data between low Earth orbit (LEO) satellites and PRC ground stations when the LEO satellites are out of view of the PRC mainland.

Geostationary Orbit (GEO) Satellites.[g] PRC presence in GEO reveals an orientation toward the PRC and East Asia. All probable PLA satellites in GEO appear positioned to maximize collection access and data throughput in or near the Chinese mainland. The field of view from GEO is significant, spanning approximately one-third of the Earth's surface, so PLA military communications and ISR satellites in GEO can theoretically provide coverage from western Africa to the mid-Pacific Ocean although signal degradation and a loss of collection capabilities likely occurs at extreme ranges and oblique angles.

The number of PLA ISR satellites in GEO has increased significantly since 2021, from six GEO ISR satellites in 2020 to a total of fourteen satellites today. The satellites offer few clues about their true missions while parked in orbit. PRC military and civilian satellites currently in GEO are shown in Figure 7. Assessed ISR satellites and their probable missions are depicted in purple. A list of GEO satellites that may provide significant capabilities in a counter-intervention scenario appears in Appendix B.

[g] A geostationary orbit or geosynchronous equatorial orbit (GEO) is a circular orbit 35,786 km above the equator that is synchronized with the Earth's rotation, so the GEO satellite appears stationary when viewed from the ground.

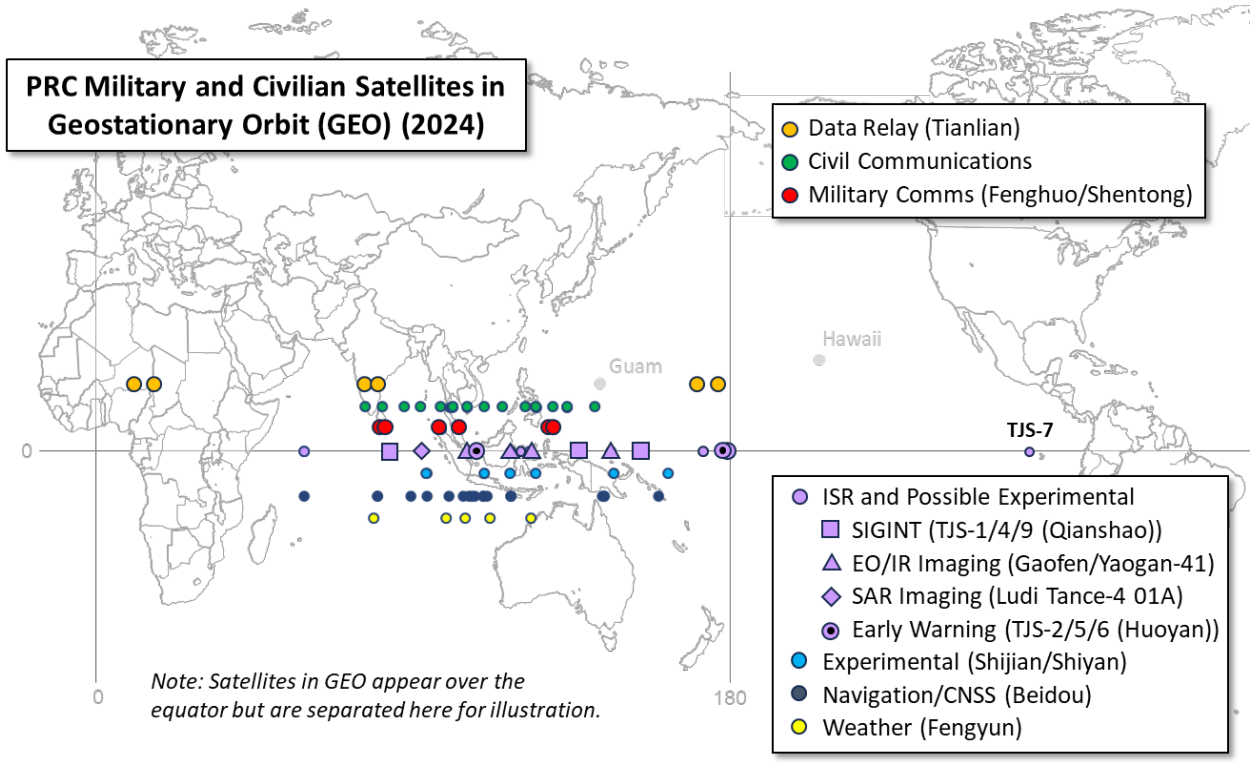

Figure 7. PRC Military and Civilian Satellites in Geostationary Orbit (GEO), 2024 [81]

The PLA probably operates at least three SIGINT satellites in GEO, the *TJS-1, -4,* and *-9*, known by their PLA designator, "*Qianshao*." The three *Qianshao* SIGINT satellites likely provide some of the most significant capabilities to support PLA counter-intervention operations. GEO satellites can be directed to "stare" at different parts of the battlespace for extended periods of time unlike low-earth orbit (LEO) satellites that only pass overhead periodically. These SIGINT satellites may be directed to geolocate signals or collect intelligence on U.S. or allied military forces operating from the Indian Ocean to the mid-Pacific. Little is publicly known about the *TJS-7*, the only PRC GEO satellite over the Western Hemisphere. It is likely an early warning satellite but could be a SIGINT collection satellite or, perhaps, serve both functions.

The PRC is reportedly the only nation with electro-optic (EO) imaging satellites in GEO, which could have significant implications for PLA counter-intervention operations. Like the *Qianshao* SIGINT satellites, these high-orbit EO satellites, can provide persistent imagery coverage across most of the Indo-Pacific to detect U.S. and allied ships. Since the satellites are so high above the Earth, the satellites cannot offer detailed image resolutions. The two ostensibly civilian *Gaofen-13* satellites, launched in 2020 and 2023, reportedly offer 15-meter image resolution. That is probably high enough to detect and track ships at sea, but probably not to identify the type of ship. The low-resolution imaging capability may still be valuable in a counter-intervention operation if, for example, the PLA cross-cues the low-resolution imaging capability with SIGINT collection to distinguish combatants from civilian ships and maintain persistent tracks on the former.

The *Yaogan-41*, launched into GEO in 2023, is almost certainly a dedicated military satellite that reportedly offers a 2.5-meter EO image resolution. If true, the *Yaogan-41* could both detect and classify different types of ships.[82] Of course, GEO imaging satellites, like their LEO counterparts, cannot see through cloud cover. In August 2023, the PRC launched the *Ludi Tance-4 01* (Land Survey-4 01), which is believed to be the world's first synthetic aperture radar (SAR) satellite in GEO. The satellite can reportedly collect 20-meter resolution images through all-weather conditions that would allow it to detect and track ships at sea.[83]

Low Earth Orbit (LEO) Satellites. LEO ISR capabilities, especially when combined with GEO ISR capabilities, create pronounced challenges for U.S. and allied forces trying to avoid detection and targeting in a PLA counter-intervention operation. The majority of PLA on-orbit capabilities are currently in LEO and consist of EO, hyperspectral, and infra-red (IR) imaging satellites, SAR imagery satellites, SIGINT and ELINT collection satellites, and a handful experimental communications satellites. It is doubtful that PRC ISR satellite technical capabilities exceed or even approach those of the U.S. National Reconnaissance Office. However, The PLA, and in some cases the PLA's commercial partners, are building dense, layered LEO constellations that provide near-constant space-based ISR coverage, especially in East Asia.

This report identifies 213 LEO ISR satellites in over a dozen constellations launched since 2018 that may provide significant capabilities to locate U.S. and allied forces in a PLA counter-intervention operation. Of those 213 satellites, 162 satellites—76 percent—have been launched since 2021.[84] A list of PLA and commercial LEO ISR satellites that may support counter-intervention operations appears in Appendix C.

LEO Imagery Satellites. LEO imagery satellites will allow the PLA to visually detect, track, and potently target U.S. and allied forces in a counter-intervention operation. Using current technology, the PLA would probably be challenged to use imagery satellites for real-time targeting of weapons against moving targets due to the time delay to download and interpret the images with either computers or human analysts. LEO satellite imagery alone is more valuable in identifying and targeting fixed or relocatable targets such as aircraft on the ground, radars, communications, or ships in port.

Beyond older, legacy systems that may still retain some capability, the PLA operates four high-resolution EO and eight SAR imaging satellites in LEO. The *Gaofen-11*, known by its likely PLA designator *Jianbing-16*, is purported to have a 10-centimeter image resolution.[85] For comparison, since 2020, U.S. and Western commercial satellite imagery providers have offered 30-centimeter resolution images that can be improved to 15-centimeter resolution with post-collection processing.[86] Open sources offer no indication of the SAR image resolution the four *Yaogan-33* and four *Yaogan-34* satellites.

The *Jilin-1* constellation of over 100 satellites in LEO may contribute significantly to PLA counter-intervention operations due to their high-revisit rates. Most of the *Jilin-1* small-form

imagery satellites offer 75-centimeter image resolution. The satellites are operated by the Chang Guang Satellite Technology Company (长光卫星技术股份有限公司), which is mostly government owned, but characterized as a commercial enterprise.[87] With over 100 imaging satellites on orbit in 2024, a Chang Guang company spokesman has suggested *Jilin-1* satellites will soon be able to image any place on Earth within ten-minutes. The *Jilin-1* constellation is expected to grow to 300 satellites by 2025.[88] Among the most concerning single *Jilin* capability may be the *Jilin-1 Kuanfu-02A*. Launched in August 2023, the satellite purportedly offers 50-centimeter resolution images that are collected in a 150-kilometer-wide swath, allowing it to cover large areas in a single image where U.S. and allied military forces may operate.[89]

LEO ELINT Satellites. The PLA's constellation of LEO ELINT satellites detects and geo-locates radar, communication, and other signals of interest and provides the PLA with an all-weather, day-night capability to detect, track, and potentially target U.S. and allied forces in a counter-intervention operation. The most capable PLA LEO ELINT satellite constellations are probably the *Yaogan-30, -31,* and *-40* satellites. The orbits of each of the thirty *Yaogan-30* satellites are evenly spaced to provide rolling, but near-constant ELINT coverage of East Asia and the Western Pacific.[90] The dense ELINT coverage offered by these satellites may create challenges for U.S. or allied forces attempting to radiate radars or communications in the apparently small gaps in LEO ELINT coverage.

The *Yaogan-31* and *Yaogan-40* ELINT satellites appear similar to those in the U.S. Naval Ocean Surveillance System (NOSS).[91] The combined fifteen *Yaogan-31* and *-40* satellites orbit in five sets of three satellites in a relatively tight formation. These formations probably detect and geolocate signals of interest, especially maritime targets. Compared to the *Yaogan-30* constellation, *Yaogan-31* and *-40* satellites provide global ELINT coverage with a much lower daily revisit rate. However, they can track targets high into the northern and southern latitudes.

LEO Multi-INT Satellite Trains. The latest generation of PLA LEO ISR satellites probably integrates multiple collection methods into a train of three satellites traveling in a line in the same orbit. The innovation may indicate that the satellites are engaged in automated "tipping and cuing." The first satellite, for example, may be an ELINT satellite to detect and geolocate a signal of interest. The trailing satellites, which may have EO, IR, or SAR payloads, are automatically cued to image the area where signals are detected to positively identify the emitter.

Little public information is available about these ISR satellite sets. The *Yaogan-35*, *-36*, and *-39* series satellites were all launched between 2021 and 2023. There are five triplets in each series—fifteen per series for a total of forty-five satellites. Again, instead of orbiting together in a tight formation like the *Yaogan-31* satellites, the satellites travel in a line, separated by between 400-1000 kilometers. A depiction of a *Yaogan-36* triplet and the satellites' field of view is shown in Figure 8.

These satellite sets may be designed to defeat U.S. or allied decoys and deception. For example, a decoy may transmit a ship's radar signal and would be located by the first ELINT satellite.

However, if the cued trailing satellite does not image a ship, the bluff is revealed. If, on the other hand, the signal does correlate to a ship, the PLA has instant confirmation of the ship's location.

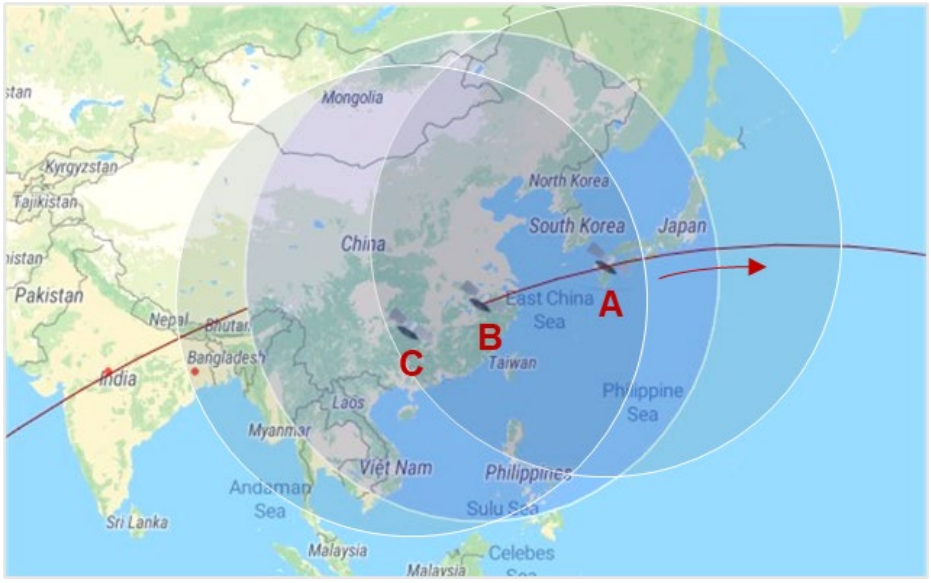

Figure 8. Yaogan-36 03A/B/C Orbits.[92]

LEO Communication Satellites. The PRC has struggled in recent years to field a constellation of LEO communications satellites. However, the PRC government has recently unveiled ambitious plans for a LEO communication constellation to rivla the U.S. company SpaceX and its constellation of over 5,000 *Starlink* satellites.

The PRC commercial company GalaxySpace (银河航天) has established an experimental constellation of six LEO satellites in what has been called "China's first LEO broadband communication test constellation in the South China Sea."[93] In 2023, GalaxySpace reportedly planned to provide high-speed satellite data service for the PRC's hypersonic flight program.[94] Those plans for LEO broadband are almost certainly being undermined by two competing PRC mega constellations of LEO communications satellites in development.

In 2024, the PRC state-owned Shanghai Gesi Aerospace Technology (上海格思航天科技有限公司), plans to launch the first 108 "*G60 Starlink*" LEO communication satellites of a planned 12,000 satellites. Meanwhile, state-owned aerospace and defense conglomerates CASC and CASIC have combined their previously struggling plans for LEO communications constellations to form the China Satellite Network Group (中国卫星网络集团有限公司), which has its own plans for a 13,000-satellite mega constellation of "*Guowang*" (国网) satellites.

PLA access to LEO communication satellites will significantly improve communication and data connectivity for mobile PLA forces including ships, aircraft, and amphibious forces on the move. An expansive LEO communications capability may also decrease the likelihood of detection and targeting of PLA forces by U.S. or allied ISR.

PLA Counter-C4ISR in Counter-Intervention Operations

- **In a counter-intervention operation, the PLA will directly and indirectly target what it considers the critical operational center of gravity for the U.S. and its allies—their C4ISR system-of-systems—to ensure battlespace information dominance. Coalition C4ISR networks will likely be priority targets for PLA counter-C4ISR strikes.**

PLA strikes on U.S., allied, and partner forces in the early stages of counter-intervention operations will be "information-centric." That is, the focus of effort, at least initially, will be to target U.S. and coalition information power—its C4ISR system-of-systems with non-kinetic and kinetic strikes. Other strikes against important targets such as air defenses, airfields, and ships operating forward will certainly occur in this phase, but the weight of PLA effort will likely be against U.S. and coalition C4ISR to achieve battlespace information dominance. The theory behind such opening moves is that if U.S. and coalition C4ISR can be removed from play, maneuver forces will simply be unable to press their intervention against PLA operations. Even if U.S. and allied commanders and decisionmakers can push through the uncertainty, PLA forces will lie in wait in the fog they created, ready to target and engage disconnected U.S. and coalition forces with potentially devastating effects.

Initial impacts on U.S. and coalition C4ISR will likely be generated through synergistic effects created by PLA C4ISR and the threat of detection and/or attack. U.S. and allied militaries will have to turning off their own communications and active sensors to avoid detection by dense, layered PLA ISR thus ceding initial information dominance to the PLA. These compounding effects will be accompanied by direct cyberattacks on U.S. and coalition networks accompanied by extensive non-kinetic electronic warfare (EW) attacks. EW effects will increase in type and intensity the closer U.S. and allied forces are to the PRC mainland. As the conflict progresses, the PLA will be prepared to escalate and launch overwhelming kinetic attacks on U.S. and coalition C4ISR. Command, control and communications hubs, satellite teleports, undersea communications cables, airborne C4ISR, and on-orbit C4ISR capabilities will be priority targets. The PLA will also seek to protect its own operational center of gravity—its C4ISR system-of-systems—that the PLA expects is at the top of the U.S. and coalition target lists for non-kinetic and kinetic attacks.

One thing that is virtually certain is that allied and coalition C4ISR networks will be priority targets for PLA non-kinetic and kinetic strikes in any counter-intervention operation involving other than U.S. military forces. Coalition C4ISR will almost certainly be less protected than U.S. C4ISR and probably the most vulnerable to PLA attack. Disrupting and destroying the C4ISR links among the U.S., its allies, and partners will likely have outsized operational and strategic effects that may significantly slow or stop a U.S. intervention in an East Asian conflict.

Which U.S. and allied C4ISR targets will likely be attacked in a counter-intervention operation and whether the system-of-systems has sufficient redundancy and resilience to continue functioning in the face of PLA attacks merits additional in-depth study. One PLA counter-

intervention capability that warrants special attention and demonstrates the interrelated, compounding synergies of information power is the PLA's substantial electronic warfare capabilities.

Electronic Warfare

- **The PLA is an electronic warfare juggernaut. The PLA possesses both the technological capabilities and significant electronic warfare capacities to conduct significant offensive and defensive electromagnetic spectrum operations that will enable, if not ensure initial PLA information dominance in a counter-intervention operation.**

In a media event for the rollout of DoD's 2023 China Military Power Report, an unnamed Pentagon official intimated that the PLA believes it is facing significant challenges in electronic warfare (EW). "Some of the things that they [the PLA] talked about are how they can operate — or need to be better prepared to operate — in what they call a complex electromagnetic environment," the official stated.[95] The PLA and its leadership certainly understand the importance of dominating the electromagnetic spectrum (EMS) and may harbor significant concerns about the inherent complexity of military operations in the EMS. However, to suggest that the PLA is not currently an extremely capable EW force is a gross mischaracterization of PLA capabilities. In point of fact, PLA electronic warfare capabilities and, more importantly, capacities vastly exceed those of the Russian military and probably even the U.S. military.

The PLA initially invested in EW capabilities in the 1980s based on observations of superpower competition during the Cold War.[96] Current PLA EW concepts are built on Soviet concepts of "radio-electronic combat" more than Western ideas about EW employment. The Soviet strategy for countering the U.S, precision strike–enabled "Second Offset Strategy" was essentially to starve U.S. smart weapons of information through EW strikes against the U.S. "reconnaissance-strike complex." China's informationized warfare strategy is, in many ways, an evolution of that Soviet approach to operational-level information superiority based on non-kinetic and kinetic EW.

The PLA's development of significant EW capabilities occurred in parallel with PLA informationized warfare development. As early as 2001, the PLA's overarching training guidance, the "Outline of Military Training and Evaluation (OMTE)," directed a force-wide focus on what the PLA started calling a "complex electromagnetic environment (CEME)" (复杂电磁环境).[97] By 2006, senior PLA leadership established a clear linkage between success in electronic warfare (电子战) and informationized warfare.[98] The PLA's 2015 Military Strategy directed the PLA to "intensify training in complex electromagnetic environments."[99] The PRC 2019 Defense White Paper identified China's national defense aims to include safeguarding "China's security interests in outer space, electromagnetic space, and cyberspace," probably a nod to the combined mission areas of the Strategic Support Force.[100] For over two decades, the same level of technology investments and innovations apparent in other advanced PLA weapons systems have also been poured into PLA EW capabilities.

In the context of military operations, the PLA concept of integrated network-electronic warfare (INEW) should be understood to emphasize electronic warfare more than cyber capabilities. Cyber capabilities will play an important role but may have limited utility in the operational battlespace and actual combat engagements. Fundamentally, cyber capabilities are challenged by access. Network and system access to cyber-hardened, closed-loop combat systems is a greater challenge than most realize. Moreover, both the PLA and its competitors may have restrictive concerns about implanted malware that cannot be controlled inside an adversary network that might result in runaway escalation during a crisis. Where the PLA does have ready access and some measure of control is the electromagnetic spectrum.

The discipline of electronic warfare consists of three interrelated functions. Electronic attack (EA), also known as electronic countermeasures (ECM), is the use of electromagnetic energy to jam or deceive enemy signals. EA may also involve the use of directed energy or anti-radiation homing weapons to physically destroy enemy electronic equipment. Electronic protection (EP), or electronic counter-countermeasures (ECCM), are measures that protect friendly electronic signals and equipment from enemy EA. Electronic warfare support (ES) is essentially synonymous with electronic intelligence (ELINT) but has the expressed purpose of detecting, identifying, and localizing enemy signals. ES has a large role in targeting support for EA or other weapons. The three interrelated EW functions correlate to the interrelated elements of information power introduced earlier (see Figure 9). No single PLA EW capability will yield EMS dominance. Taken together, however, their synergies will likely generate outsized effects.

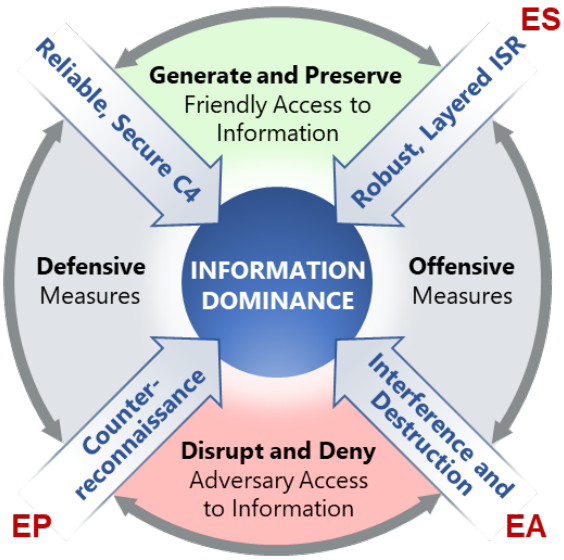

Figure 9. EW Functional Alignment to Information Power Capabilities Conceptual Framework.

Qualifying or quantifying capabilities in the three areas—EA/ECM, EP/ECCM, and ES—is challenging given the nature of EW capabilities and technical features that are not readily observable through publicly available sources. PRC scientists and defense-related research institutions have been publishing world-class radar, communications, and electronic warfare

research papers for over a decade. Where some PLA EW-related capabilities can be observed, it is abundantly clear that the PLA is making significant and growing investments in EW.

Electronic Attack (EA). Many of the PLA's current EA capabilities and capacities reside in ground-based, road-mobile ECM brigades. The SSF operates substantial ground-based ECM brigades that probably focus on air defense of Beijing or other strategic targets.[101] The PLAAF, PLAN, and PLARF each have service ECM brigades that provide ES and EA capabilities to the TCs. PLA EA vehicles are seldom displayed publicly but have occasionally been noted in commercial satellite imagery.[102] Individual EA vehicles marketed by PRC defense manufacturers indicate specialized vehicles may jam different types of targets (e.g. datalinks, radars, etc.) or in different frequency bands (millimeter-wave-, X/Ku-, C-, L-, and S-band jammers have been noted).[103]

EA Aircraft. While ground based EA may be effective against airborne targets, EA aircraft offer better wide-area coverage of targets. The PLAAF does not appear to currently have a significant number of purpose-built EA aircraft.[104] However, several new types have appeared in the past few years and their numbers are growing. The PLAAF still apparently flies older Y-8G EA aircraft. As part of the surge in special mission aircraft production mentioned earlier, the PLAAF began adding new Y-9G EA aircraft to its inventory in 2019.[105] 2021 China Air Show saw the debut of the PLAAF J-16D, an EA-version of the J-16 fighter-bomber similar to the U.S. Navy EA-18G *Growler*. The J-16D is apparently operational and was noted conducting exercises near the Taiwan Strait in 2022.[106]

Anti-Radiation Weapons. Perhaps more significant than ground-based or airborne jammers may be the different types of EA anti-radiation weapons that guide themselves into electromagnetic signals to "hard-kill" radar or communications targets. The PLAAF acquired the Russian AS-17 anti-radiation missile (ARM) in 2000 and successfully retro-engineered it into the YJ-91 ARM. Since 2020, several new PRC-produced ARMs have emerged.[107] The TL-30, possible also known as the AKF088C, was first noted on a PLAAF aircraft at the 2022 China Air Show. The TL-30/ AKF088C is an anti-radiation cruise missile that can fly up to 280 kilometers (150 nautical miles) and loiter while searching for targeted signals.[108] The PRC defense industry also markets anti-radiation seekers for ballistic missiles indicating that these types of seekers are probably incorporated on PLARF ballistic missiles that might be employed against U.S. or allied forces.[109]

In early 2024, media reports indicated that Iranian-produced Shahed-136 "kamikaze" attack drones were used by the Russian military in Ukraine to great effect. Based on appearance alone, the Shahed-136 is almost certainly an Iranian knock-off of the PRC-produced ASN-301 "mobile anti-radiation drone system," which has been in the PLA inventory since at least 2017.[110] These types of low-altitude, slow flying anti-radiation drones can be particularly potent since they are designed to approach a target area undetected and loiter. Then, when an air defense radar illuminates to engage an aircraft or ballistic missile, for example, the drone will home in on the radar and destroy it.

Counterspace EA. Since 2020, there has been a significant increase in the SSF's ability and capacity to conduct counterspace EA against foreign satellite communications (SATCOM). Non-kinetic attacks against U.S. and allied SATCOM will likely be the first moves in any PLA counter-intervention operation.

SSF counterspace EA capabilities have been consolidated under the SSF's counter-space ECM brigade, the 32090 Unit (32090 部队), headquartered in Langfang, Hebei, PRC.[111] The Langfang facility, which houses road-mobile SATCOM jamming battalions, saw significant upgrades to base infrastructure between 2021 and 2022.[112] The SSF's Yingtan counterspace ECM facility, located in eastern China, also houses road-mobile SATCOM jammers and was the only other counterspace ECM facility identified in open sources prior to 2020. Since 2020, six additional 32090 Unit counterspace ECM facilities have been constructed in Tibet, near Shanghai, and on Hainan Island. By 2022, the six facilities represented a 500 percent increase in fixed antenna infrastructure to identify and track SATCOM signals in support of PLA counterspace EA.[113] An additional battalion of road-mobile SATCOM jammers was also identified on Hainan Island.[114] Since 2022, many of the newly constructed facilities have continued to expand with some doubling in size by early-2024.

The effectiveness of PLA non-kinetic EA capabilities is next to impossible to assess based on open sources. Even if PLA jamming capabilities were estimated based on PRC EW research, jamming necessarily involves the interaction between a jammer and a receiver—a radar, communications, or other system. Without intimate knowledge of the EP capabilities of EA targets, comprehensive effectiveness cannot be assessed. The PLA likely enjoys significant EA capabilities against older military systems or commercial systems with little or no EP. How PLA EA might fare against EP hardened, advanced U.S. military systems probably cannot be determined based on open-source research.

Electronic Protection (EP). PLA EP capabilities are among the most difficult to observe and assess. Given the PLA focus on EW, PLA radars, communications, and ISR certainly have hardware or signal processing that protects those systems from enemy EA, but this is not apparent from open sources. A more obvious measure of PLA efforts at EP is the frequency diversity in PLA C4ISR systems. The PLA fully anticipates electronic jamming attacks as well as kinetic attacks against its C4ISR. Therefore, the PLA covers a broad range of the frequency spectrum with such a diversity of systems, that even a sophisticated adversary would be challenged to simultaneously jam or destroy enough PLA C4ISR electronic systems to significantly constrain the PLA's access to battlespace information.

Large numbers of diverse PLA systems cover a wide swath of the frequency spectrum. Ground-based radars employed for ISR range from the HF-skywave over-the-horizon radar mentioned earlier, to VHF-, UHF-, L-, S-, C-, and X-band radars.[115] Similarly, PLA communications systems extend from lower frequency HF communications all the way up to Extremely High Frequency (EHF) satellite communications in the Q/V-bands. The PLA also remains invested in

older communications technologies like difficult to intercept and jam troposcatter communications against which U.S. and allied EW probably have little-to-no capabilities.[116]

In 2007, the PLA began fielding a joint datalink system that is similar to, if not based on, the U.S. Link-16/Joint Tactical Information Distribution System (JTIDS) data link. That PLA datalink is known as the "Joint Information Distribution System" or "JIDS" (联合信息分发系统). Link-16, and probably JIDS, are frequency hopping data links that are resistant to intercept and jamming. The PLA may now be incorporating a new generation of tactical data link, the DTS-03, developed by PLA defense conglomerate CETC. DTS-03 purportedly has a significantly higher data exchange rate at much lower latency than Link-16/JIDS and incorporates ad-hoc technology to create a dynamic, jam-resistant mesh network.

Electronic Warfare Support (ES). PLA ES capabilities were outlined in earlier discussions of ISR capabilities. SIGINT collection facilities on the Chinese mainland combined with ELINT sensors on deployed ships, GEO and LEO satellites, UAVs, and special mission aircraft provide a robust, layered, redundant ES capability to support EA and kinetic targeting.

Electromagnetic Spectrum Operations (EMSO). Recently revised U.S. military doctrine has placed electronic warfare functions under the umbrella of EMSO, which includes management of the electromagnetic spectrum.[117] Here too, the PLA has evolved significant capabilities, especially in military operations where the PLA enjoys a "home field advantage." In a counter-intervention operation against U.S. and allied forces, the PLA will be operating in the same electromagnetic environment where they live, operate, and train day-to-day.

The PLA also appears to have a well-developed frequency management apparatus that deconflicts frequency spectrum use among military units and with civil authorities.[118] The PRC's 2010 Radio Control Regulations assign military responsibility for frequency spectrum management to the Military Electromagnetic Spectrum Management Agency (军队电磁频谱管理机构) and Military Region electromagnetic spectrum management agency (军区电磁频谱管理机构). In 2016, in conjunction with the above-the-neck reforms, what is apparently now called the Frequency Spectrum Control Group (Dadui) (频谱管控大队) was transferred to the CMC Joint Staff Department.[119] The current TC's have probably incorporated the former MR spectrum management agencies and converted them to theater frequency spectrum control groups, mirroring the organization of the CMC Joint Staff Department.

Electronic warfare capabilities and electromagnetic spectrum operations are clearly a priority for the PLA. The PLA will likely exploit its ready access to its local electromagnetic environment and deliver non-kinetic EW strikes on U.S. and allied forces in the opening moves of a counter-intervention operation. As the conflict escalates, the PLA will probably employ destructive, kinetic EW capabilities to ensure dominance in the electromagnetic environment and the information battlespace.

Conclusions and Recommendations

PLA C4ISR is layered and dense, ensuring a significant capability to detect, track, and target U.S. and allied forces seeking to intervene against the PLA. The PLA C4ISR system-of-systems combined with reliable long-range weapons poses a serious, if not critical threat to U.S. and allied freedom of action in an East Asian conflict.

A large-scale conflict that pits the PLA against the U.S. military will likely be fundamentally different in terms of scope and complexity than any other near-term conflict currently facing either nation. Both the U.S. and PRC have invested in complex and expansive C4ISR systems-of-systems that are not well understood by policymakers or even the militaries themselves. The complex interactions and cascading effects that may be created across the opposing C4ISR systems-of-systems of these competitors is difficult to comprehend and merits further study.

In August 2023, the USCC issued a request for proposals on "China's Advanced Remote Sensing Technologies and Applications," which will likely be an excellent contribution to the Commission's understanding of the important issue of PRC C4ISR technologies.[120] U.S. policymakers may also wish to consider the following recommendations:

- **Conduct a comprehensive net assessment of U.S. and allied C4ISR and counter-C4ISR capabilities in a large-scale conflict with the PLA.** The complex interactions and cascading effects created in a U.S.-PRC conflict across respective C4ISR systems-of-systems would be exceedingly complicated and are becoming more complex each year. Assessing and modeling C4ISR and counter-C4ISR engagements in a virtual system-of-systems model may be a costly and time-consuming endeavor. However, if policymakers wish to understand likely outcomes in a U.S.-PRC system-of-systems confrontation, make informed C4ISR capability investments, and develop effective mitigation strategies, modeling and analysis combined with a comprehensive net assessment will be critical.

- **Engage the U.S. military regarding future C4ISR strategies and the need to emphasize more defensive capabilities including significant redundancy within the U.S. C4ISR system-of-systems.** A 2023 U.S. Government Accountability Office (GAO) report described programs like DoD Joint All-Domain Command and Control (JADC2) as principally improving joint force integration and interoperability. "JADC2 must connect headquarters to forces so that joint command and control decisions are executed at a faster pace than potential adversaries to maximize operational effectiveness."[121] Perhaps it is implied, but there is no mention in the GAO report for JADC2 to be redundant or resilient in the face of integrated PLA C4ISR capabilities and counter-C4ISR attacks that have been specifically designed to paralyze the U.S. command and control. Redundancy and resiliency will be a prerequisite to basic survivability and successful combat employment.

- **Invest in significant counter-reconnaissance capabilities including physical, virtual and electromagnetic camouflage, concealment and deception (CCD) measures.** PLA ISR in East Asia is fantastically dense, featuring layered and overlapping coverage from different types of collection—EO/IR/hyperspectral imagery, synthetic aperture radar imagery, and different types of SIGINT. These detection capabilities combined with long-range PLA weapons systems will deny the U.S. and its allies the sanctuaries to base and operate that they enjoyed since the end of the Cold War. Robust defensive that include significant CCD measures that either deceive or overwhelm PLA ISR will be necessary to ensure U.S. and allied forces can operate in contested battlespaces.

- **Invest in robust, redundant, and resilient coalition C4ISR links and networks to increase combat interoperability among critical allies and partners and deny the PRC military battlespace information dominance that might separate the U.S. from a coalition.** The PLA understands that allies and partners are a significant force multiplier for the U.S. military. Allied and partner bases in the Indo-Pacific will be critical to any intervention in a military conflict involving the PRC. Moreover, allies and partners may provide combat forces to fight alongside U.S. forces, but only if those forces can securely share, interpret, and act upon critical battlespace information in real-time. The PLA will target coalition C4ISR networks early and often in a conflict to disaggregate the coalition force and achieve information dominance to enable follow-on kinetic strikes.

- **Fund additional U.S. Intelligence Community capabilities to analyze current and future PLA counter-C4ISR capabilities and strategies (if required).** As a near-peer competitor and potential military adversary, the PLA has adopted a strategy to target, disrupt, and destroy enemy C4ISR with a goal of establishing battlespace information dominance. The U.S. Intelligence Community is no doubt keenly aware of PLA counter-C4ISR capabilities and strategies. However, there is no one DoD institutional champion for U.S. C4ISR. While individual joint and service programs drive requirements to understand threats to individual C4ISR systems, no single DoD official is responsible for the broader system-of-systems that the PLA will ultimately target. This bureaucratic segregation may dilute intelligence requirements for a more comprehensive understanding of how PLA counter-C4ISR capabilities might threaten the broader U.S. C4ISR enterprise. Comprehensive intelligence on PLA counter-C4ISR capabilities and strategies will lead to better strategic and operational outcomes and inform effective policy and budget decisions.

- **Publish a detailed open-source assessment of PLA C4ISR and counter-C4ISR threats to U.S. and allied military forces.** PLA progress on weapons systems and platforms—missiles, aircraft, ships, and tanks—are widely reported in public sources. The public and policy community should be better educated on critical military capabilities that will likely have outsized impacts on Information Age warfare. Special attention should be paid to PLA's rapid advances in space based C4ISR from open-source material for the purposes of public debate.

- **Fund additional U.S. Intelligence Community capabilities to analyze current and future PLA electromagnetic spectrum operations (EMSO) capabilities and strategies (if required).** Many dedicated Intelligence Community professionals are certainly focused on PLA EMSO capabilities and strategies. However, as with the C4ISR system-of-systems, there is no DoD institutional champion for electronic warfare, which may result in a lower priority and consequently fewer Intelligence Community resources directed at PLA EMSO. Policymakers may wish to consider whether Intelligence Community collection and analysis of PLA EMSO and electronic warfare is commensurate with the importance the PLA clearly attaches to those capabilities and the outsized role EMSO has in informationized warfare. Comprehensive intelligence on PLA EMSO capabilities and strategies will lead to better strategic and operational outcomes and inform effective policy and budget decisions.

- **Publish a detailed open-source assessment of PLA electronic warfare capabilities and threats to U.S. and allied military forces.** As a stand-alone effort or in conjunction with the recommended assessment of counter-C4ISR threats, the subject of electronic warfare should receive special attention. In future combat operations, electronic warfare will be as significant if not more significant than cyber warfare. Electronic warfare threats and the potential vulnerabilities created by a EW capable challenger like the PLA have not received the same level of attention and scrutiny as issues related to conventional weapons and platforms or cyber. A better public understanding of PLA electronic warfare capabilities and strategies will inform DoD and Intelligence Community budget priorities and guide program development.

Appendix A. PLA C4ISR Aircraft and UAVs

Table 2. PLAAF and PLANAF Special Mission Aircraft [122]

Aircraft Model	*Gaoxin* Designator	PLA System Designator	Mission	PLA Service *Notes*
Y-8G	GX-3		Electronic Attack	**PLAAF** *Being replaced by Y-9G*
Y-8W	GX-5	KJ-200	AEW&C	**PLAAF/PLANAF** *Being replaced by Y-9W/KJ-500*
Y-9Q	GX-6	KQ-200	ASW/Maritime Patrol (MARPAT)	**PLANAF**
Y-8XZ	GX-7		Psychological Warfare	**PLAAF** *Being replaced by Y-9XZ*
Y-9JB	GX-8		SIGINT/ELINT	**PLAAF/PLANAF**
Y-9XZ	GX-9		Psychological Warfare	**PLAAF**
Y-9W	GX-10	KJ-500	AEW&C	**PLAAF/PLANAF**
Y-9G	GX-11		Electronic Attack	**PLAAF**
Y-9DZ	GX-12		SIGINT/ELINT	**PLAAF (prob.)**

Project designations based on the prefix *Gaoxin* (GX)— "高新" or "high-tech"—appear to be collectively assigned by Chinese aviation enthusiasts as aircraft appear in photographs for the first time.

Table 3. Select PLA Uncrewed Aerial Vehicles (UAV) / Uncrewed Combat Aerial Vehicles (UCAV) [123]

UAV / UCAV	External/Mission Payload	Max Speed	Max Ceiling	Endurance
BZK-005	150 kg (330 lb)	210 km/hr (113 kt)	8,000 m (26,000 ft)	40 hrs
GJ-1 Wing Loong I	200 kg (441 lb)	280 km/hr (151 kt)	7,000 m (23,000 ft)	20 hrs
Wing Loong I-D	400 kg (882 lb)	280 km/hr (151 kt)	7,500 m (24,600 ft)	35 hrs
GJ-2 Wing Loong II	480 kg (1058 lb)	370 km/hr (200 kt)	9,000 m (29,500 ft)	20 hrs
CH-5	480 kg (1058 lb)	300 km/hr (162 kt)	8,300 m (25,000 ft)	35 hrs
TB-001	100 kg (220 lb)	300 km/hr (162 kt)	8,000 m (26,000 ft)	36 hrs
WZ-7 Soaring Dragon	650 kg (1400 lb)	750km/hr (405 kt)	18,000 m (60,000 ft)	10-11 hrs

Appendix B. Significant Geostationary Orbit (GEO) Satellites Supporting Counter-Intervention Operations

Table 4. Select PRC Communication Satellites in GEO [124]

Satellite Name	Likely PLA Designator	Likely Mission	GEO Slot (Deg. Longitude)	Launched
ChinaSat 1A	*Fenghuo* 2A	Military Comms C- and UHF-bands	129.8	2011
ChinaSat 1C	*Fenghuo* 2C	Military Comms C- and UHF-bands	81.0	2015
ChinaSat 1D	*Fenghuo* 2D	Military Comms C- and UHF-bands	130.0	**2021**
ChinaSat 1E	*Fenghuo* 2E	Military Comms C- and UHF-bands	98.1	**2022**
ChinaSat 20A	*Shentong* 1A	Military Comms Ku-Band	130.0	2010
ChinaSat 2A	*Shentong* 2A	Military Comms Ku-band	98.0	2012
ChinaSat 2C	*Shentong* 2C	Military Comms Ku-band	103.4	2015
ChinaSat 2D	*Shentong* 2D	Military Comms Ku-band	130.0	2019
ChinaSat 2E	*Shentong* 2E	Military Comms Ku-band	98.1	**2021**
Tiantong-1 01	(commercial)	Mobile SATCOM S-band	101.4	2016
Tiantong-1 02	(commercial)	Mobile SATCOM S-band	125.0	**2020**
Tiantong-1 03	(commercial)	Mobile SATCOM S-band	81.4	**2021**
Tianlian-1 Series (5 satellites)	-	Data Relay (LEO-to-ground)	10.5, 16.9, 77.0, 77.1, 176.7	2008, 2011, 2012, 2016, **2021**
Tianlian-2 Series (3 satellites)	-	Data Relay (LEO-to-ground)	10.7, 79.9, 171.0	2019, **2021, 2022**

Table 5. Select PRC Intelligence Collection Satellites in GEO [125]

Satellite Name	Possible PLA Designator	Likely Mission	GEO Slot (Deg. Longitude)	Launched
TJS-1	*Qianshao*-3 1	SIGINT	155.1	2015
TJS-4	*Qianshao*-3 2	SIGINT	83.5	2019
TJS-9	*Qianshao*-3 3	SIGINT	137.3	**2021**
TJS-2	*Huoyan*-1	Early Warning (probably IR)	107.4	2017
TJS-5	*Huoyan*-1	Early Warning (probably IR)	178.0	2020
TJS-6	*Huoyan*-1	Early Warning (probably IR)	179.0	**2021**
TJS-7	*Qianshao* or *Huoyan* (?)	SIGINT or Early Warning	-99.0	**2021**
TJS-10	(?)	Unknown	173.3	**2023**
TJS-11	(?)	Unknown	120.4	**2024**
Yaogan-41	(?)	Poss. 2.5m EO + IR Imagery	123.5	**2023**
Gaofen-4	(civil-military)	50 m EO + IR Imagery	105.7	2015
Gaofen-13	(civil-military)	15 m EO + IR Imagery	118.0	2020
Gaofen-13-02	(civil-military)	15 m EO + IR Imagery	146.7	**2023**
Ludi Tance 4-01	(civil-military)	SAR Imagery L-band	90.5	**2023**

TJS stands for *Tongxin Jishu Shiyan* (通信技术试验), which means "communication technology test." *Gaofen* (高分) is "high resolution." *Yaogan* (遥感) is "remote sensing." *Ludi Tance* (陆地探测) is "land survey." *Qianshao* (前哨) is "outpost" or "frontline." *Huoyan* (火眼) is "fire eye."

TJS-2, -5, and -6 are likely *Huoyan* satellites—a constellation of satellites with an infra-red (IR) imaging capability used for ballistic missile early warning. These early warning satellites probably support the PRC's significant increase in fixed nuclear ballistic missile silos and the PLA's shift to a "launch-on-warning" nuclear retaliation strategy.

Appendix C. Significant Low Earth Orbit (LEO) Satellites Supporting Counter-Intervention Operations

Table 6. Select PRC Intelligence Collection Satellites in LEO [126]

Satellite Series	Possible PLA Designator	Satellites in Constellation	Likely Mission	Orbit Type	Year Launched (# of satellites)
Gaofen-11	*Jianbing*-16	4	EO Imaging (< 0.2 m)	Sun Synchronous	2018 (1), 2020 (1), **2021 (1), 2022 (1)**
Jilin-1 Gaofen-02	(commercial)	4	EO Imaging (0.75 m)	Sun Synchronous	2019 (2), **2021 (2)**
Jilin-1 Gaofen-03	(commercial)	64	EO Imaging & Video (0.75-1 m)	Sun Synchronous	2019 (1), 2020 (9), **2021 (3), 2022 (32), 2023 (9)**
Jilin-1 Gaofen-06	(commercial)	30	EO Imaging (0.75 m)	Sun Synchronous	**2023 (30)**
Jilin-1 Kuanfu-02A	(commercial)	1	EO Imaging (0.5 m x 150 km)	Sun Synchronous	**2023 (1)**
Jilin-1 Hongwai-A	(commercial)	8	IR Imaging	Sun Synchronous	**2022 (6), 2023 (2)**
Yaogan-33	Follow-on to JB-5 (?)	4	SAR Imaging (?)	Sun Synchronous	2020 (1), **2022 (1), 2023 (2)**
Yaogan-34		4	SAR Imaging	Inclined (63.4°)	**2021 (1), 2022 (2), 2023 (1)**
Yaogan-30 (CX-5)		30	ELINT	Inclined (35°)	2017 (9), 2018 (3), 2019 (3), 2020 (6), **2021 (9)**
Yaogan-31	*Jianbing*-8 (6) (JB-8)	12 (4 triplets)	ELINT	Inclined (63.4°)	2018 (3), **2021 (9)**
Yaogan-32		4	SIGINT/ELINT (?)	Sun Synchronous (2), Inclined (2)	2018 (2), **2021 (2)**
Yaogan-40		3 (1 triplet)	ELINT	Inclined (86°)	**2023 (3)**
Yaogan-35		15 (5 triplets)	Multi-Int (?) ELINT/EO/SAR	Inclined (35°)	**2021 (3), 2022 (12)**
Yaogan-36		15 (5 triplets)	Multi-Int (?) ELINT/EO/SAR	Inclined (35°)	**2022 (12), 2023 (3)**
Yaogan-39		15 (5 triplets)	Multi-Int (?) ELINT/EO/SAR	Inclined (35°)	**2023 (15)**

Gaofen (高分) is "high resolution." *Yaogan* (遥感) is "remote sensing." *Jianging* (尖兵) is "vanguard" or "pioneer/trailblazer"

Notes

[1] "C4ISR" as a recognized acronym has apparently been dropped from the latest *DOD Dictionary of Military and Associated Terms*. "ISR" (intelligence, surveillance, and reconnaissance) is currently defined as, "An integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. See, Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, (Washington DC: The Joint Staff, 2021), p. 109.

[2] Several Chinese sources add a 'K'—either C4KISR or C4ISRK—that includes an additional category of weapons systems or "killing." This reflects references to C4ISRK and concepts of integrated kill chains advanced by the U.S. military in the early 2000s. See, for example, NDU, *战略学 (2020) [Science of Military Strategy (2020)]*, p. 336.

[3] Thea Clark and Terry Moon, "Assessing the Military Worth of C4ISR Information" in *7th International Command and Control Research and Technology Symposium*, (Quebec City, Canada, CCRP, 2002), p. 2, http://www.dodccrp.org/events/7th_ICCRTS/Tracks/pdf/059.PDF.

[4] Jiang Zemin, *江泽民文选第三卷 [Jiang Zemin's Selected Works, Volume III]* (Beijing: People's Publishing House, 2006), pp. 578–579. The referenced enlarged meeting of the CMC took place in December 2002. Hu Jintao had replaced Jiang Zemin as the Chinese Communist Party general secretary during the Sixteenth National Party Congress in November 2002. However, Jiang retained the CMC chairmanship until 2004.

[5] While these insights on informationized warfare were credited to Jiang as the CMC chairman, given the nature of the organization, Jiang's observations likely reflected the consensus position of the CMC and PLA leadership.

[6] PRC National Defense University (NDU), *战役学 [Science of Campaigns]*, ed. Zhang Yuliang et al. (Beijing: NDU Press, 2006), pp. 23-27.

[7] PRC NDU, *战役学 [Science of Campaigns]*, 24. For a more recent source describing information power, see, Wu Siliang and Zhao Shiheng, "探寻战斗力生成释放科学路径" [Explore the Scientific Path to Generate and Release Combat Power], *解放军报 [PLA Daily]*, January 27, 2022, http://www.81.cn/jfjbmap/content/2022-01/27/content_308367.htm, or Wu Siliang, "现代战争视阈下的'歼灭战'" ['War of Annihilation' from the Perspective of Modern Warfare], *解放军报 [PLA Daily]*, July 7, 2022, http://www.81.cn/jfjbmap/content/2022-07/07/content_319275.htm.

[8] PRC Academy of Military Science, *战略学 (2013 年版) [Science of Military Strategy (2013 Edition)]*, ed. Shou Xiaosong (Beijing: Military Science Press, 2013), pp. 129-130.

[9] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China (aka China Military Power Report (CMPR))*, (Washington, DC: DoD, 2023, 94. https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[10] A career communications officer, Dai Qingmin was promoted to major general in 1995 and served as the dean of the PLA's Academy of Electrical Engineering through 1999. Between 2000 and 2006, Dai was the head of the General Staff Department (GSD), 4th Department (4PLA). 4PLA was responsible for radar and electronic warfare. 4PLA may have also adopted responsibility for the emerging field of computer network attack in the early 2000s. In retirement, Dai Qingmin continued to serve as the director of the PLA's Informationization Expert Advisory Committee. See, Dai Qingmin, *求道无形之境 [Seeking the Invisible Realm]* (Beijing: People's Liberation Army Press, 2009), IX.

[11] Dai Qingmin, "论夺取制信息权" [On Seizing Information Supremacy (English as provided in article)],

中国军事科学 [Chinese Military Science] 16, no. 2 (2003): pp. 9–10.

[12] "Active offense" - 积极进攻. Dai Qingmin, "创新、发展信息作战思想" [Innovating and Developing Views of Information Operations (English as provided in article)], *中国军事科学 [Chinese Military Science]* 13, no. 4 (2000): p. 75.

[13] Dai, “论夺取制信息权” [On Seizing Information Supremacy], p. 16.

[14] Dai Qingmin, “论信息化作战的‘四种能力’” [On the “Four Capabilities” of Informationized Operations], *解放军报 [PLA Daily]*, July 1, 2003, p. 6.

[15] Dai, “创新、发展信息作战思想” [Innovating and Developing Views of Information Operations], 76.

[16] Dai Qingmin, “论网电一体战” [On Integrating Network and Electronic Warfare], *中国军事科学 [Chinese Military Science]* 15, no. 2 (2002): pp. 113–114.

[17] Dai, “创新、发展信息作战思想” [Innovating and Developing Views of Information Operations], p. 76, also, Dai Qingmin, “论军队信息化建设与信息战建设” [On Development of Military lnformationization and Information Warfare (English as provided in article)], *中国军事科学 [Chinese Military Science]* 15, no. 6 (2002): p. 69.

[18] PRC National Defense University (NDU), *战略学 (2020) [Science of Military Strategy(2020)]*, ed. Xiao Tianliang (Beijing: NDU Press, 2020), pp. 182-185.

[19] Ibid, p. 265.

[20] Ibid, p. 265

[21] NDU, *战略学 (2020) [Science of Military Strategy (2020)]*, p. 183 (note “C4ISR” is rendered “C4ISRK”). See also, Wang Ronghui and Deng Shifeng, “辩证认识联合作战的单域与多域” [A Dialectical Understanding of Single-Domain and Multi-Domain Aspects of Joint Operations], *解放军报 [PLA Daily]*, January 20, 2022, http://www.81.cn/jfjbmap/content/2022-01/20/content_307852.htm.

[22] Xi Jinping, “在中国共产党第二十次全国代表大会上的报告” [Report at the 20th National Congress of the Communist Party of China] (October 16, 2022), *Xinhua News Agency [新华社]*, October 25, 2022, http://www.gov.cn/xinwen/2022-10/25/content_5721685.htm.

[23] Michael Dahm, “Chinese Debates on the Military Utility of Artificial Intelligence,” *War on the Rocks*, June 5, 2020, https://warontherocks.com/2020/06/chinese-debates-on-the-military-utility-of-artificial-intelligence/.

[24] This subsection section draws material directly from “‘Above-the-Neck’ Reforms and Operational Command & Control (C2)” in J. Michael Dahm and Alison Zhao, “China Maritime Report No. 28: Bitterness Ends, Sweetness Begins: Organizational Changes to the PLAN Submarine Force Since 2015,” China Maritime Report No. 28, China Maritime Studies Institute, June 2023, https://digital-commons.usnwc.edu/cmsi-maritime-reports/28.

[25] Edmund J. Burke and Arthur Chan, “Coming to a (New) Theater Near You: Command, Control, and Forces,” in *Chairman Xi Remakes the PLA*, ed. Phillip C. Saunders, Arthur S. Ding, Andrew Scobell, Andrew N.D. Yang, and Joel Wuthnow (Washington, DC: National Defense University Press, 2019), p. 237.

[26] Ryan D. Martinson, “China’s Far Seas Naval Operations, From the Year of the Snake to the Year of the Pig,” *Center for International Maritime Security*, February 18, 2019, https://cimsec.org/chinas-far-seas-naval-operations-from-the-year-ofthe-snake-to-the-year-of-the-pig/, and 南部战区海军远海联合训练编队紧贴实战练兵影像 [Images of the Southern Theater Command Navy Far seas Joint Training Task Force’s Actual Combat Training], *解放军报 [PLA Daily]*, February 19, 2019, p. 9, cited in Roderick Lee and Morgan Clemens, “Organizing to Fight in the Far Seas: The Chinese Navy in an Era of Military Reform,” China Maritime Report No. 9, China Maritime Studies Institute, October 2020, p. 6, https://digital-commons.usnwc.edu/cmsimaritime-reports/9/.

[27] While PLAN carrier strike group operations east of Taiwan would most likely be controlled or at least coordinated through the Eastern Theater, the carrier strike groups belong to the Northern TC Navy (CV-16 *Liaoning*) and Southern TC Navy (CV-17 *Shandong*). Michael Dahm, “Lessons from the Changing Geometry of PLA Navy Carrier Ops,” *Proceedings* 149/1, no. 1439 (January 2023), https://www.usni.org/magazines/proceedings/2023/january/lessons-changing-geometry-pla-navy-carrier-ops.

[28] Terms for sub-centers appear in a number of Chinese language sources. See, for example, Xun Ye, Li Wenyuan, Wu Dongdong, and Ji Yongsong, “新体制下战区战时联勤组织指挥模式研究” [Research on the Command of Theater Wartime Joint Logistics Organizations Under the New System], *军事交通学院学报 [Journal of the*

Military Transportation University], 22, no. 11 (November 2020), p. 69, Zeng Zhudong, "实战实训,锤炼新任干部" [Practical Training Tempers New Cadres], *人民海军 [People's Navy]*, 22 October 2020, p. 3.

[29] Dahm and Zhao, p. 5.

[30] For a detailed assessment of PLA Rocket Force organization, see, Ma Xiu, *PLA Rocket Force Organization,* (Montgomery, AL: China Aerospace Studies Institute, 2022), https://www.airuniversity.af.edu/CASI/Display/Article/3193056/pla-rocket-force-organization/.

[31] The PLANAF retained control of its three J-15 aircraft carrier fighter battalions and a single land-based J-11 fighter battalion on Hainan Island for operations over the South China Sea. The PLANAF also retained control of its special mission aircraft and uncrewed aerial vehicle (UAV) regiments for maritime surveillance, communications, and airborne command and control of PLAN forces. For an excellent overview of the PLANAF reorganization, see, Rod Lee, "PLA Naval Aviation Reorganization 2023," *China Aerospace Studies Institute*, July 31, 2023, https://www.airuniversity.af.edu/CASI/Display/Article/3475163/pla-naval-aviation-reorganization-2023/.

[32] Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* Report prepared for the USCC, (McLean, VA: Northrop Grumman, 2009), p. 32, https://www.govinfo.gov/content/pkg/GOVPUB-Y3-PURL-LPS123422/pdf/GOVPUB-Y3-PURL-LPS123422.pdf.

[33] Costello and McReynolds, p. 21.

[34] Kristin Burke, *The PLA's New Base for Space Situational Awareness*, (Mongomery, AL: China Aerospace Studies Institute, September 2023), 1. https://www.airuniversity.af.edu/CASI/Display/Article/3498588/the-plas-new-base-for-space-situational-awarenessopportunities-and-challenges-f/.

[35] Costello and McReynolds, p. 22.

[36] Ibid.

[37] Ibid.

[38] Western assessments that the SSF has leading role in PLA psychological operations are probably overstated. While there appear to be many military academics that write on psychological operations, there is little evidence to suggest that the SSF has organizational responsibly for the type of PLA/PRC psychological operation that might be directed against the U.S. or its allies in a counter-intervention operation. As part of the 2015 reforms, the SSF reportedly inherited the 311 Base (61716 部队) from the former General Staff Department, General Political Department (GPD). Limited, but credible open-source intelligence indicates the 311 Base is focused exclusively on psychological warfare and propaganda that targets public opinion on Taiwan. Very little evidence has emerged that the SSF has control over psychological or propaganda operations against other targets, regionally or globally. SSF cyber capabilities certainly may play a role in collecting intelligence and spreading disinformation as part of a broader malign influence campaign, but there is scant evidence that the SSF has overall responsibility for political warfare within the PLA or the PRC government. See, Mark Stokes and Russel Hsiao, *The People's Liberation Army General Political Department* (Washington, DC: 2049 Institute, 2013), 29, https://project2049.net/wp-content/uploads/2018/04/P2049_Stokes_Hsiao_PLA_General_Political_Department_Liaison_101413.pdf, also, John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, (Washington, DC: National Defense University, 2018), p. 17, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

[39] Mark Stokes, *The PLA General Staff Department Third Department Second Bureau,* Project 2049 Institute, July 27, 2015, 13, https://project2049.net/wp-content/uploads/2018/04/P2049_Stokes_PLA_General_Staff_Department_Unit_61398_072715.pdf.

[40] Krekel, p. 32.

[41] Elsa B. Kania and John Costello, "Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power," Journal of Strategic Studies, 44, no. 2 (2021): p. 253, https://doi.org/10.1080/01402390.2020.1747444, see also, Zhang Dapeng, Kang Zizhan, Wang Lingshuo, and Zhang Shaobo, "淬炼新域新质'新锋刃'" [Tempering the New Domain, New Quality, 'New Forward Edge'], *解放军报 [PLA Daily]*, December 21, 2022, http://www.mod.gov.cn/gfbw/wzll/yw_214068/4928766.html.

[42] Chen Xin and Zhang Nenghua, "连长翁春芳: 守护挖不断冲不垮的高原通信线" [Company Commander Weng Chunfang: Guarding and Constantly Excavating Plateau Communication Lines that Cannot be Broken], (source *央广网 [CCTV]) PRC Ministry of National Defense*, December 3, 2018, http://www.mod.gov.cn/gfbw/tp_214132/zgjr/4831084.html.

[43] Kania and Costello, 253. Note, the Information Communication Base (ICB) should not be confused with the CMC Joint Staff Department ICB – Information and Communications Bureau (信息通信局) or JSD ICB.

[44] Zhang Dapeng, Yu Tao, Xu Yuzhe, and Zhang Shaobo, "体系支撑 信息制胜" [System Support, Information Victory], *解放军报 [PLA Daily]*, October 22, 2022, http://www.81.cn/2022zt/2022-10/22/content_10194235.htm. Apparently, as part of the ICB subordination/reorganization, in 2020, the ICB (61001 部队) launched the official "The Eternal Wave" (永不消逝的电波) across seven social media platforms, Yang Fanfan, "永不消逝的电波" 官方授权号开通试运行" [The Official Authorized Account of "The Eternal Wave" has been Launched for Trial Operation], *中国军网 [China Military Network]*, November 20, 2020, http://www.81.cn/yw_208727/9939915.html. In media articles highlighting ICB personnel, images show uniformed personnel with SSF shoulder patches. See, for example, Zhang Xiushan et al, "'金键'精兵" ['Golden Key' Elite Soldier], *解放军报 [PLA Daily]*, December 20, 2022, http://www.81.cn/jfjbmap/content/2022-12/20/content_330242.htm.

[45] Zhang Xiaohan, "学思践悟, 重点突破备战保通" [Study, Think and Practice, Focus on Breakthroughs & Prepare for Success], *解放军报 [PLA Daily]*, April 2, 2023, http://www.mod.gov.cn/gfbw/wzll/yw_214068/16213872.html. There is conflicting information about the organization and subordination of PLA information communication forces. On the one hand, it seems clear that the lead IC Base (61001 Unit), which sources indicate is physically located in southwest Beijing, commands several SSF ICB brigades throughout China. However, PLA media makes numerous references to apparently remote "information communication bases." This may be an informal term that simply describes where IC brigades and other ICB units are physically located. See, for example, "情注一缆通滇藏 – 记某信息通信基地四营五连连长翁春芳" [A Cable Connects Yunan and Tibet – A Record of Weng Chunfang, Commander of the Fourth Battalion Fifth Company of an Information Communications Base], *新华网 [XinhuaNet]*, December 3, 2018, http://www.xinhuanet.com/politics/2018-12/03/c_1123801663.htm. Attempts to sort out these inconsistencies are further exacerbated by the fact that other PLA services maintain their own information communication brigades and information communication units. See, "正赛 (通信兵专业比武邀请赛)" [Main Match (The Signal Corps Professional Competition Invitational Tournament)], *永不消逝的电波 [The Eternal Wave]*, June 27, 2023, https://m.thepaper.cn/newsDetail_forward_23645590. Additional research on PLA communication and signal corps organization, roles, and responsibilities is required.

[46] Per the 2023 CMPR, the SSF Space Systems Department is also called the Aerospace Force (ASF) (航天部队); the SSF Network Systems Department is also called the Cyberspace Force (CSF) (网络空间部队), see, Office of the Secretary of Defense, p. 70.

[47] See, for example, Zhuang Yong and Qu Liang, "向战发力！地方专家骨干走进某预备役信息通信大队" [Applying Force to War! Key Local Experts Visited a Reserve Information Communication Group (Brigade)], *解放军报 [PLA Daily]*, June 13, 2023, http://www.81.cn/zz_208563/jdt_208564/16230833.html.

[48] U.S. Air University's China Aerospace Studies Institute (CASI) briefly mentions that "The Network Systems Department likely commands… an information and communications base…" See, CASI, *PLA Aerospace Power: A Primer on Trends in China's Military Air, Space, and Missile Forces*, 3rd ed. (Montgomery, AL: China Aerospace Studies Institute, 2022), 72, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2022-08-15%20PLA%20Primer%203rd%20edition.pdf.

[49] See, for example, references to the SSF Eastern Base, "区领导开展 '八一' 走访慰问活动" [District Leaders Carried Out 'Bayi' Visit and Condolence Activities], *Xinjian District People's Government*, August 8, 2020, http://xjq.nc.gov.cn/xjqrmzf/zhxw/202008/e28802a974aa465abf061339f918cbd1.shtml, or Central Base listed as a technology customer in, 星环信息科技（上海）股份有限公司, 首次公开发行股票并在科创板上市申请文件 [Xinghuan Information Technology (Shanghai) Co., Ltd., Application Documents for Initial Public Offering of Shares and Listing on the Science and Technology Innovation Board], May 13, 2022, p. 8-1-1-84, http://static.sse.com.cn/stock/information/c/202205/222fed3f8d34438594d79de57679386f.pdf.

[50] For an earlier assessment, see, Costello and McReynolds, p. 32.

[51] Graphic derived from J. Michael Dahm, *Introduction to South China Sea Military Capabilities Studies*, (Laurel, MD: Johns Hopkins Applied Physics Laboratory, 2020), p. 6. https://www.jhuapl.edu/sites/default/files/2022-12/IntroductiontoSCSMILCAPStudies.pdf.

[52] In over twenty-years of counterterrorism/counter-insurgency operations in Southwest Asia and elsewhere, the U.S. military quickly learned that its sophisticated C4ISR system-of-systems was often challenged and, in some cases, defeated by a primitive adversary C4ISR system-of-systems that consisted of human lookouts, cell phones, and messengers.

[53] For a comprehensive examination of PLA concepts of system-of-systems confrontation, see, Jeffery Engstrom, *Systems Confrontation and System Destruction Warfare*, RR-1708-OSD (Santa Monica, CA: RAND, 2018), https://www.rand.org/pubs/research_reports/RR1708.html.

[54] Unidentified PRC National Defense University authors, "信息化战争 – 未来战争基本形态" [Informationized Warfare – The Basic Form of Future Warfare], *北京日报 [Beijing Daily]*, February 21, 2001, http://www.people.com.cn/GB/junshi/192/3868/20010221/400680.html.

[55] Liu Jixian, "世界新军事变革形势与应对思考" [Reflections on the Situation and Response to the World Revolution in Military Affairs], *学习时报 [Study Times]*, June 11, 2007.

[56] Office of Navy Intelligence, *The PLA Navy: New Capabilities and Missions for the 21st Century* (Washington, DC: Office of Navy Intelligence, 2015), p. 28, https://www.oni.navy.mil/portals/12/intel agencies/china_media/2015_pla_navy_pub_print_low_res.pdf?ver=2015-12-02-081233-733.

[57] Li Xiaokun, "China sails through 'first island chain,'" *China Daily,* August 2, 2013, https://www.chinadaily.com.cn/cndy/2013-08/02/content_16864064.htm.

[58] For example, Michael Dahm, "Lessons from the Changing Geometry of PLA Navy Carrier Ops.

[59] Yue Jiucheng, 亲历国防通信网建设 30 年 [30-Years' Experience Building the National Defense Communication Network], *新华月报 [Xinhua Monthly]*, no 8. (2008). https://web.archive.org/web/20240313114400/http://www.wenxue100.com/baokan/58246.thtml.

[60] Xie Feng, Li Haiqiang, and Wu Yanmei, "军民互联确保网络无限畅通" [Military and Civilian Interconnection Ensures Unlimited Network Connectivity], *Science & Technology Daily*, September 24, 2015, p. 12.

[61] J. Michael Dahm, *SCS MILCAP Study: Undersea Fiber-Optic Cable and Satellite Communications*, NSAD-R-20-046 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory (JHU/APL), 2020), pp. 2-3, https://www.jhuapl.edu/sites/default/files/2022-12/UnderseaFiber-OpticCableandSATCOM.pdf.

[62] Robert S. Ross, "The 1995-1996 Taiwan Strait Confrontation," *International Security*, Vol. 25, No. 2 (Fall 2000), pp. 120-121.

[63] "Qu Dian" – "区电" for "区域综合电子系统." Andrew Erickson and Ryan Martinson, *China's Near Seas Combat Capabilities*, CMSI Red Book, no. 11 (Newport, RI: U.S. Naval War College, 2014), p. 89. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1010&context=cmsi-red-books.

[64] Michael Dahm, "China's Desert Storm Education," *Proceedings,* 147/3 no. 1,417 (March 2021), https://www.usni.org/magazines/proceedings/2021/march/chinas-desert-storm-education.

[65] Kevin Pollpeter et al, *Enabling Information-Based System of System Operations, The Research, Development, and Acquisition Process for the Integrated Command Platform*. SITC Policy Briefs no. 9 (San Diego, CA: Study of Innovation and Technology in China, 2014), https://escholarship.org/uc/item/6f26w11m.

[66] The likely skywave OTH radar transmitter is in Hubei, China at 32°20'16.9"N 112°42'14.6"E https://maps.app.goo.gl/2sqmyr41oxhDLa9E6. The receiver is located at 31°37'19.7"N 111°54'51.2"E, https://maps.app.goo.gl/d5ErfVHqKn6wXruQ6.

[67] J. Michael Dahm, *SCS MILCAP Study: Special Mission Aircraft and Unmanned Systems,* NSAD-R-20-090 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory (JHU/APL), 2020), p. 5, https://www.jhuapl.edu/sites/default/files/2022-12/SpecialMissionAircraftandUnmannedSystems.pdf.

[68] "运-9 到底有多厉害?" [How Powerful is the Y-9?], CCTV.com, November 24, 2018, http://news.cctv.com/2018/11/24/ARTIPC0zeumXkIhGFoWUTsZS181124.shtml, cited in J. Michael Dahm, *SCS MILCAP Study: Air & Surface Radar,* NSAD-R-20-047 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory (JHU/APL), 2020), p. 9

[69] Liu Xuanzun, "China Mass-Produces Special Mission Aircraft," *Global Times,* December 8, 2019, https://www.globaltimes.cn/content/1172715.shtml, cited in cited in J. Michael Dahm, *SCS MILCAP Study: Air & Surface Radar,* 5.

[70] Eli Turk, *PLAN Special Mission Aviation Air Base Renovation and Expansion Activities*, (Montgomery, AL: China Aerospace Studies Institute, 2022), 1, https://www.airuniversity.af.edu/CASI/Display/Article/3505090/plan-special-mission-aviation-air-base-renovation-and-expansion-activities/.

[71] Japan Joint Staff, press releases, 2020-2023, www.mod.go.jp/js/press/index.html.

[72] Bill Gertz, "Exclusive: China begins military flights from disputed South China Sea Bases: AWACS, surveillance planes on two reef bases signal routine PLA air operations from Spratlys," *The Washington Times*, July 13, 2021, https://www.washingtontimes.com/news/2021/jul/13/china-begins-military-flights-disputed-south-china/.

[73] Japan Ministry of Defense, Joint Staff, press releases, 2020-2023, www.mod.go.jp/js/press/index.html.

[74] Japan Joint Staff Press Release: Chinese Military Aircraft Trends (Tokyo: Ministry of Defense, August 23, 2023), 1, https://www.mod.go.jp/js/pdf/2023/p20230825_04.pdf.

[75] J. Michael Dahm, *SCS MILCAP Study: Undersea Fiber-Optic Cable and Satellite Communications*, pp. 6-7, 11.

[76] Andrew S. Erickson, "Quick Look Summary – CMSI's 11-13 April 2023 Conference: Chinese Undersea Warfare: Development, Capabilities, Trends," *Andrew S. Erickson* (blog), May 5, 2023, https://www.andrewerickson.com/2023/05/quick-look-summary-cmsis-11-13-april-2023-conference-chinese-undersea-warfare-development-capabilities-trends/.

[77] Rick Joe, "The Chinese Navy's Growing Anti-Submarine Warfare Capabilities," *The Diplomat,* September 12, 2018, https://thediplomat.com/2018/09/the-chinese-surface-fleets-growing-anti-submarine-warfare-capabilities/.

[78] *United States Strategic Command and United States Space Command in review of the Defense Authorization Request for FY 2025 and the Future Defense Program*, 118th Congress, February 29, 2024, (statement of General Stephen N. Whiting Commander, United States Space Command), https://www.armed-services.senate.gov/imo/media/doc/whiting_statement.pdf.

[79] Prior to 2000, the only military related satellites previously operated by the PRC were the Jianbing-1/1A JB-1 electro-optic imagery satellites, which conducted 14 missions between 1975-1993. The JB-1/1A returned film to earth using recoverable capsules.

[80] For comparison, the U.S. conducted 116 space launches in 2023. Andrew Jones, "Chinese Satellite Internet Mission Rounds Off Record Year for Global Launches," *Space News*, December 31, 2023, https://spacenews.com/chinese-satellite-internet-mission-rounds-off-record-year-for-global-launches/

[81] Union of Concerned Scientists (UCS) Satellite Database, 1 May 2023, (PRC owned and operated satellites in GEO, accessed March 13, 2024), https://www.ucsusa.org/resources/satellite-database Supplemented by current information from Gunter D. Krebs, "Gunter's Space Page," accessed March 13, 2024, from https://space.skyrocket.de/index.html.

[82] Clayton Swope, *No Place to Hide: A Look into China's Geosynchronous Surveillance Capabilities* (Washington, DC: Center for Strategic and International Studies, 2024), https://www.csis.org/analysis/no-place-hide-look-chinas-geosynchronous-surveillance-capabilities.

[83] Andrew Jones, "China launches first geosynchronous orbit radar satellite," *Space News*, August 14, 2023, https://spacenews.com/china-launches-first-geosynchronous-orbit-radar-satellite/.

[84] The 213 LEO ISR satellites plus the 14 probable GEO ISR satellites is 227 ISR satellites. This is well short of the PRC's reported 359 ISR satellites. The larger number probably included "one-off" systems not included in this report as well as "Earth observation" satellites that have legitimate scientific, surveying, or meteorological uses.

There are also a number of older PLA LEO satellites that are still in orbit that are either beyond their service life or may not provide significant capabilities in a PLA counter-intervention operation.

[85] Karthik Naren, "China Launches Gaofen 11-04," *Space Intelligence*, December 27, 2022, https://www.spaceintel101.com/post/china-launches-gaofen-11-04.

[86] See, for example, Chris Formeller, "Introducing 15 cm HD: The Highest Clarity From Commercial Satellite Imagery," *Maxar* (blog), November, 12, 2020, https://blog.maxar.com/earth-intelligence/2020/introducing-15-cm-hd-the-highest-clarity-from-commercial-satellite-imagery.

[87] Chang Guang Satellite Technology Co., Ltd., "About," Accessed March 15, 2024, https://www.jl1global.com/about/.

[88] Ling Xin, "China Sends Record 41 Satellites to Join Jilin-1 Hi-Res Constellation," *South China Morning Post*, June 19, 2023, https://www.scmp.com/news/china/science/article/3224636/china-sends-record-41-satellites-join-jilin-1-hi-res-constellation.

[89] "China's Commercial CERES-1 Y8 Rocket Launches New Satellite," *Xinhua*, August 25,2023, https://english.news.cn/20230825/8dc82f06f7ae4557ac5626c2e13dc4b9/c.html.

[90] Gosnold, "China Completes the Yaogan-30 Constellation," *SatelliteObservation.net* (blog), November 25, 2020, https://satelliteobservation.net/2020/11/25/china-completes-the-yaogan-30-constellation/.

[91] Andrew Jones, "China Launches Trio of Yaogan-31 Ocean Reconnaissance Satellites," *Space News*, February 24, 2021, https://spacenews.com/china-launches-trio-of-yaogan-31-ocean-reconnaissance-satellites/.

[92] Yaogan-36 03A/B/C orbits, August 28, 2023, ~1700 GMT, data and visualization from SatFlare, http://www.satflare.com.

[93] "GLOBALink | Open-sea testing of China's first low-Earth orbit broadband communication test constellation is conducted in the South China Sea," *Xinhua,* June 17, 2023, https://english.news.cn/20230617/da2429ac13e0486c99b5dc054594a659/c.html.

[94] Stephen Chen, "Private Internet Satellite Company Joins China's Hypersonic Race," *South China Morning Post,* April 22, 2023, https://www.scmp.com/news/china/science/article/3217714/private-internet-satellite-company-joins-chinas-hypersonic-race.

[95] Colin Demarest, "China May Struggle in Electromagnetic Spectrum Fighting, Pentagon Says," *C4ISRNet,* October 23, 2023, https://www.c4isrnet.com/electronic-warfare/2023/10/23/china-may-struggle-in-electromagnetic-spectrum-fighting-pentagon-says/. See also, Mark Pomerleau, "China Perceives Shortfalls Operating in Complex Electromagnetic Spectrum Environment: Pentagon," *DefenseScoop,* October 19, 2023, https://defensescoop.com/2023/10/19/china-perceives-shortfalls-operating-in-complex-electromagnetic-spectrum-environment-pentagon-report/.

[96] Larry Wortzel, *The Chinese People's Liberation Army and Information Warfare,* (Carlisle, PA: U.S. Army War College Press, 2014), p. 11. https://press.armywarcollege.edu/monographs/506/.

[97] Bernard Cole, "China's Navy Prepared: Domestic Exercises, 2000–2010," in *Learning by Doing, the PLA Trains at Home and Abroad*, ed. Roy Kamphausen, David Lai, and Travis Tanner (Carlisle, PA: US Army War College Press, 2012), 25–26, cited in J. Michael Dahm, *Electronic Warfare and Signals Intelligence*, South China Sea Military Capability Series (Laurel, MD: Johns Hopkins Applied Physics Laboratory, 2020), p. 2. https://www.jhuapl.edu/sites/default/files/2022-12/EWandSIGINT.pdf.

[98] Hu Jintao, then Party Secretary and Chairman of the CMC stated, "*Information dominance is in effect electromagnetic dominance; therefore, we should not only place high-tech weapons and equipment into complex electromagnetic environments to get them trained and tested, but also should carry out comprehensive exercises and drills with tactical backgrounds under such conditions."* Leng Feng, *Toward the Transformation of PLA Military Training Under Conditions of Informationization* (Stockholm: Institute for Security and Development Policy, 2014), p. 23, https://web.archive.org/web/20201231030347/https://isdp.eu/content/uploads/publications/2014-leng-feng-toward-the-transformation-of-PLA-military-training.pdf.

[99] PRC State Council Information Office, "中国的军事战略 (2015 年 5 月) [China's Military Strategy (May, 2015)]," see section V, "Preparation for Military Struggle," November 1, 2017, http://www.81.cn/jwzl/2017-11/01/content_7808797_7.htm.

[100] PRC State Council Information Office, "新时代的中国国防" [China's National Defense in the New Era], see section II, China's Defensive National Defense Policy in the New Era, July 2019, http://www.81.cn/zt/2023nzt/rmjdlsyct/16230673.html.

[101] See, for example the likely SSF ECM brigade garrison and vehicles in Qinhuangdao, Hebei, PRC at 39°53'17.7"N 119°26'36.8"E, https://maps.app.goo.gl/TgxKbq8VDn69NK3W8.

[102] Michael R. Gordon and Jeremy Page, "China Installed Military Jamming Equipment on Spratly Islands, U.S. Says," Wall Street Journal, April 9, 2018, https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320, cited in, J. Michael Dahm, *Electronic Warfare and Signals Intelligence*, p. 4.

[103] J. Michael Dahm, *Electronic Warfare and Signals Intelligence*, p. 7.

[104] As of mid-2023, the PLAAF may have only had seven J-16D. See, Akhil Kadidal, "China Adds Additional J-16s, J-20s to Operational Units," *Janes,* July 7, 2023, https://www.janes.com/defence-news/news-detail/china-adds-additional-j-16s-j-20s-to-operational-units.

[105] Andrew Tate, "PLAAF Operating ECM Variant of Y-9 Aircraft," *Janes*, March 11, 2019, https://www.janes.com/defence-news/news-detail/plaaf-operating-ecm-variant-of-y-9-aircraft.

[106] Guo Yuandan, Liu Xuanzun, and Leng Shumei, "PLA's J-16D Electronic Warfare Aircraft Spotted for 1st Time Near Taiwan," *Global Times,* January 25, 2022, https://www.globaltimes.cn/page/202201/1246818.shtml.

[107] An unidentified missile suspected of being an anti-radiation missile appeared in a PLAAF video in 2020. See, Liu Xuanzun, "Air Force Video Reveals Chinese Fighter Jet's Mysterious New Missile," *Global Times,* November 11, 2020, https://www.globaltimes.cn/content/1206531.shtml.

[108] "TL-30 Anti-Radiation Loitering Missile," *China Defence*, accessed March 10, 2024, https://www.militarydrones.org.cn/tl-30-missile-p00664p1.html.

[109] Defense Intelligence Ballistic Missile Analysis Committee, *2020 Ballistic Missile and Cruise Threat,* (Dayton, OH: National Air and Space Intelligence Center (NASIC), 2020), p. 14, https://media.defense.gov/2021/Jan/11/2002563190/-1/-1/1/2020 BALLISTIC AND CRUISE MISSILE THREAT_FINAL_2OCT_REDUCEDFILE.PDF.

[110] The technology in the PRC-produced ASN-301 probably originated with the Israeli Harpy program. See, Ami Rojkes Dombe, "China Unveils a Harpy-Type Loitering Munition," *Israel Defense,* January 3, 2017, https://www.israeldefense.co.il/en/node/28716. See also, "ASN-301 Anti-Radiation Radar Loitering Munition Suicide Drone System," *China Defence*, accessed March 10, 2024, https://www.militarydrones.org.cn/china-asn-301-anti-radiation-uav-system-p00145p1.html.

[111] Kristin Burke, PLA Counterspace Command and Control, (Mongomery, AL: China Aerospace Studies Institute, September 2023), 30. https://www.airuniversity.af.edu/CASI/Display/Article/3612979/pla-counterspace-command-and-control/.

[112] See Google Earth archived images, January 5, 2021; June 18, 2021; and March, 2022 of Langfang, China, 39°34'13.9"N 116°45'38.7"E, https://maps.app.goo.gl/v41mXoqV4kwNiqgy6.

[113] Steve Trimble, "Satellite Imagery Exposes China's Space Jammer Buildup," *Aviation Week*, November 1, 2022, https://aviationweek.com/defense-space/sensors-electronic-warfare/satellite-imagery-exposes-chinas-space-jammer-buildup.

[114] Matthew P. Funaiole, Joseph S. Bermudez, Jr., and Brian Hart, "China is Ramping Up its Electronic Warfare and Communications Capabilities Near the South China Sea," *Center for Strategic and International Studies*, December 17, 2021, https://www.csis.org/analysis/china-ramping-its-electronic-warfare-and-communications-capabilities-near-south-china-sea. This article identifies a new SSF base near Mumian, Hainan Island. The suspected EW vehicles identified in the article are, in fact, SATCOM jammers.

[115] J. Michael Dahm, *SCS MILCAP Study: Air and Surface Radar,* NSAD-R-20-047 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory (JHU/APL), 2020), pp. 2-12, https://www.jhuapl.edu/sites/default/files/2022-12/AirandSurfaceRadar_v3.pdf.

[116] J. Michael Dahm, *SCS MILCAP Study: Inter-Island Communications,* NSAD-R-20-048 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory (JHU/APL), 2020), pp. 2-6, https://www.jhuapl.edu/sites/default/files/2022-12/Inter-IslandCommunications.pdf.

[117] The Joint Staff, *Joint Pub 3-85 – Joint Electromagnetic Spectrum Operations,* (Washington, DC: Department of Defense, 22 May 2020), p. v, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.

[118] PRC Radio Management Bureau, "中华人民共和国无线电管制规定, 2010" [PRC Radio Control Regulations, 2010], *PRC Ministry of Industry and Information Technology*, November 3, 2021, https://wap.miit.gov.cn/jgsj/wgj/flfg/art/2021/art_1f8b7b710b444344abe4c530fd3c5c8a.html.

[119] Liu Yiwei, 频谱管控大队转隶军委联合参谋部 [Spectrum Management and Control Group (Dadui) Transferred to the CMC Joint Staff Department], *解放军报 [PLA Daily],* March 21, 2016, https://web.archive.org/web/20160403034749/https://military.china.com/news/568/20160321/22221894.html.

[120] "Request for Proposals on China's Advanced Remote Sensing Technologies and Applications," *U.S.-China Economic and Security Review Commission*, August 8, 2023, https://www.uscc.gov/research/request-proposals-remote-sensing.

[121] U.S. GAO, *Battle Management: DoD and Air Force Continue to Define Joint Command and Control Efforts,* GAO-23-105495, (Washington, DC: GAO, 2023), p. 16, https://www.gao.gov/assets/gao-23-105495.pdf.

[122] J. Michael Dahm, *SCS MILCAP Study: Special Mission Aircraft and Unmanned Systems*, p. 6.

[123] J. Michael Dahm, *SCS MILCAP Study: Special Mission Aircraft and Unmanned Systems*, p. 22. Data from "BZK-005C," 北京北航天宇长鹰无人机科技有限公司 [Beihang UAS Technology Co, Ltd.], "Wing Loong I UAS," "Wing Loong I-D UAS," "Wing Loong II UAS," trade brochures (中国航空工业集团公司 [Aviation Industry Corporation of China, Ltd.], 2018); Deng Xiaoci and Liu Xuanzun, "Maritime Version of China's CH-5 Drone Makes First Test Flight," *Global Times*, July, 16, 2020, https://www.globaltimes.cn/content/1194771.shtml; "Tengden TB-001 Drone," *China Defence*, accessed March 10, 2024, https://www.militarydrones.org.cn/tb001-reconnaissance-strike-drone-p00209p1.html; Thomas Newdick, "Japanese Fighters Intercept China's High-Flying WZ-7 Drone For First Time, *The Warzone*, January 2, 2023, https://www.twz.com/japanese-fighters-intercept-chinas-high-flying-wz-7-drone-for-first-time.

[124] Data aggregated from multiple databases, visualization tools, and media sources including: UCS Satellite Database, https://www.ucsusa.org/resources/satellite-database; Gunther's Space Page, https://space.skyrocket.de/index.html; Satflare, https://www.satflare.com/home.asp; and N2YO, https://www.n2yo.com/.

[125] Ibid.

[126] Ibid.