TAKSHASHILA INSTITUTION

New Frontiers in China's Military Organisation

From SSF to ISF, CSF and ASF

Anushka Saxena

Takshashila Discussion Document 2025-28
Version 1.0, October 2025

A study reviewing the efficiencies and challenges of China's three new strategic military forces on information, cyber and aerospace.

Recommended Citation:
Anushka Saxena, ``New Frontiers in China's Military Organisation'', Takshashila Discussion Document 2025-28, Version 1.0, October 2025, The Takshashila Institution

Contents

1 Executive Summary

This paper finds that the Chinese People's Liberation Army's three latest support forces, the Information Support Force, the Cyberspace Force, and the Military Aerospace Force, are reformed and specialised units created to establish the military's dominance over the "three strategic commanding heights" in new-age warfare. They bring with themselves three key opportunities and challenges:

- **Unified Force Structure Drives Offensive Capability and Risk:** The restructuring of the PLA's Cyberspace and Information Support Forces centralises offensive cyber and electromagnetic warfare expertise, potentially streamlining tactics and enhancing operational sophistication. Simultaneously, however, it likely heightens risks of unintended escalation and demands careful differentiation between peacetime and wartime activities.
- **Persistent Integration and Adaptation Challenges:** Despite reorganisation, the PLA faces persistent challenges integrating diverse services and theaters. Technological obsolescence, resource management, and personnel informational adaptability remain key vulnerabilities, especially for network-centric operations and in high-stress combat environments.
- **Strategic Momentum Meets Institutional Fragility:** While the Aerospace Force's modernisation underscores China's ambition to counter US capabilities in space and missile domains, ongoing issues with equipment maintenance, infrastructure protection, and corruption will likely continue to plague force credibility and operational effectiveness, exposing these new forces to both internal and external pressures.

2 Introduction

The People's Liberation Army (PLA) Strategic Support Force (SSF) was disbanded on April 19, 2024, and was restructured into three independent support arms under direct command of the Central Military Commission (CMC). The SSF already included the Space and Network Systems Departments, and so the new Aerospace (ASF) and Cyberspace (CSF) forces became theater-level organisations absorbing the erstwhile mandates of their vice-theater-level predecessors. The Information Support Force (ISF), however, was a wholly new creation, amalgamating functions of other intelligence- and reconnaissance-related departments of the SSF.

There are three potential reasons behind the disbandment of the SSF and the creation of these independent support arms.

Firstly, the three newly-established forces cover five major domains: intelligence, technical reconnaissance, electronic countermeasures, cyber offence-and-defence, and psychological warfare. Being under direct control of the CMC, they also effectively bring the PLA closer to the centrally-mandated goals of becoming an "informatised" and "intelligentised" force capable of fighting and winning new-age wars. Further, their formation is a central pillar for fulfilling the Chinese military's need to "coordinate the construction and application of network information systems," as highlighted in Chinese President Xi Jinping's 'Report to the 20th National Congress of the Communist Party of China'.[1]

Going further back, they can also be linked to the 2019 'White Paper on China's National Defense in the New Era',[2] which identified information, space, and cyberspace as the key emerging security domains, and the "three strategic commanding heights" of the military. The document stressed the accelerating shift to "informationized" and intelligent warfare; the strategic importance of space as the commanding height of great-power competition; and the increasing severity of cybersecurity threats. Hence, the coming into being of the ISF, CSF, and ASF, and their subsequent endeavours, are geared towards improving the PLA's joint and multi-domain combat capabilities based on the principles of systems-of-systems warfare and the construction and effective utilisation of network information systems in new-age battle. It thus also made symbolic sense for General Li Wei, the newly appointed political commissar of the ISF, to address the launch ceremony for the force instead of its commander, Lt. Gen. Bi Yi. Li said the force is determined to "Implement Chairman Xi's important instructions, resolutely obey the command of the party Central Committee, the Central Military Commission and Chairman Xi, faithfully perform duties, and never betray the trust of the party and the people."[3]

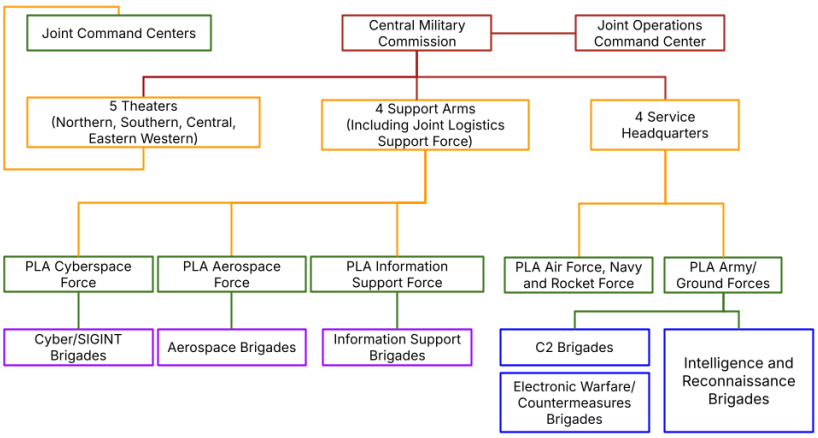

Figure 1: Non-exhaustive organogram of intelligence and network-centric combat-related units in the PLA and CMC | Prepared by Author | Data sourced from 81.cn and US Department of Defense's 2024 Report, 'Military and Security Developments Involving the People's Republic of China'[1]

Secondly, the breakup of the SSF shows that the amalgamation of complex new and emerging warfare domains – including cyberwarfare, space and information – under a single umbrella support force was a failed experiment for China. The SSF brought together several specialised branches of the CMC General Staff Department, including the Third Department, which handled espionage and technical reconnaissance in cyberspace, the Informatization Department, which worked on information systems security and the Aerospace Reconnaissance Bureau. These units had suffered from overspecialisation within their respective organisational silos, which in turn meant there was virtually no interchange of resources. That was the motivation for creating the SSF as a joint force encompassing specialists from the space, cyberspace and information domains under a single commander with authority to mobilise resources jointly. Now, it seems that the SSF suffered from similar problems as the GSD did, leading to the decision to divide the branch into three constituent parts under the direct control of the CMC, which Xi personally chairs.

[1] "Military and Security Developments Involving the People's Republic of China: 2024," Annual Report to Congress: U.S. Department of Defence, 18 December 2024.

Interchange of resources pertains to the sharing of best practices, tactical know-how, and even personnel for training between different services, units, or even departments of a single support force. For example, despite progress in integrating cyber and space operations, the Strategic Support Force still retained overlapping, yet siloed functions between its two departments on 'Space Systems' and 'Network Systems'. This meant that full structural integration remained incomplete and certain 'siloed' tendencies persisted. See: China Security Strategy Report 2022, The National Institute for Defense Studies, Japan.

Thirdly, their creation can be potentially linked to inefficiencies in the SSF and the need felt by the CMC to bring their house in order, given the vitality of network-centricity in new-age warfare. The past few years have yielded significant revelations about the extent of procurement-related corruption in the PLA. Xi's long-term strategy of leveraging his anti-corruption campaign to put loyalists into key positions in the military has clearly backfired. This is quite evident from the disappearances and purges of former Minister of National Defense Li Shangfu, former Rocket Force political commissar Xu Zhongbo and former SSF Commander Ju Qiansheng. Though there is no official confirmation, Ju's disappearance in February 2024 spurred intense speculation regarding the effectiveness of the SSF and possible corruption in the erstwhile branch.[4] With the restructuring of domains previously under the command of the SSF into specialised forces under the direct control of the CMC, it is evident that the country's highest military decision-making body wishes to keep a close eye on potential graft in equipment procurement and management. The restructuring will simplify the chain of accountability by removing the SSF commander as a mediator.

The likely goal in terms of improving efficiency, is to ensure that nothing interferes with the preparedness of the military's space, cyberspace and information warfare units to avoid presenting vulnerabilities that competent potential foes like the US might exploit to handicap the PLA in "informatization-led" warfare. This is also given that for the last two decades, the PLA has been referred to as a "half-mechanised, half-informatised" force.[5]

This study assesses the mandate and endeavours of the ISF, the CSF and ASF, in the one-and-a-half years since their establishment. The paper is divided into three subsequent sections, covering each of the forces individually, and focusing on aspects such as their combat training, equipment, recruitment, parade displays, and mandates.

3 The Information Support Force's Networked Endeavours

On the day of the establishment of the three new support services, Senior Colonel Wu Qian, spokesperson for the Chinese Ministry of Defense and Director of the Ministry's Information Bureau, argued that establishing the ISF was a "major decision" made by the CPC Central Committee and the CMC for the "cause of building a strong military," and a "strategic step to establish a new system of services and arms and improve the modern military force structure with Chinese characteristics." He confirmed that the ISF is a brand-new strategic arm of the PLA and a profoundly important pillar for "coordinated development and application/ utilisation of the network information system."

Subsequently, a commentary appearing in the PLA Daily newspaper, published post the launch of the ISF, explained the need for creating a unique force instead of having erstwhile departments or CMC bureaus serve the purposes of informatisation. The author of the commentary argued the metaphor that, "When the commander gives orders with the weight of a thousand junctures, the troops must follow with one heart."[6] Hence, the emphasis on both the core and the comprehensive role of the ISF as the underbelly of joint informational warfighting is evident. The importance given to network-centric war preparedness in the PLA is interrelated with the decision to establish such a force, and is expounded by the author as well, who further argues:

> "Network information technology has become the "greatest variable" in contemporary battlefield developments, as well as an important new source of combat power for the armed forces. The ISF is the key support for coordinating the construction and application of the network information system, and it occupies an important position and shoulders great responsibilities in promoting the high-quality development of the PLA and in winning modern wars."

The ideas of the commentary also tie in with the basic doctrinal emphasis of the PLA in the new age of battle. Its three assertions are: victory lies in information access; modern warfare is a system-to-system confrontation, a contest between systems; and whoever possesses information superiority seizes the initiative in war.

3.1 Mandate

The Chinese text of Xi Jinping's speech at the founding ceremony of the three new forces at the Bayi building in Beijing, laid out the ISF's three 'Core Tasks' and described the 'Four Musts' the force must follow.[7]

Core Tasks: In driving the modernisation and restructuring of armed forces, the ISF must focus on its positioning (as the literal 'nervous center' of an informatised military force); take on critical tasks (like making multi-domain operations a reality); and empower overall combat capabilities (coordinated efforts; smooth flow of information).

Four Musts:

- The first 'Must' pertains to people, polity and professionalism. The ISF must uphold the Party's absolute leadership; comprehensively plan the military's overall core setup; maintain basic operational principles; enhance mission awareness; carry out strict discipline; cultivate excellent style; build strong organisation (hierarchy, clearer roles for grassroots officers, and so on); and build a force that is "absolutely loyal, absolutely pure, absolutely reliable."
- The second 'Must' pertains to resources and strategy. The ISF must focus on supporting combat; strengthening the use of information technology and the joint operations system; deepening the fusion of military-civil information resources, promoting innovation; deepening cooperation and joint operations with relevant military and civilian departments; and continuously improving information support for multi-domain operations.
- The third 'Must' pertains to technological front-footedness. The ISF must encourage innovation-driven development; use reform as the driving force; strengthen talent incentives; build novel network competition capabilities; sharpen the information support team's core combat abilities; and continuously enhance quality and efficiency.
- The fourth 'Must' pertains to standardised governance and team-building. The ISF must focus on team building and basic foundation-building; strictly implement comprehensive requirements for effective management (of forces and equipment); strengthen standardised management systems to avoid ad-hocism; preserve team discipline; improve supervision methods; build a high-quality, stable team; and ensure high standards and safety.

Further, to infer the responsibilities and mandate of the ISF, one must assess not only Xi's speech, but also scholarly articles and official writings explaining the nature of wars the PLA is preparing to fight and win.

As China's official strategic affairs writings regularly explain, the electronic information domain has emerged as an essential pillar of modern warfare and a decisive factor in determining victory or defeat.[8] The side that succeeds in mastering high-end technologies in the electronic information and related fields will secure the initiative on future battlefields. In the information age, network information systems – driven by continual advances in information technology – profoundly shape the

generation, release, and employment of combat power. The level of construction and operationalisation of these systems directly influences the effectiveness of command and control, intelligence reconnaissance, precision strike, and integrated support capabilities. Modern warfare has thus evolved into a contest between opposing systems and networks. The side that dominates the information network effectively grasps the adversary's operational lifeline and holds the key to achieving victory.

Empirical studies indicate that in traditional, manually controlled command systems, commanders expended approximately 85 per cent of their time on information processing, leaving only 15 per cent for operational decision-making. Following the integration of command information systems into networked architectures, this ratio has been effectively reversed, allowing commanders to devote 85 per cent of their time to creative, decision-oriented tasks, thereby substantially improving command efficiency.[9]

The establishment of the ISF, hence, represents an institutional response to these challenges. The force is intended to overcome the legacy of fragmented "vertical silos" and dispersed resource allocation, often described metaphorically as "pepper-sprinkling investments." It seeks to dismantle the technical and institutional barriers among services, departments, and sectors, and to promote unified, holistic construction under an "all-in-one" framework.

3.2 The Flag

On August 1st, 2025, the day of the PLA's 98th founding anniversary, the new flags for the four 'support arms' – ISF, ASF, CSF, and the Joint Logistics Support Force (JLSF) – were unveiled at a celebratory ceremony.

As official reportage on the flags suggests, the colored band below serves as a visual shorthand for each unit's operational domain.

Figure 2: Flag of the Information Support Force | Source: 81.cn

Though, through a Weibo post[10] published by the PLA Daily, the colours' official descriptors are discernible. With the ISF in particular, the flag shows the colour 'Quantum Purple', which symbolises "Seizing the Information High Ground". Hence, the ISF's mandate is to enable the informational high ground for the PLA in battle, ensuring there are no lags in communication and network-based integration. PLA commentators often use the phrase "high ground" to demarcate the advantageous and leading position in any scenario. They argue, "Victory depends on the strategic location." That principle applies to the ISF in the information domain as well.[11]

Further, presumably, the decision to use purple on ISF's flag could also be inspired by how other military cultures use it. The purple colour in vexillology indicates electronic warfare-, signals intelligence-, or communication-related symbolism. For example, the traditional colour for Itä-Suomen Viestipataljoona (Eastern Finland Signals Battalion), part of the Finnish defence corps' Karelia Brigade, has the branch colours of the signals corps: purple and gold.[12]

In other cultures, purple indicates jointness and integration in the chain of command. As written by an officer working with the US Wright-Patterson Air Force Base, Ohio, in 2019, " 'Purple', in military jargon, means joint. It's a term used to describe a situation, or event, that includes people and units from different military branches who come together to accomplish a shared mission." In the Indian military, similarly, in April 2025, a batch of officers newly trained in joint skills came to be popularly known as "purple officers."[13] This is because the colour purple is a blend of the traditional army, navy and air force colours – green, blue, and sky blue – respectively.

3.3 Inspection

For the first time since its establishment (and so far, the only reported time), Xi Jinping inspected the ISF on 4 December 2024. At the event, conducted at the ISF's HQ in Haidian district of Beijing, Xi pointed out that in its initial stages, the ISF must comprehensively strengthen its own development, pay attention to laying foundations and undertaking work that benefits the long-term vision of combat readiness and victory, and firmly build the roots for future growth. Putting his 'Thought on Strengthening the Military in the New Era'[14] at the centre, and pushing for the meeting of thought with practice, Xi further instructed the force to:

Resolve the fundamental issues of ideology, deepen ideological rectification, strictly enforce conduct, discipline, and anti-corruption, and ensure the force is loyal, pure, and reliable; Strengthen entrepreneurial awareness and pioneering spirit, assume its initial responsibilities, select and build strong leadership teams at all levels, strengthen frontline command units and combat bastions, and enhance the leadership, organisational, and executive power of Party organisations; and Implement the concept of "whole-chain construction" of the military (a comprehensive, integrated effort), develop innovative models for talent cultivation, and create a high-quality, specialised corps of network information professionals. On cultivating specialised professionals, Xi clarified that the ISF is "first and foremost, a combat force." So all technological talents are meant to be troops and soldiers first.

The instructions surrounding the enforcement of discipline and combatting of corruption, though not unusual, are vital in the context of a series of high-profile purges and investigation-related disappearances rocking the PLA and the CMC in the past few years.[15]

Subsequently, Xi listened to work reports from ISF officials and demanded that they focus on integrating and effectively utilising various types of data and information. He also asked them to place great importance on network information security and protection, and lead innovation in command models and transformation in operational methods. His explicit message to the ISF was for it to evolve itself into a cutting-edge force for new-age warfare.

Post the inspection, a PLA Daily commentator talked about the conclusions of the inspection, and argued:[16]

> "Building the network information system is a systematic and long-term project that runs through every link and field of military activity. At all levels, the entire military must strengthen overall planning, innovate development models, actively explore practical approaches, and solidly advance all aspects of network information system construction."
>
> "Upholding the principles of information dominance

> and joint victory, ensuring smooth information links, and integrating information resources are necessary. Focusing on the ability to fight and win, efforts should be made to optimise modes of information service and support, effectively integrate and utilise various types of data and information, and attach great importance to the protection of cyberspace and network information."
>
> "The pace of integration into, driving, and empowering the [military] system *(since the ISF is new)* must be accelerated, leading to innovations in command models and transformations in operational methods. Reform tasks should continue to be implemented, work operation mechanisms improved, supporting laws and regulations refined, and a healthy ecosystem of co-construction, sharing, and joint use created. This will improve the quality and effectiveness of network information system development."

3.4 University

On 15 May 2025, Senior Colonel Jiang Bin, Deputy Director of the Chinese Defense Ministry Information Bureau, announced that the PLA Information Support Force Engineering University/ College was formed.[17] Its basis is the National University of Defense Technology (NUDT)'s Information and Communications College and the PLA Army Engineering University's NCO Communications School, with its main campus located in Wuhan, Hubei. The NCO school is based in Chongqing city.

This University is now the first higher education institution for the PLA ISF, and the only directly affiliated university for one of the newly built strategic forces.

In a piece published on Huanqiu (Chinese-language tabloid of Global Times) shortly after the creation of the ISF University, its author explained[18] what the mandate and responsibilities of the institution shall be, and what the achievements of its predecessor, the NUDT ICT college, have been:

- The university is a specialised higher education institution for branch-specific training. It serves as the primary institution for training ISF troops, a distinctive academy for new domains and new qualities, and a professional institution in the cyber and information fields. It hosts an academicians' workstation and a post-doctoral research station, and has over 90 experts, including National Natural Science Foundation award recipients and specialists from the CMC Science and Technology Committee, the Equipment Development Department, and other sectors.
- [The NUDT ICT College] has established seven national- or provincial-level key laboratories. As one of the first military academies to enrol and train master's students in military

science, it was also among the earliest institutions to conduct theoretical research on information warfare. In recent years, it has won over 300 national and military/provincial-level awards, and has been recognised as an "Outstanding Teaching Unit" and an "Advanced Unit for Learning and Talent Development" within the entire PLA.

- The [newer] university focuses on novel-domain, novel-quality areas within the network information system, offering 10 undergraduate majors: Communications Engineering, Optoelectronic Information Science and Engineering, Data Link Engineering, Electromagnetic Spectrum Engineering, Information Security, Intelligent Vision Engineering, Data Science and Big Data Technology, Command Information Systems Engineering, Software Engineering, and Network Engineering.
- It also supports six disciplinary clusters: Information Network Science and Technology, Data Intelligence and Cloud Computing, and Software Engineering and Command & Control Systems. Together, these form a new disciplinary structure led by network information technology that covers the full range of cyber and information fields.

3.5 Meat of the Matter: Exercises

In 2025, three crucial reports published by CCTV speak to how the ISF is preparing itself for combat. Even before that, in 2024, drills were being experimented with, but official communication seems to have only started being published in 2025.

The first report was published on July 18, 2025,[19] when an Information Support Force Brigade experimented with a unified "Networked System" to improve the effectiveness of communications and command. This report also highlighted that there was training conducted in 2024, and when that ended, the ISF brigade in question proactively solicited opinions and suggestions from participating units. Some units gave feedback that network information support had "not been precise enough," and that fault handling was not always timely. Hence, the brigade's Party committee concluded that the traditional model of communications support could no longer meet the operational and training needs of frontline units, and that finding a breakthrough solution was urgent.

To this end, they assigned professional personnel to work closely with different service arms, to understand their real-world requirements. They also established a special project team to study technological trends in the military communications field. Ultimately, they decided to build a new model of communications support under the principle of "embedding network-information detachments at the front, supported by rear-area platform systems."

Subsequently, the ISF also introduced a new training concept of building a "unified networked system." Such a system coordinates with and provides support to multiple frontline combat groups. At the brigade command post, a training staff officer explained that this year, instead of relying on the traditional model of "sitting in the rear to provide support," the ISF has shifted to a model of full-time accompaniment, supporting units throughout even their training and simulation deployments.

The scene-setting for the exercise, which is always a crucial component to Chinese descriptions of such drills, is as follows. It also speaks to how the ISF has channelised naval components, manned-unmanned teaming, and distributed unit roles:

> "In the skies, drones accompany helicopter formations, opening aerial signal channels; at sea, support boats sail alongside warships, creating localised communication networks; near shore, multiple types of equipment operate efficiently, setting up stable frequency bands for logistics transport groups... On the field training ground, an Information Support Force brigade dispatched multiple detachments to embed themselves in different combat groups, providing continuous network-information support to training units."
>
> "Further, one brigade cadre told the CCTV reporter that when planning this year's training deployment, they designed the scheme around the operational characteristics of different task groups, conducting high-intensity joint testing and calibration under extreme natural weather conditions and complex electromagnetic environments. They also drafted multiple contingency plans for various scenarios to ensure that network information detachments could fully play their role as communications hubs during training. Here, they are referring to the individually deployed units as 'network information detachments'. It will likely be a term one hears more of going forward."

During the drill itself, on the training ground, as several task groups penetrated into "enemy" positions, network-information detachments used drones to provide regional signal coverage, and employed "new portable equipment" (presumably informatised radios or battlelink devices) to relay battlefield situations instantly. They cooperated with each group to successfully complete training tasks.

Per usual, there was a post-drill review, where it was concluded that the "cloud-based" review and consultation mechanism was successful. This mechanism regularly brought forward-deployed network-information detachments together with rear-area specialists to discuss complex contingencies and support difficulties encountered during training. Together, they also put forward countermeasures and practical improvement methods to

further enhance capabilities.

The report of this drill concludes with stage-setting for a night-time practice that was also organised on the same training ground, at the same time period. There is no detailed assessment of the conduct and post-drill review, but there is one thing of importance to note – the PLA referring to its battlelink as the 'all-domain/ global network':

> "Facing complex electromagnetic interference, the embedded network-information detachments calmly and steadily responded. With drones taking off and new equipment coming online, each task group rapidly connected into the all-domain/ global network and launched coordinated attacks on "enemy" positions..."

Before that, in May 2025, an ISF unit had similarly conducted a "realistic combat support training" exercise. According to reports, during this training, multiple innovative achievements independently developed by the troops underwent battlefield testing, successfully resolving several support difficulties.[20]

The scene of the exercise is as follows:

> "Under 'enemy' artillery harassment, the road has been 'damaged.' Your unit is ordered to quickly advance and repair!" Late on a spring night, with this command, a unit of the ISF launched an intense session of realistic combat support training. Operating engineer Dong Hao, wearing a piece of independently developed equipment, led his repair detachment to the target area. This device enables construction machinery to function under low-visibility conditions, significantly improving operation precision and efficiency. The troops acted swiftly, coordinated closely, and completed road repairs and other tasks with high quality."
>
> "Inside the unit's command hall, Sergeant Major Third Class Zou Lijie stared intently at the command screen as two devices he had led in developing were about to undergo live testing. "Camouflage effect confirmed!" As an unmanned reconnaissance drone flew over the camouflaged area and transmitted back real-time images, both innovations successfully passed the trial."
>
> "Meanwhile, several kilometers away at the training ground, a piece of construction machinery failed to start properly. After installing a system independently developed by the team led by Sergeant Major First Class Li Wei, the malfunction was quickly eliminated. When the training concluded, the troops immediately collected and organised data, quantifying and assessing the contribution of these innovations to combat effectiveness."

Here, the report speaks of three highly interesting and declared proprietary technologies in use by the PLA ISF:

- A camouflage "device" that apparently hides military-grade construction machinery when it is engaged in repair operations, especially when aerial view is deployed using a drone; and
- A device/ software (the report just refers to it as a 'system') that fixes malfunctions in construction machinery (most likely those affiliated with wiring, but one cannot ascertain this through official reportage).

This camouflage device could potentially refer to a disruptive pattern tarpaulin, or to Self-Adaptive Photochromism (SAP). In December 2024, scientists from the University of Electronic Science and Technology of China reportedly developed synthetic SAP – material that deploys colour switchability at the molecular level, to adapt to, and essentially blend in with, the environment. Given the chameleon-like behaviour of such material, and the applications of that technology in military uses, it is likely that SAP is being experimented with in the PLA.

Effectively, these demonstrations were meant to convey that the ISF is rather successfully experimenting with an 'innovation traction + talent incubation + application of results' model.

How this technology works is yet to be ascertained, and yet, if true, in the context of PLA deployment in, say, the complex terrains and high altitude areas covered by the Western Theatre Command (WTC), such devices/ systems will come in more-than-handy in resolving snow accumulation or landslide-related blockages. In fact, it is the WTC's consistent endeavour to provide intense terrain training to its troops, and have them cultivate soft combat skills like snow shovelling and machinery operations. Now, it may be that the ISF can quite literally "support" such troops.[21]

Finally, on August 2, the report of a third exercise in 2025 came out.[22] In it, a "certain" ISF Unit conducted an invisible attack-defence simulation drill. The exercise assessment basically consists of a few statements spoken by Bi Sheng, a soldier of the ISF unit in question. Much of what he says has great dramatisation and virtue-signalling, but one can read a little between the lines to understand the tactics the ISF is experimenting with. He argues:

> "The moment a USB drive is inserted, it can implant a multi-layer camouflaged Trojan virus. Once activated, within seconds it can paralyze the entire system. Building a 'cyber Great Wall of electronic defense' is about providing solid support for joint operations."
>
> "Amid the roaring artillery of Shangganling [referring to the Battle of Triangle Hill, 1952], our forebears used their own bodies to conduct electricity, keeping battle communications connected. Today, we fight in

> the 'tunnels' etched onto chips, facing possible 'data bombardments' at any moment. Though the form of technology has changed, the 'never-interrupted nerve' has never changed."
>
> "How do we defend this binary Great Wall of 0s and 1s? We must adhere to information dominance, winning through joint operations, deeply integrating into the PLA's joint operational system, carrying out precise and efficient information support. Behind this effort stands a group of nameless soldiers, holding the line and fighting. When we become a drop of water within the great joint system, we form the PLA's iron fist of combat, and merge into the magnificent rivers and mountains of our motherland!"

There are two main takeaways in this script:

- Openly, the ISF soldier is informing the reader that "multi-layered camouflaged" Trojan viruses will be crucial to the PLA's network warfare tactics, and defensive capabilities will revolve around building a cyber firewall to bar enemy intrusion attempts.
- The ISF's definition of information dominance includes shielding against data bombardments and effectively removing the chaff to get to the grain.

Most recently, the ISF displayed a formation at the grand September 3 military parade commemorating the 80th anniversary of the victory in the Chinese People's War of Resistance Against Japanese Aggression and the World Anti-Fascist War. The ISF's equipment display included battlefield network-cloud-equipped vehicles, "digital intelligence empowerment" vehicles, space-ground networking vehicles, and information integration vehicles, all capable of rapidly building new network-information systems to strongly support joint operations.[23]

A July 2025 article in Qiushi magazine explains the conceptual boundaries of "digital intelligence empowerment," though in the context of China's industrial manufacturing sector.[24] It argues:

> "According to Zhang Guolong, Senior Director of Final Assembly Technology at the Engineering and Technology Department of China FAW, since its completion and start of production in 2021, the Hongqi Prosperity Plant has been operating at full capacity, with an average of about 1,000 vehicles rolling off the production line each day. "To meet the needs of Hongqi's brand expansion and new product launches, the Hongqi Prosperity Plant has built an intelligent manufacturing model that integrates automation systems with information systems vertically through the industrial internet, while also achieving cross-system horizontal integration. This model

> enables equipment to self-diagnose faults, production control to self-adapt, quality management to self-learn, and energy management to self-decide," he said."

Essentially, it is the holistic incorporation of ML-enabled/ informatised technologies with any process to achieve as much autonomy as possible, with only expert/ professional human intervention required when necessary. It speaks to the centrality of human-machine teaming in all aspects of the PLA's work, including but not limited to information superiority in battle.

3.6 Key assessments

Evidently, in the leadership's assessment, the SSF left much to be desired in terms of bringing about seamless integration of services and theaters, and creating a network-centric force. It is highly likely that the creation of an individual unit in the form of the ISF, will lead to more effective strategising across the PLA. There is likely to be uniformity in electromagnetic warfare doctrine, and sustained budgetary and personnel resources will be channelled in the ISF to deal with challenges, such as the inability to sustain coordinated communications under electronic and kinetic stress. In effect, the ISF represents a clear formalisation of Beijing's endeavour to become an informational warfighter. And so, if the ISF is able to see its mandate through and develop its core competencies well, the key challenges posed to adversaries would be two-fold: The PLA's strong foothold over electromagnetic fogging, jamming and spoofing, as well as its ability to significantly shorten the time between detection, decision and response. Together, these may directly put a rival fighting force at a disadvantage vis-à-vis the high tempo of conflict they will be forced to deal with.

Yet, there is no guarantee that the ISF will be able to address key bottlenecks and concerns that plagued the PLA's network-centricity endeavours in the past. The first is the inability of the different services to adapt their troops to diverse informational requirements of their theaters. For example, submariners in the PLA Navy often find it difficult[25] to operate complex radar and targeting systems on board. Similarly, drone pilots have faced challenges in operating drone units in the high-altitude and windy terrains of Tibet.[26] Even if the ISF could provide them with relevant expertise, in wartime, not only will the Force's resources be divided and distributed, but they will also not be able to compensate for a lack of informational adaptability of troops.

The ISF's immaturity requires that it be prepared to avoid accidental informational escalation, manage resource provisions to uphold theater autonomy, and stay free of corruption. Especially given the potential charges of corruption against the former SSF Commander Ju Qiansheng, the ISF's reputation is dependent on trustworthiness. Not to mention, any obsolescence or inefficiency

in technology deployment and adaptation would defeat the purpose of carving out this altogether new force.

4 Cyberspace: The Invisible Battlefield

China's vision for multi-domain precision warfare requires that cyber dominance be a key pillar of military preparedness. To fulfill this requirement, the CSF hence came into being on 19 September 2024, and was created from the erstwhile Network Systems Department of the Strategic Support Force. During the inauguration ceremony, Wu Qian explained the reasoning behind its creation, arguing:

Cybersecurity is a global challenge and also a severe security threat that China faces. Advancing the development of cyberspace forces and vigorously enhancing cybersecurity defense measures are significant for strengthening the country's cyber border defenses, promptly detecting and repelling cyber intrusions, and safeguarding national cyber sovereignty and information security. We actively advocate for a peaceful, secure, open, and cooperative cyberspace, and are committed to working with the international community to jointly build a community with a shared future in cyberspace.

Further, as discussed above, the 2019 Defense White Paper categorised cyber security and cyberspace sovereignty as "major security fields" for China, elevating them to the same pedestal in national security strategy as nuclear and outer space capabilities.[27] The creation of the CSF rightfully follows the spirit of reform articulated in both the White Paper and Xi's Report to the 20th Party Congress, while also streamlining the distributed focus of the PLA's various services, units and bureaus, on cyber dominance.

4.1 The Flag

In addition to the standard golden stripes signifying "honour and mission" in the flags of the support forces, the colour of the alternating stripes on the CSF's flag has been officially titled 'Cyber Gray'. It symbolises "Victory in the Invisible Battlefield".

Figure 3: Flag of the Cyberspace Force | Source: 81.cn

4.2 Mandate

The CSF is a professional technical arm designed to address the complex battlefield of cyberspace. The ISF, by contrast, is a strategic arm that provides key support for coordinating and employing network and information systems across all services in joint operations. However, the protection and preservation of the network system deployed is in the hands of the CSF.

As highlighted in the above-cited Qiushi magazine article, adhering to the integration of ideological and simulative construction with application, practical combat effectiveness is an important endeavour for the CSF.[28] To do this, the force should engage with a "research-testing-operations" closed-loop feedback mechanism, continuously optimise system functions through simulations and live-force exercises, and ensure resistance to interference, damage, and paralysis in complex electromagnetic and cyber confrontation environments.

4.3 Recruitment and University

The CSF was formed from the SSF Network Department, which in turn amalgamated the former CMC General Staff Department's Third Department, Fourth Department (in part), Second Department (in part), and the General Armaments Department (in part). As a result, today, units directly subordinate to the CSF include an Electronic Countermeasure Brigade, Units 61726 (hacker unit) and 61786 (information technology research institution), the 56th, 57th, and 58th Research Institutes of the PLA Cyberspace Force (covering computer design, automation, SIGINT and cyber-reconnaissance), and Technical Reconnaissance Bases (TRBs) for the Eastern, Southern, Western, Northern, and Central Theaters. This is in addition to the CSF's General Staff Department, Political Work Department, Logistics Department (Unit 32047), Equipment Department, Military

Representative Offices in Shanghai, Tianjin, Nanjing, Chengdu, Guangzhou, Shenzhen, and Wuhan, and individual Network and Informatization Bureaus.

Given its organisational nature, the CSF is unlikely to be open to non-military inductions. However, as suggested in an article published by the Wangdun Cybersecurity Training School in Hubei Province, a probable pathway for recruitment would be through "civilian positions" that the military sometimes opens publicly for technical roles.[29] Even these, however, may be limited to those trained within military academies. The article also warns that a closed environment might lead to a technological gap, since much of the PLA's IT infrastructure is currently outsourced to third-party companies, and given that cybersecurity in the military context is not just about setting up basic defensive technologies – firewalls, intrusion detection systems, document protection, or network monitoring – but also about breaking through technical bottlenecks, deepening theoretical research, innovating legal and institutional frameworks, and enhancing comprehensive defense capabilities.

To this end, according to the 'Interim Regulations on the Management of Active-Duty Officers', the 'Interim Provisions on the Supplementary Selection of Active-Duty Officers', and related policies, and in line with the unified deployment of the entire military, the CSF also organised direct recruitment of specialist officers in the second half of 2024.[30]

The recruitment announcement revealed the CSF's skill-based priorities. By targeting "Double First-Class" university graduates, overseas top-200 university alumni, and technical specialists in disciplines like computer science and cryptography, the PLA is professionalising cyberspace capabilities. The strict exclusion of adult/ online education graduates emphasises elite, rigorously trained talent. Moreover, the effort to draw from both civilian universities and military academies reflects a hybrid approach, leveraging China's broader talent ecosystem while preserving military standards.

The training of the recruited talent takes place at the CSF-affiliated Information Engineering University (IEU), which is separate from the ISF's IEU (discussed above). The University started as a specialised Institution affiliated with the SSF. In 2024, however, months after the SSF's disbandment,[31] NUDT claimed the erstwhile SSF IEU's External Training Brigade as a subordinate department of its School of Foreign Languages, and handed off the School's Luoyang campus for training and intelligence instruction to the new IEU under the CSF.[32]

Today, the CSF IEU's subordinate institutions include a Basic Department, the School of Information Systems Engineering (First Academy), the School of Geospatial Information (Second Academy), the School of Cryptography Engineering (Third Academy), the School of Cyberspace Security (Fourth Academy), the School of Data and Target Engineering (Fifth Academy), the

Information Science and Electronic Countermeasure Systems Research Institute, the Luoyang Camp, the Kunming Training Brigade, and the Lanzhou Training Brigade (the latter two are managed by the School of Cryptography Engineering).

4.4 Combat Preparedness and Equipment

Of the few public combat preparedness endeavours CSF has undertaken in just over a year, perhaps its displays at the September 3 military parade, are most vital. CSF's formation at the parade demonstrated China's professional strength and technological reserves in cyber defence, showing that China has the ability to deal with all kinds of cyber threats and challenges. The four types of equipment displayed by CSF units were meant to demonstrate integrated command and control, reconnaissance and sensing, and cyber-electronic confrontation. What is interesting about the Armoured Personnel Vehicles (APCs) aboard which the equipment was displayed, is that they are new and indigenised versions of previously used APCs of the PLA, and have been designed specifically for deployment by the CSF.

In the aftermath of the parade displays, Qi Xiangdong, Chairman of Qi An Xin Technology Group, emphasised the need for preparing to fight and win in the "invisible battlefield" from the Chinese perspective. Hence, cyberspace and the information domain have become the "new frontiers" for safeguarding national sovereignty in PLA doctrine. Further, remarks by entrepreneurs such as Qi and Zhou Hongyi of the 360 Group (who was also interviewed in the aftermath of the CSF's September 3 demonstrations) underscore the close alignment of state defence priorities with the commercial cybersecurity sector. Their comments reveal how civilian tech elites are being symbolically co-opted into the defence narrative, reinforcing the notion of a civil-military fusion strategy in cyberspace.[33]

Overall, electronic warfare and cyberattacks can render troops "blind" and cause weapons to lose their combat capability, making networking, digitalisation, and intelligence crucial in modern warfare. Hence, realising the CSF's role and mandate in fulfilling China's vision of multi-domain precision warfare shall be an essential component of combat preparedness efforts going forward.

4.5 Key Assessments

The Cyberspace Force has a strong grounding in the roles and mandates of the erstwhile departments of the CMC and the SSF. Answerable to it are diverse research institutes and technical reconnaissance bureaus working on an array of specialisations ranging from espionage and intelligence operations to data management and cyber reconnaissance. This creates intensive expertise on various aspects of offensive cyber capabilities for the PLA. All of their toolkits and best practices are also now

pooled under a singular, independent force, which will streamline offensive operational tactics.

It is highly likely that, going forward, the PLA's cyber operations will become more sophisticated, and the CSF's core competencies shall be strengthened – including in the psychological warfare domain. This is also given that PLA-affiliated Advanced Persistent Threat (APT) Actors, such as PLA Unit 61398 or 'APT 1', and ShadyRat, have been responsible for critical attacks across economies like Singapore, Indonesia, Vietnam, the US, Taiwan, the UK, India, Canada, Japan, Hong Kong, the Republic of Korea, Switzerland, and Germany. In fact, APT 1 has targeted the high-tech companies of these economies, such as Lockheed Martin and Telvent, in a bid to conduct intellectual property theft.[34] Hence, in peacetime, the CSF is likely to have sophisticated under-the-threshold techniques at their disposal, which may potentially drastically disrupt global cybersecurity.

The big potential challenge the CSF itself may face could revolve around unintended escalation. Often, cyberattacks with cascading consequences are construed by governments as acts of war. The CSF must prepare to clearly differentiate between peacetime and wartime, and between preparedness and real-time implementation. Further, the CSF will have to make a concerted effort to prevent the creation of siloes between its various sub-units, or else economies of scale across theaters and services would be difficult to achieve.

5 Venturing Beyond: The Military Aerospace Force

The ASF, like the CSF, is a reformed unit spun off from the Aerospace Systems Department of the SSF. On the day of its formation, Wu Qian explained the need to build a military force that would safeguard China's interests in outer space, despite Beijing's opposition to its militarisation. He argued:

> "Space is a shared asset of humanity. Space security provides strategic assurance for national and social development. Building the Aerospace Force is of great significance to strengthening the capacity to safely enter, exit and openly use space, enhancing crisis management and the efficacy of comprehensive governance in space and promoting peaceful utilization of space. China's space policy is clear. We are committed to peaceful utilization of space and stand ready to work with all countries with the same commitment to strengthen exchanges, deepen cooperation and contribute to lasting peace and common security in space."

Essentially, the ASF is modelled along the US Space Command, with a goal to preserve and secure China's ability to engage

in spacefaring missions, while also creating the capability to deny "enemies" access to space and space-based resources. Its organisation has also absorbed most key subordinate units of the erstwhile SSF Space Systems Department, such as the Astronaut Corps of the PLA, the Beijing Aerospace Flight Control Center, the Jiuquan, Taiyuan, and Xichang Satellite Launch Centers, and Units 63680 (Maritime Satellite Tracking and Control Department/ PLA 23rd Test and Training Base),63750 (Xi'an Satellite Tracking and Control Center/ PLA 26th Test and Training Base), and 63650 (the Malan Nuclear Test Base).

5.1 The Flag

In addition to the standard golden stripes signifying "honour and mission" in the flags of the support forces, the colour of the alternating stripes on the CSF's flag has been officially titled 'Deep Space Blue'. It symbolises "The military's advance into outer space".

Figure 4: Flag of the Military Aerospace Force | Source: 81.cn

5.2 Talent, Recruitment and University

Soldiers of the ASF are expected to carry forward the spirit of the "Two Bombs, One Satellite" programme, which culminated in the testing of China's nuclear weapons capability at Lop Nur, Xinjiang in 1964. In contemporary times, their foremost goal is to establish China's manned spaceflight programme and "write a new chapter in the history of China's space enterprise."[35] ASF troops are expected to inculcate sensitivity to numbers and train in pursuit of precision. Not to mention, they are required to contribute to the digitalisation and intelligentization of China's space programme.

While no official announcements for recruitment in the ASF have been made public in 2024 or 2025, the Malan Nuclear Base (MUCD 63650) in particular has launched a recruitment drive in March 2025.[36] Even though the Base has not proactively tested

nuclear systems since 1996, it continues to remain active as a training center. Hence, per the recruitment announcement, the unit's affiliated institutions are looking for talented individuals from both the military and civilian domains to advance their skills in domains such as nuclear physics, optical and aerospace engineering, composite materials technology, and space systems chemistry. Said affiliated institutions are located in Xi'an, Luoyang, Xinxiang, Hefei, and other cities, and are recruiting jointly with national-level key laboratories, postdoctoral research stations, and Ministry of Education key laboratories.

In general, troops of the ASF are to be trained at the PLA Space Engineering University.[37] It is a higher education institution that systematically trains personnel for China's space programs. It is designated as a "Double First Class" university in China, and is known for setting up one of the PLA's first 'National Defense Science and Technology Innovation Special Zone' workstations. It was jointly established by the State Administration for Science, Technology and Industry for National Defense (SASTIND) and the SSF Space Systems Department.

The University also runs a Non-Commissioned Officers' (NCO) School, for which it recruits from several technical colleges in China. This is evident from an inspection of the Nanjing University of Industry Technology (NUIT) conducted by the Senior Colonel Wang Jinmiao, Vice President and Chief of Education of the Space Engineering University NCO School. He led a delegation of six to visit the NUIT for inspection and research in December 2024.[38]

Per the details of the visit, Wang emphasised that ASF academies are key bases for cultivating new-generation space talent, adhering to the principles of moral and professional development, and preparing students for "combat-oriented careers." The NCO school, in particular, focuses on developing "Commanders+Scientists." Wang's discussions with NUIT stakeholders covered topics such as the establishment of undergraduate programs for associate degrees and the integrated training of professional courses, competitions, and certifications.

5.3 Exercises, Formation and Equipment

While there is little official information on the nature of combat preparedness exercises being conducted by the ASF, a report published by the Chinese Ministry of National Defense spoke of a Flag Guard and Instructor Wang Gexuan, who highlighted the common training practice all ASF troops engage in: pressure testing. "If the pressure gauge [presumably onboard an aerospace system] shows a value just three points below the required standard," he explained, "the entire operation must be halted for inspection."[39] In one case, he exclaimed, the troops spent six hours tracing several kilometres of pipeline just to locate a tiny gasket causing a minor air seal discrepancy. Hence, just like any other support force or service in the PLA, ASF troops are required

to cultivate soft combat and technical skills to maintain equipment efficiency and combat readiness.

Further, at the September 3 parade, an electronic warfare formation was displayed at Tiananmen Square, and it was assembled from units of an ASF base and the Northern Theater Command Ground Forces. The five core pieces of electronic warfare equipment displayed by the formation are reportedly capable of all-frequency reconnaissance, control and precision suppression.[40] They can also defend against aerospace threats and disrupt networks and communications, and constitute the leading operational electronic warfare equipment currently in service. They have been referred to as the "electromagnetic sword" for "seizing battlefield initiative," and have all been indigenously developed in China.

An interesting report appearing on CCTV Channel-13 in January 2025 also shed some light on the equipment the ASF is experimenting with.[41] It discussed a Space Force monitoring and Early-Warning Station. Likely located in Heilongjiang Province, the station is equipped with a large-scale early-warning radar array capable of detecting incoming intercontinental ballistic missiles (ICBMs) in advance.

Pictorial representations speak of massive radar antennas aboard the station, far exceeding the size of shipborne or vehicle-mounted radars. It can reportedly accurately determine critical parameters of incoming high-threat missiles – instantaneous position, velocity, launch point, and impact point – providing the highest military authorities with timely missile warning intelligence.[42] Moreover, PLA early-warning radars have reconnaissance and signal intelligence functions, and they are equipped with high-frequency radio direction-finding systems to monitor communications in key regional areas.

This equipment is likely the same long-range strategic early warning radar for interception of long-range ICBMs, displayed by the ASF in their New Years' Greetings video in early January 2025.[43] This radar could be paired with the previously revealed HQ-19 missile defense system and the mid-course missile interception system, forming a key component of China's National Missile Defense Interception System (CTMD). The likely detection range of the radar is ~5,500 kilometers, and boasts gallium nitride (GaN) phased-array Transmit/ Receive (TR) Module technology. Chinese military commentator Du Wenlong has also remarked that this system is the Chinese version of the American "Pave Paws" radar network, with the difference being that the former has a circular radar array and the latter has a hexagonal one.[44]

This radar was built in 2017 by the China Electronics Technology Group Corporation (CETC)'s 14th Institute. It is a P-band radar, and its long wavelength enables it to penetrate mass more deeply, thereby making stealth target detection possible. Further, as compared with Gallium Arsenide (GaAs)-based radar arrays, GaN-based arrays are more efficient and produce greater power. Phased array also means digital beamforming without unnecessary antenna movement. Nonetheless, it is noteworthy that the CETC deemed the radar "historic" in 2017, when the US "Pave Paws" was sold to Taiwan in 2000 itself. See: China's Pave Paws? Domestically Produced P-Band Long-Range Early Warning Faced Radar..., Sina, 8 October 2017.

Due to military sensitivity, it is rare for authoritative media like CCTV to broadcast land-based large early-warning radar in news programmes. Even when the PLA conducts mid-course missile interception tests, CCTV usually keeps coverage partial, rarely showing kinetic interceptor launches or radar detection of incoming missiles. However, in the past few years, the PLA appears to have shifted toward more transparent displays of advanced weaponry, revealing previously secret systems. Examples include:[45]

- The HQ-19 surface-to-air missile, a high-level terminal interceptor;
- The DF-31AG ICBM tested over the Western Pacific with a 12,000 km range; and
- The first global flight of sixth-generation fighter prototypes, informally dubbed J-36 and J-50.

Open-source information suggests the deployment of similar radars in Heilongjiang, Zhejiang, and Xinjiang,[46] covering air activity over the Arctic, North America, Europe, and the second island chain, particularly against ballistic missile threats. The ASF also operates the Yuanwang space support ships used in tracking satellites.[47]

5.4 Key Assessments

The Aerospace Force is perceived, at least in China, to be a counter to the US's Space Force. The incorporation of missile strategy under its ambit indicates that the force is not only engaging to disrupt space-based capabilities of Beijing's rivals but also ensure that airspace as a whole is protected against missile attacks. And while China maintains a no-first-use approach to the use of nuclear missiles especially, it insists upon the ability to respond rapidly and harshly.

In this regard, the ASF's main challenge could be the maintenance of its high-tech gear and systems. The ASF is known to be experimenting with Anti-Satellite Weapons Systems, China's best Phased-array AESA Radars, and, of course, critical equipment necessary to maintain seamless ground-satellite communications. Its telemetry and tracking stations are also responsible for vital operations involving space-based surveillance, ICBM launch

tracking, and real-time reconnaissance and warning. Hence, inefficiencies in equipment procurement and management is moderately likely to significantly throw the ASF into disarray, and make its leaders subject to Xi Jinping's wide-sweeping anti-corruption campaign. Given fears and rumours surrounding PLA Rocket Force missiles being filled with water and soldiers using rocket fuel to make hot-pot, concerns surrounding the management of sensitive military equipment are consistent in China, and the ASF could potentially emerge as their next target.

The ASF also requires consistent upgrades in the protection of its C4ISR infrastructure. Given a lack of engagement with rival foreign militaries, the ASF is likely to struggle to fathom the exact extent of electromagnetic jamming and fogging capabilities of, say, the US. In this regard, an important aspect of the ASF's work would have to pertain to continuous investment in infrastructure protection. If not, technological obsolescence will most likely lead to compromised C4 and satellite ISR in battle.

6 Conclusion

The restructuring of the SSF into the independent Information Support, Cyberspace, and Military Aerospace Forces, marks a transformative step in aligning military organisation with the demands of system-of-systems warfare and multi-domain operations. Through institutional reforms, advanced talent cultivation, innovation-driven technologies, and increasingly transparent operational practices, these forces bring the PLA closer to achieving its goals of informatisation and intelligentisation. The creation and rapid development of these specialist arms has positioned the PLA to effectively assert dominance across information, cyberspace, and aerospace domains and achieve operational superiority in new-age warfare.

However, public information remains shallow and official rhetoric thrives lucidly. Hence, despite the impressive advances and ambitions of these newly restructured PLA support forces, they face significant challenges, including the integration of diverse technological systems, overcoming legacy organisational silos, and the recruitment and training of highly specialised personnel. In particular, maintaining information dominance requires safeguarding against increasingly sophisticated cyber threats, managing vulnerabilities introduced by rapid digitisation, and ensuring operational security in a contested electromagnetic environment. Moreover, the reliance on civil-military fusion and the need for continuous innovation in doctrine and equipment present persistent obstacles, which must be addressed for the ISF, CSF, and ASF to achieve effective, unified, and resilient multi-domain capabilities.

Endnotes

1. "Full text of the report to the 20th National Congress of the Communist Party of China," International Department, Central Committee of the CPC, 2 August 2023.
2. "Full Text: China's National Defense in the New Era," The State Council, the People's Republic of China, 24 July 2019.
3. Anushka Saxena, "Xi Jinping's vision of war seen in creation of 'Information Force'," Nikkei Asia, 2 May 2024.
4. Han Yong Hong, "China deepens purging of the military to prepare for battle," ThinkChina, 29 September 2023.
5. Masaaki Yatsuzuka, "PLA's Intelligentized Warfare: The Politics on China's Military Strategy," The National Institute for Defense Studies, Japan, 5 January 2022.
6. "PLA Daily commentator: Strive to build a strong modern information support force," People's Liberation Army Daily, 20 April 2024.
7. "Study Card | What kind of force is the newly established Information Support Force? A complete explanation in one picture," CCTV News Client, 20 April 2024.
8. Dong Junlin, "[illegible]," Qiushi, 8 June 2025.
9. Li Yeyu, "Unveiling China's New Strategic Arm: The PLA Information Support Force, Directly Under the Central Military Commission," Bauhinia Magazine, 29 April 2024.
10. Weibo Post by PLA Daily, 6 August 2025.
11. Liang Min Gao Fei, "[illegible]," People's Liberation Army Daily, 19 July 2022.
12. "Military colours, standards and guidons," Military History Fandom, n.d.
13. Siddhartha Dave, "A Purple Dawn: India's first batch of 'Purple Officers' and the march towards joint command," Organiser, 20 April 2025.
14. Robert Lawrence Kuhn, "Xi Jinping Thought on Strengthening the Military," CGTN, 11 October 2022.
15. Anushka Saxena, "Another one Bites the Dust," 'Eye on China' Substack, 29 November 2024.
16. "PLA Daily commentator: Creating a new situation in the construction of our military's network information system," People's Liberation Army Daily, 6 December 2024.
17. "2025[illegible]," Ministry of National Defence, People's Republic of China, 15 May 2025.
18. "[illegible]," Huanqiu, 17 May 2025.
19. "[illegible]," CCTV, 18 July 2025.
20. "[illegible]," CCTV, 3 May 2025.
21. Anushka Saxena, "Assessing Operations and 'Jointness' in the PLA Western Theater Command," The Takshashila Institution, 16 May 2024.
22. "[illegible]," CCTV, 2 August 2025.

23. Anushka Saxena, "Left, Right, Left!," 'Eye on China' Substack, 3 September 2025.

24. Cao Pengyuan, Xue Qinfeng and Tang Lan, "[illegible]," Qiushi, 18 July 2025.

25. Christopher Sharman and Terry Hess, "China Maritime Report No. 34: PLAN Submarine Training in the "New Era"," US Naval War College Digital Commons: China Maritime Studies Institute, 10 January 2024.

26. Anushka Saxena, "Assessing Operations and 'Jointness' in the PLA Western Theater Command," The Takshashila Institution, 16 May 2024.

27. "Full Text: China's National Defense in the New Era," State Council Information Office, 24 July 2019.

28. Dong Junlin, "[illegible]," Qiushi, 8 June 2025.

29. NetShield Cybersecurity Training School, "[illegible]?," Sohu, 14 May 2024.

30. Cyberspace Force, 2024[illegible]," Military Talent Network, 4 November 2024.

31. Tian Qiang et al., "2024[illegible]–[illegible]," People's Liberation Army Daily, 17 June 2024.

32. Suzhou Veteran Affairs Bureau, "[illegible]," Weixin, 29 September 2024.

33. Southern Metropolis Daily, "[illegible], [illegible]," NetEase, 3 September 2025.

34. "Survey of Chinese Espionage in the United States Since 2000," Center for Strategic and International Studies, n.d.

35. Zhu Chuanchao and Lu Dongfang, "[illegible]: [illegible]," Ministry of Defense, People's Republic of China, 4 September 2025.

36. Unit 63650 of the PLA, "2025[illegible]63650[illegible]," Military Talent Network, 19 March 2025.

37. "[illegible]," Xiangtan University Employment Information Network, n.d.

38. "[illegible]," Nanjing University of Industry Technology, 24 December 2024.

39. Zhu Chuanchao and Lu Dongfang, "[illegible]: [illegible]," Ministry of Defense, People's Republic of China, 4 September 2025.

40. Xinhua News Agency, "[illegible]:"[illegible]"[illegible]," QQ, 3 September 2025.

41. Ibid.

42. [illegible], "[illegible]," WForum, 26 January 2025.

43. Wendu History, "[illegible]," NetEase, 22 February 2025.

44. "[illegible]," Min News, 28 October 2025.

45. [illegible], "[illegible]," WForum, 26 January 2025.

46. [illegible], "[illegible], [illegible]", [illegible]," QQ, 26 January 2025.

47. "Military and Security Developments Involving the People's Republic of China: 2024," Annual Report to Congress: U.S. Department of Defence, 18 December 2024.

The Takshashila Institution is an independent centre for research and education in public policy. It is a non-partisan, non-profit organisation that advocates the values of freedom, openness, tolerance, pluralism, and responsible citizenship. It seeks to transform India through better public policies, bridging the governance gap by developing better public servants, civil society leaders, professionals, and informed citizens.

Takshashila creates change by connecting good people, to good ideas and good networks. It produces independent policy research in a number of areas of governance, it grooms civic leaders through its online education programmes and engages in public discourse through its publications and digital media.