PEOPLE'S LIBERATION ARMY STRATEGIC SUPPORT FORCE: IMPLICATIONS AND OPTIONS FOR INDIA

ANIL CHOPRA

In March 2021, the Red Echo hacker group, affiliated with the Chinese government, reportedly attacked India's power grid control rooms causing widespread outages.[1] According to India's Ministry of Power, the cyber attackers could not succeed to infiltrate the secure system, and there was no information breach. Earlier, the Ministry of Defence, Government of India too, in its year-end review, had acknowledged that "microwave weapons"[2] had been used by Chinese PLA in Ladakh. These were described as "unorthodox weapons".[3]

In December 2015, China effectuated reforms in its People's Liberation Army (PLA). These included changes to the organisational structure, war-

Air Marshal **Anil Chopra** PVSM AVSM VM VSM (Retd.) is Director General at the Centre for Air Power Studies, New Delhi.

1. Tanya Thomas, Prasid Banerjee, "China Hackers Did Not Penetrate Grids: Govt", *Livemint*, March 02, 2021, at https://www.livemint.com/news/india/chinese-group-likely-behind-mumbai-october-blackout-say-cybersecurity-firm-11614592399387.html. Accessed on June 26, 2021.
2. Aakriti Sharma, "Has India Finally Acknowledged That Chinese PLA Used Microwave Weapons Against Indian Soldiers In Ladakh?" *The EurAsian Times*, January 6, 2021, at https://eurasiantimes.com/has-india-finally-acknowledged-that-chinese-pla-used-microwave-weapons-against-indian-soldiers-in-ladakh/. Accessed on June 26, 2021.
3. Year End Review – 2020 Ministry of Defence, Press Information Bureau, Government of India, January 1, 2021, at https://pib.gov.in/Pressreleaseshare.aspx?PRID=1685437. Accessed on January 26, 2021.

fighting approach and military culture. A Strategic Support Force (SSF) was created to integrate PLA's space, electronic warfare, cyber and psychological warfare capabilities under one umbrella. SSF's C4ISR capabilities enable conduct of joint operations and "system vs. system" warfare that is very important for winning modern wars.[4] With this, China has shifted from being a land-centric defensive force to one capable of aggressive global power projection, including through space and cyberspace. China is currently preparing to engage in and win informationised wars. The SSF is meant to support the PLA combat operations so as to gain additional advantages. SSF will also build new synergies between various elements for strategic information operations (IO) that are considered crucial in wars of the future.[5] Like all theatre level elements, the SSF comes directly under the Central Military Commission (CMC). It has two semi-independent branches under it: the Space Systems Department and the Network Systems Department. All the sub-components and their vertical and lateral interactions in the new system have been redefined. The SSF is responsible for strategic information support and strategic information operations.[6]

Many are comparing the PLA reforms to the US reforms under the Goldwater-Nichols Department of Defence Reorganization Act of 1986. Clearly the aim is to transform military structure for joint warfare. The SSF will also help China to compete with a major adversary such as the USA. By combining all information warfare capabilities, particularly cyber, electronic and psychological warfare, SSF will be able to effectively coordinate and support theatre command levels.

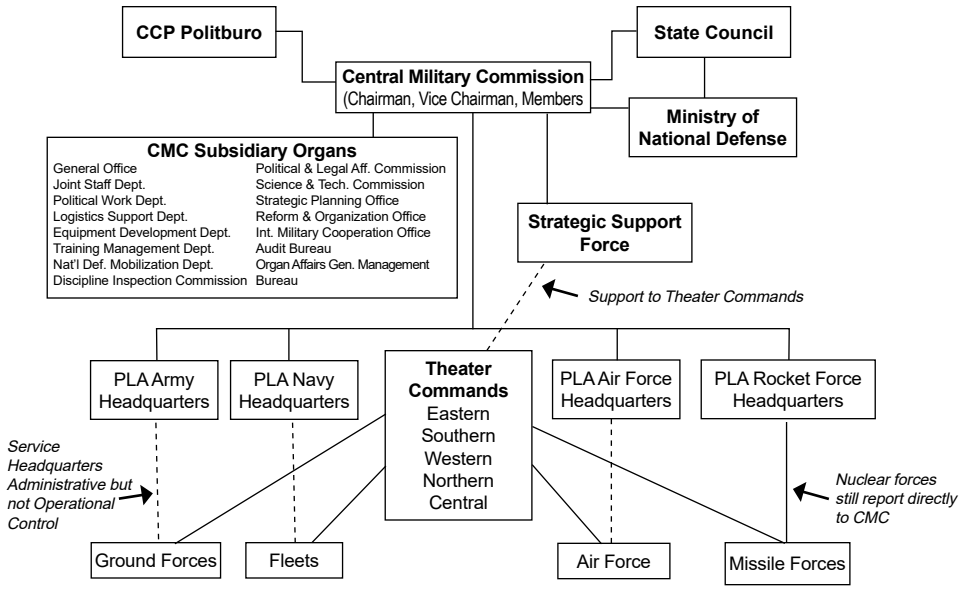
This paper examines the constitution, functioning and operations of PLASSF.

4. Kevin L. Pollpeter, Michael S. Chase, Eric Heginbotham, "The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations", Rand corporation, 2017, https://www.rand.org/pubs/research_reports/RR2058.html Accessed June 26, 2021
5. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era", National Defense University Press, October 02, 2018, at https://ndupress.ndu.edu/Media/News/Article/1651760/chinas-strategic-support-force-a-force-for-a-new-era/ Accessed June 26, 2021.
6. Ibid. Accessed on June 26, 2021.

BROAD STRUCTURE

The SSF reports directly to the CMC. In many ways it is structured like the People's Liberation Army Rocket Force. The SSF was formed by amalgamating the existing units handling space, cyber and electronic warfare across the PLA. It also got the cyber-espionage units, those handling the electronic support measures. They also incorporated space related ISR systems, the Aerospace Reconnaissance Bureau and Satellite Main Station, the launch, telemetry, tracking and control facilities and research and development organisations. The SSF is also responsible for collection and collation of technical intelligence, and giving strategic intelligence support to theatre commands. It is a critical element of PLA power projection, defence in the space and nuclear domains, for all kinds of joint operations.

Broad PLA Structure[7]



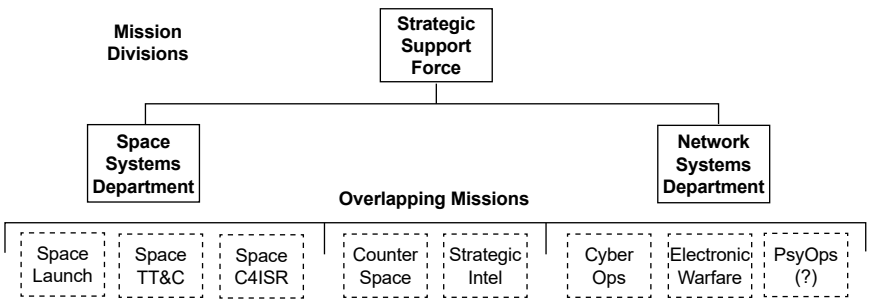
The SSF has been constituted as an independent theatre command. This gives it the importance and stature that China wants to accord for such

7. Central Military Commission, globalsecurity.org., at https://www.globalsecurity.org/military/world/china/cmc.htm. Accessed on June 26, 2021.

The Theatre Commands are fed by two co-equal, semi-independent branches of the SSF: the SSD, which is responsible for space operations, and the NSD, which is responsible for information operations.

capabilities in order to enable their effective employment in conflict. The SSF has a standard administrative structure like others, with a Staff Department, Equipment Department, Political Work Department and a Logistics Department. Then there are the operational Space Systems Department (SSD) and Network Systems Department (NSD). For the purpose of structure, the official phrase used is that "CMC leads, theatres fight, and services build". Some elements of the SSF are with the theatre commands for operations. Yet, the SSF being significantly strategic, it reports directly to the CMC for operations.[8]

PLASSF Missions and Structure[9]



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

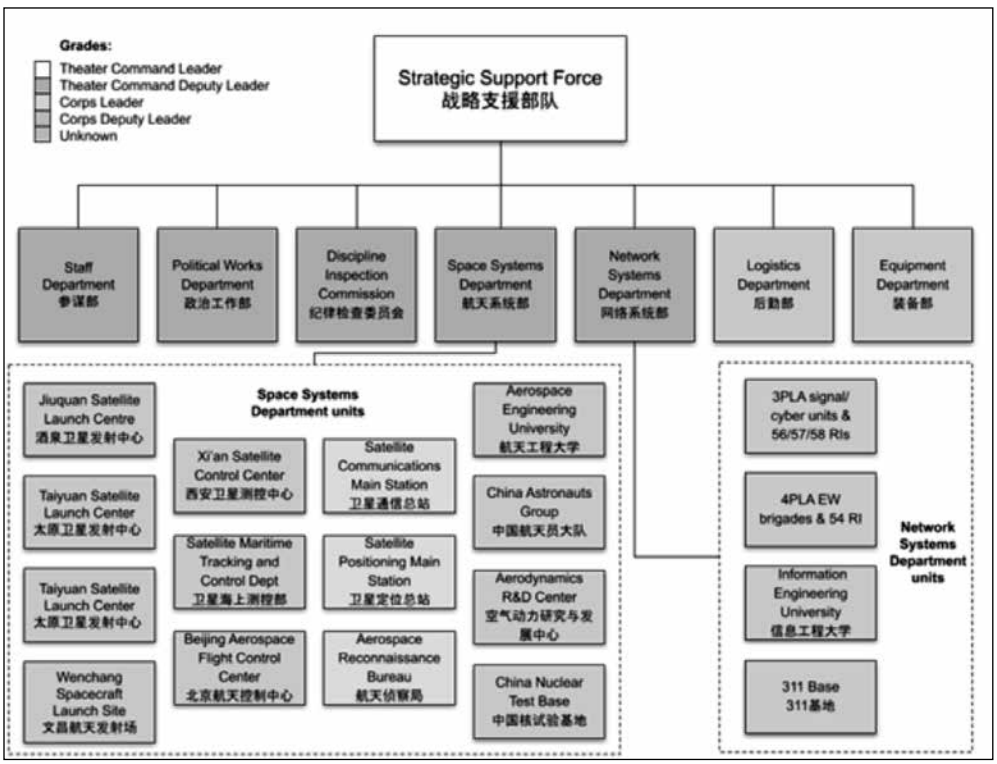
ORGANISATION LEVEL DETAILED STRUCTURE

The Theatre Commands are fed by two co-equal, semi-independent branches of the SSF: the SSD, which is responsible for space operations, and the NSD, which is responsible for information operations. Both independently

8. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era, Testimony to the U.S.-China Economic and Security Review Commission", National Defense University, February 15, 2018, at https://www.uscc.gov/sites/default/files/Costello_Written%20Testimony.pdf. Accessed on June 27, 2021.
9. Adam Ni, Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019", Publication: China Brief Volume: 19 Issue: 10, The James Town Foundation. May 29, 2019, at https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/. Accessed June 26, 2021.

develop their own personnel plan, execute their training and develop capabilities. The CMC coordinates integration where overlaps exist. The SSF components are relatively static. SSF forces are organised as "bases," that are a corps leader grade units.[10] Yet SSF has a dedicated space-based surveillance, survey, mapping and satellite navigation functions. SSF also controls and manages the Beidou satellites. The SSF regional bases continue to be created.

Organisation Level Detailed Structure[11]



10. Kevin L. Pollpeter, Michael S. Chase, Eric Heginbotham, "The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations", Rand Corporation, 2017, at https://www.rand.org/pubs/research_reports/RR2058.html. Accessed June 27, 2021.
11. Ibid.

SPACE SYSTEMS DEPARTMENT (SSD)

The Space Systems Department has all PLA's space-based C4ISR systems. These include the major satellite launch centres at Jiuquan, Taiyuan, Xichang and Wenchang.[12] The Space telemetry, tracking and control is fully amalgamated, and includes the aerospace flight control centre at Beijing, satellite control centre at Xi'an and the maritime satellite tracking and control. They also include Aerospace Research and Development, the Astronaut Corps and Network Systems Department, among many others.

THE SSD AND CHINA'S SPACE FORCES

The SSF's space mission is handled by the SSD. Getting all the military space elements together was a complex exercise. They now control the entire chain from launch, telemetry control, tracking, satellite or space systems control, space-based information flow, attack from space and defence of space-based assets and information security. Some non-military programs like China's manned space missions remains under the CMC Equipment Development Department. However, the ground station to feed all information to the PLA systems from Beidou navigation satellite system is now under the SSD.

It is unclear as to who controls the ballistic missile defence (BMD). On this count, there appears to be some overlap with the PLA Rocket Force, as well as the PLA Air Force (PLAAF). The July 2017, DN-3 anti-satellite missile test launch was reportedly carried out from the Jiuquan Satellite Launch Center,[13] possibly indicating that it could be under SSF. Clearly the SSF will be the main agency for space-based C4ISR.

NETWORK SYSTEMS DEPARTMENT (NSD)

The NSD integrates PLA's information warfare and cyber capabilities, and is responsible for the network mission, which includes signals

12. Mark Stokes, Gabriel Alvarado, Emily Weinstein, and Ian Easton, "China's Space and Counterspace Capabilities and Activities", Prepared for: The U.S.-China Economic and Security Review Commission, March 30, 2020, at https://www.uscc.gov/sites/default/files/2020-05/China_Space_and_Counterspace_Activities.pdf, pp. 26-27. Accessed on June 26, 2021.
13. Brian Weeden, "Current and Future trends in Chinese Counterspace capabilities", IFRI (French Institute of International Relations), November 2020, p. 26, at https://www.ifri.org/sites/default/files/atoms/files/current_and_future_trends.pdf. Accessed on June 27, 2021.

intelligence, cyber espionage, computer attack, electromagnetic warfare and psychological operations. Some of the selected erstwhile EW brigades have become part of the NSD. In addition, the 54th Research Institute and the Information Engineering University is also now under the NSD. Thus, it has the dominant role for all signal intelligence, cyber and EW tasks.[14] Both offensive and defensive cyber capabilities are now with SSF. Also part of it are the SSF Network Security Base, the Luoyang Electronic Equipment Testing Center, and the "Three Warfare" base that specialises in psychological operations.

INFORMATION OPERATIONS

The strategic Information Operations (IO) entails the engagement of all SSF elements to neutralise the adversary operational elements, and paralyse command and control in the early part of the conflict. It is achieved by the integrated use of various methods and elements of information warfare (IW), cyber espionage and cyber offensive. The entire IW force development, campaign planning and operations are part of IO. SSF is also tasked with PLA's psychological and political warfare. China's IW strategy[15] includes destruction of adversary military command and control (C2) structures; using state of the art electronic equipment to disrupt the communication system; use of illusions, and other techniques to outsmart the adversary intelligence system; and application Psychological Warfare (PW) through propaganda, disinformation and using various forms of media, to attack and mould enemy psychology.

CYBER AND ELECTRONIC WARFARE

China has created a new across-the-board structure for cyber and electronic warfare missions, and integrated networks and electronic warfare. The espionage and offense cyber operations are part of it. The

14. Ni and Gill, n. 9 .
15. D S Murugan Yadav, "China's Information Warfare Strategy and its implications for India", Centre for Land Warfare Studies, January 15, 2021, at https://www.claws.in/chinas-information-warfare-strategy-and-its-implications-for-india/. Accessed on June 26, 2021.

SSF also looks after technical reconnaissance. It now focuses and controls the intelligence sourcing for critical operational needs. China has also evolved a new strategy and doctrine for the use of force in cyberspace. The cyber operations allow China a low-cost deterrent and conflict-escalation control.[16]

The Network Systems Department (NSD) the "cyberspace force" controls the cyber mission. Their missions include cyber warfare, EW and psychological warfare. All erstwhile strategic cyber espionage forces are now a part of the NSD, as also are the related research institutes, the PLA Information Engineering University[17] and Luoyang Foreign Language Institute. The former PLA's computer network attack forces have now been integrated with the cyber-espionage elements.

For strategic EW missions, China uses separate dedicated units for attacking computer networks and radars. They have created a joint Network-Electronic Bureau (NEB) that is responsible for the cyber and EW missions for the entire Chinese military.[18] The 54th Research Institute, responsible for research and development of operational electronic and network countermeasures, is part of NSD now.[19]

Earlier EW units under the SSF, were called "electronic countermeasure brigades."[20] The PLA's integrated network and electronic warfare, is based on close coordination of cyber and electronic warfare. These cannot fight

16. OFFICE OF THE SECRETARY OF DEFENSE, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2020, p. 74, at https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF .Accessed on June 27, 2021.
17. Saikiran Kannan and Abhishek Bhalla, "Inside China's cyber war room: How PLA is plotting global attacks", *India Today*, August 6, 2020, at https://www.indiatoday.in/world/story/inside-china-s-cyber-war-room-how-pla-is-plotting-global-attacks-1708292-2020-08-06. Accessed on June 27, 2021.
18. Kartik Bommakanti, "Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army", Observer Research Foundation, p. 17, at https://www.researchgate.net/publication/334605543_Electronic_and_Cyber_Warfare_A_Comparative_Analysis_of_the_PLA_and_the_Indian_Army. Accessed June 27, 2021.
19. Ni and Gill, n. 9 .
20. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era, Testimony to the U.S.-China Economic and Security Review Commission", National Defense University, February 15, 2018, at https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf. Accessed on June 27, 2021.

independent battles. The SSF put the two together for the conduct of both espionage and offense operations.

IMPORTANCE OF PUTTING TOGETHER THE SSF

China's approach to coordinating and combining the space, cyber and electromagnetic domains, which is now part of the SSF, has been in special focus recently. China closely watched and imbibed lessons from the 1991 Persian Gulf War, and learnt the importance of informationised warfare. China not only understood the future of warfare, it also understood its own vulnerabilities. It was clear after the Gulf War that information technology integrated warfare could be a game-changer and support clear military superiority.[21] From there came the concept of "network-centric warfare." The space-based command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) was the key to informationised warfare. China then went big into space-based assets such as Beidou navigation satellites, space-based surveillance platforms and communications and relay satellites. All these would support surveillance, reconnaissance and precision strikes.

After a series of high-visibility cyber incursions targeting the US defence and other strategic websites, the sophistication and scope of China's military cyber forces became known. In 2007 China also demonstrated anti-satellite capabilities. The SSF will clearly support China's military posture, which has shifted from territorial defence to power projection well beyond its shores. The putting together of the three critical correlated domains will also help to ensure better access to each other. They will also support counter-intervention.

China's SSF has obviously looked closely at the US Strategic Command (USSTRATCOM), which broadly has similar responsibilities for space, cyber, strategic EW and strategic information support.

21. Peter Mattis, "China's 'Three Warfares' in Perspective", War on the Rocks, January 30, 2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/. Accessed on June 27, 2021.

The SSF's space, cyber and electronic missions support the psychological operations by providing cross-domain inputs and increase overall impact.

The SSF's space mission has elements responsible for space-based C4ISR. The SSF's information warfare mission handles technical reconnaissance and offensive cyber operations. Psychological operations were also incorporated into the SSF. The psychological domain is very important for PLA's "Three Warfares", which includes combining effects of public opinion influence, psychological warfare and legal interventions.[22]

THE SSF AND THE THREE WARFARES

The SSF also handles the military's "Three Warfares" missions[23] to support Chinese propaganda and information warfare themes and undermine those of the adversary. Peacetime integration and operations allow smooth transition during hostilities. The SSF's space, cyber and electronic missions support the psychological operations by providing cross-domain inputs and increase overall impact.

THE JOINT STAFF DEPARTMENT (JSD) AND THE SSF

The CMC now also has the Joint Staff Department (JSD) that acts as an interface with SSF and conveys operational decisionsto the CMC. The JSD also provides administrative support for strategic missions and units. A separate JSD has dedicated bureaus to coordinate various SSF operations for battlefield environment support.

WARTIME OPERATIONAL COMMAND

The SSF maintains dedicated regional branches at the five joint force Theatre Commands and national-level elements of the Rocket Forces, the Air Force and the Navy, with distinct cyberspace command elements down

22. Ibid.
23. Ibid.

to the Independent Operational Group (IOG) level in order to support combat operations particularly during major wars against sophisticated militaries.[24] The IOG is a joint force created during operations for waging information warfare. Subordinate elements, called the "groups", will be put in place for cyber warfare, EW, psychological warfare, air defence electronic countermeasures and information support. The SSF has both operational and administrative roles.

The SSF now has intelligence responsibilities and is in charge of centralising the strategic-level technical collection. The PLA understands "intelligence" as analysis from all-sources that support command decision making.

INTELLIGENCE AND TECHNICAL RECONNAISSANCE

The SSF now has intelligence responsibilities and is in charge of centralising the strategic-level technical collection. The PLA understands "intelligence" as analysis from all-sources that support command decision making. The "technical reconnaissance" on the other hand refers to technical intelligence collection for military operations. Like all modern forces, China uses satellites, signals intelligence (SIGINT) sites, ships, and aircraft, radars, Unmanned Air Systems, ISR aircraft, antisubmarine warfare sensors and external—especially Russian—assistance.[25] Any data becomes meaningful only when processed into usable intelligence. The newly formed JSD Intelligence Bureau receives and processes intelligence inputs received from the theatre commands, who gather and analyse their own operational and tactical intelligence. The whole exercise has been done to move away from old army-dominated system.

24. Yossef Bodansky, "The Real Culprit – The PLA's Strategic Support Force", ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 669, February 2020, at https://www.ispsw.com/wp-content/uploads/2020/02/669_Bodansky-1.pdf Accessed on June 27, 2021.
25. Lt Col Thomas R. McCabe, USAFR, (Retired), "Chinese Intelligence, Surveillance, and Reconnaissance Systems", *Journal of Indo-Pacific Affairs*, Spring 2021, at https://media.defense.gov/2021/Mar/07/2002595026/-1/-1/1/25%20MCCABE.PDF. Accessed on June 27, 2021.

NETWORK AND ELECTRONIC WARFARE

The JSD-NEB manages the cyber and electronic warfare missions in the new structure, for all entities including the SSF, theatre commands and other services. The JSD-NEB is responsible for all the integration functions. They also provide operational guidance, de-conflicting areas of responsibility, and establishing rules of engagement.[26] The SSF cyber force concentrates on strategic national-level operations. The operational and tactical level EW and cyber are handled by services and theatre commands. A national joint Network-Electronic Countermeasure organisation supports building of a network of electronic countermeasure (ECM) centres. The ECM centres also handle electronic intelligence, electronic support measures and offensive action covering the entire electromagnetic spectrum.

INFORMATION AND COMMUNICATIONS BUREAU

The JSD's Information and Communications Bureau (ICB) now provides force-wide information systems, communications and support for high-level war-fighting command and control. The PLA's information support base has also moved under the JSD. However, the SSF controls ground-based satellite communication infrastructure. The SSF is also responsible for the flow of operational space-based data. Clearly there are some overlaps between the SSF and the JSD-ICB.

THE SSF'S STRATEGIC MISSIONS AND ROLES

China fully understands that information is a strategic resource in warfare. Using the outer space to advantage, and combining with cyber and exploitation of the electromagnetic spectrum, and denying these to the adversaries is the only way for PLA to dominate the war zone. Denial of these domains will adversely affect operations of any modern military force that depends on networked systems. The creation of the SSF unified all information related strategic functions and created the centralised support

26. Lt Gen (Dr) R S Panwar, "China's Strategic Support Force And Its Implications For India, Future Wars", June 16, 2020, at http://futurewars.rspanwar.net/chinas-special-support-force-and-its-implications-for-india-part-ii/. Accessed June 28, 2021.

to the field units. This unification greatly improves the chances of PLA achieving information superiority.

STRATEGIC INFORMATION SUPPORT

The SSF's space force contains the "strategic brace support," which includes the critical space-based intelligence and communications. SSF relies on its many space-based intelligence and communications assets for strategic information flow. Cyber force provides cyber-related technical data for both offensive and defensive operations. SSF helps centralise technical intelligence collection, as well as its management and dissemination to all concerned, including theatre commands. This will also allow power projection in space and nuclear domains, and enable joint operations.

ENABLING PLA POWER PROJECTION

The SSF conducted many joint exercises and training across China in 2019. Among them was a joint drill off China's south-eastern coast. SSF units also conducted joint communications training to the theatre commands.[27] SSF is the main information support for deep sea maritime forays, long-range precision air strikes, extended range unmanned aerial vehicle operations and strategic offensive and deterrent air operations. Even the conventional strikes are heavily dependent on target information, en route information support and electronic warfare support. Additionally, the PLA Rocket Force also depends on the SSF for target detection, identification, targeting, and battlefield damage assessment. SSF information flow is also critical to the maritime operations of the PLA Navy.

STRATEGIC INFORMATION OPERATIONS

The SSF is the primary force for information warfare by PLA element, and for "information dominance" in conflict. Paralysing enemy operational

27. OFFICE OF THE SECRETARY OF DEFENSE, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China", 2020, p. 62, at https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF. Accessed on June 28, 2021.

systems in the early phases of war, while securing own will be the military aim. Clearly information dominance is mandatory for military success today. The SSF will launch a multidimensional information warfare campaign using all SSF sub-components and run it through the war. Psychological and electronic warfare are important for pre-war period to highlight and scare the adversary about the political and military risks associated with aggression. EW has the ability to greatly supplement the cyber operations. EW of course also means transition to open warfare. Electronic warfare is used by the PLA both for defensive operations and also for coercion and information denial. China now has a concept called "cyber-electromagnetic sovereignty."[28] PLA could one day treat it a right to deny or degrade adversary satellite-based sensors and systems.

Electronic warfare will be used as a key standoff weapon. It will significantly diminish the intelligence collection and information processing capacity of an adversary. Such attacks will be coordinated between the land, air and sea-based platforms. Even as the full scale war begins, psychological operations will support own public morale and weaken or dent the enemy's will to fight. It will also support diplomatic and political narratives. Chinese believe information dominance is the core of the "three dominances" of information, air and space.[29] Cyber and intelligence operations are time-sensitive, requiring quick updates and techniques that are constantly changing and evolving. Cyber and electronic attacks cannot be repeated. Their effects are particularly pronounced in the initial stages of conflict.

US AND CHINESE APPROACH

There are clear differences between USCYBERCOM and the SSF's cyber force operational responsibilities. The SSF is responsible for "all" aspects of information warfare, including those involving kinetic, cyberspace, electromagnetic and psychological domains. The PLA believes space and

28. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era, Testimony to the U.S.-China Economic and Security Review Commission", National Defense University, p. 40, February 15, 2018, at https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf. Accessed on June 28, 2021.
29. Ibid., p. 46 Accessed on June 28, 2021.

cyber must work in unison. Currently, the US does not consider the need for convergence of cyber, space and electronic warfare at the strategic level. The United States views cyber warfare in terms of destruction and denial. They focus more on the cyber-attacks with kinetic effects and the destruction and manipulation of data. China also believes that psychological operations must also be part of the same domain, and that cyber operations must be used for psychological manipulation.

CHALLENGES AHEAD FOR THE SSF

While the SSF integrates many components, there are still many organisational issues that need addressing. There are pulls and pressures between the civilian and military elements of cyber threats and responses, and who must control what. The SSF having dual responsibilities for both "force construction" and operations bothers both the service HQs and Theatre Commanders. The USSTRATCOM provides direct support to the US combatant commands. The SSF is more a service-oriented force that serves a functional role. Perhaps one-day, PLA may also create joint functional combatant commands akin to those in the US. Yet CMC may keep the nuclear, space and information warfare under very close central control. Keeping the SSF as a separate force also makes it cost-effective in times of counter-productive rivalry for funding and resources.

Some argue that over centralisation of such cutting-edge missions contradicts the PLA's goals of rapid expansion and modernisation. China is clearly aware of the necessity for resource conservancy and centralised control for better development. Could functional services like the SSF and PLA Rocket Force, sitting atop the theatres, weaken the Theatre Commander's flexibility and control?

Beyond just civil-military issues, the PLA faces challenges to field a modern cyber force. SSF's cyber operations are overwhelmingly focused on espionage and offense, and PLA's cyber defence. How will the SSF manage cyber defence of private, civilian and critical infrastructure networks? This is the responsibility of the Ministry of Public Security and Cyberspace Administration of China,

In last three decades, China has made high investments in the space programs and achieved major milestones. They have an operational global satellite navigation system now. Most elements of the Chinese Space Station are in place.

who are responsible for securing China's critical information infrastructure.[30] There are critical questions as to how PLA will handle the unclear divide between peacetime and wartime targeting. SSF reinforces China's growing military strength and readiness for informatised war at global scale. China does have the technical and operational capability to use these for strategic effects.

CHINA'S SSF – IMPLICATIONS AND CHALLENGES FOR INDIA

China is investing heavily and has surpassed India in most of the domains controlled by the SSF. Chairman Mao had declared in 1958 to make China an equivalent superpower. This aspect has nearly been achieved. In last three decades, China has made high investments in the space programmes and achieved major milestones. They have an operational global satellite navigation system now. Most elements of the Chinese Space Station are in place. China has surpassed USA in annual space launches for the last three years. Of interest to SSF is also the Yaogan satellite constellation[31] meant to survey China's neighbourhood using space-based Synthetic Aperture Radar (SAR), electro-optical systems, and also recording of radio transmissions and electro-magnetic signatures. The satellites include optical, radar and signal intelligence instruments on board.[32] China is known to have over 200 military satellites in orbit, and plans to launch 100 more satellites by

30. Rogier Creemers, Paul Triolo, Xiaomeng Lu, and Graham Webster, "Chinese Government Clarifies Cybersecurity Authorities" (Translation). New America, September 25, 2020, at https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-government-clarifies-cybersecurity-authorities-translation/. Accessed on June 28, 2021.
31. Younis Dar, "Why China's Latest Military Satellites Give It Unparalleled Advantage Over BECA Allies – US & India", *Eurasian Times*, October 28, 2020, at https://eurasiantimes.com/chinas-latest-military-satellites-give-it-unparalleled-advantage-over-us-india/. Accessed on June 28, 2021.
32. Elizabeth Howell, "China has 3 new spy satellites in orbit after Long March 4C launch", Space.com. March 20, 2021, at https://www.space.com/china-yaogan-31-military-satellite-launch-march-2021. Accessed on June 28, 2021.

2025.[33] Communications satellites will allow quick transfer of data for all SSF missions.

For electronic warfare, SSF will use satellites, and dedicated EW aircraft, including the powerful H 6G aircraft variant.[34] Most PLAAF aircraft have EW suites. China has also dedicated EW ships. Chinese have been extensively involved in hacking computers and personal data the world over. China's successful hacking attempts helped them collect huge data, and this when applied with artificial intelligence makes it very useful for applications.[35] China has a long history of meddling with Indian servers. In 2008, Chinese hackers tried to break down servers of the National Informatics Centre, the National Security Council and the Ministry of External Affairs.[36]

Chinese bombarded the Indian power system with malware after the Galwan Valley clashes in June 2020. The cyber weapons, which are low cost and give plausible deniability, are being preferred. The Indian Ministry of Defence's annual report makes reference to the PLA's use of "unorthodox weapons" along the LAC.

Chinese bombarded the Indian power system with malware after the Galwan Valley clashes in June 2020.[37] The cyber weapons, which are low cost and give plausible deniability, are being preferred. The Indian Ministry of Defence's annual report makes reference to the PLA's use of "unorthodox weapons" along the LAC. Earlier there were

33. "China to launch 100 additional satellites by 2025: Official", *Global Times*, July 10, 2019, at https://www.globaltimes.cn/content/1157389.shtml. Accessed on June 28, 2021.
34. Bureau report, "China Modifies H-6G Bomber into Electronic Warfare Aircraft", Defense World, January 22, 2018, at https://www.defenseworld.net/news/21806/China_Modifies_H_6G_Bomber_into_Electronic_Warfare_Aircraft#.YNmFtegzZPY. Accessed on June 28, 2021.
35. Garrett M. Graff, "China's Hacking Spree Will Have a Decades-Long Fallout", *Wired*, February 11, 2020, at https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/. Accessed on June 28, 2021.
36. Prabhjote Gill, "The Chinese cyber threat is real — and India's best defence right now is to keep its outage time limited", *The Business Insider*, April 9, 2021, at https://www.businessinsider.in/defense/news/the-chinese-cyber-threat-is-real-and-indias-best-defence-right-now-is-to-keep-its-outage-time-limited/articleshow/81981886.cms. Accessed on June 28, 2021.
37. The Print Team, "How Chinese cyber-attacks, Mumbai blackout depict a new era of low-cost high-tech warfare", The Print, March 03, 2021, at https://theprint.in/opinion/how-chinese-cyber-attacks-mumbai-blackout-depict-a-new-era-of-low-cost-high-tech-warfare/614892/. Accessed on June 28, 2021.

reports that these could be some sort of Chinese directed-energy microwave weapons.[38] India has a fairly robust space and missile program. With the formation of Defence Space Agency (DSA), the coordination between the armed forces and the space agencies has increased for optimum utilisation of space assets for operational purposes. India is enhancing its military capabilities in space with new sensors and satellites.[39]

However, India lags behind China and Pakistan on information warfare and psychological operations. Similarly, a much more ethical India has refrained from utilising cyber to target adversary utilities. With the formation of Defence Cyber Agency (DCA), the cyber warfare capability is expected to have increased. This form of warfare will be critical during lead up to the actual conflict. India does have Cyber and Information Security (C&IS) division,[40] which deals with matters relating to cyber-crime, cyber-security, national information security policy and guidelines (NISPG), and their implementation.

Induction of Rafale has brought in the latest SPECTRA EW suite[41] for a modern aircraft. DRDO's Defence Avionics Research Establishment (DARE) has been developing avionics for upgrade programs for several Indian Air Force (IAF) aircraft, including the AEW&C aircraft. It works closely with HAL. LCA EW suite is currently being evolved by the Israeli firm Elisra,[42] in consultation with DRDO. Defence Electronics Research Laboratory (DLRL) has developed the HIMRAJ Ground Based Mobile ELINT System (GBMES).

38. Aakriti Sharma, "Has India Finally Acknowledged That Chinese PLA Used Microwave Weapons Against Indian Soldiers In Ladakh?", *The EurAsian Times*, January 6, 2021, at https://eurasiantimes.com/has-india-finally-acknowledged-that-chinese-pla-used-microwave-weapons-against-indian-soldiers-in-ladakh/. Accessed on June 28, 2021.
39. Manjeet Negi, "India enhancing military capabilities in space with new sensors, satellites", *India Today*, March 26, 2021, at https://www.indiatoday.in/india/story/india-military-capabilities-space-drdo-dsa-sensors-satellites-1784084-2021-03-26. Accessed on June 30, 2021.
40. Cyber and Information Security (C&IS) division, Ministry of Home Affairs, Government of India, at https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division. Accessed on June 30, 2021.
41. SPECTRA, state-of-the-art Rafale multi-spectral integrated defensive aids suite, Thales Group, at https://www.thalesgroup.com/en/spectra-state-art-rafale-multi-spectral-integrated-defensive-aids-suite. Accessed on June 30, 2021.
42. ANI, "Israeli firm bags electronic warfare suite deal for LCA Tejas", *Business Standard*, December 26, 2018, at https://www.business-standard.com/article/news-ani/israeli-firm-bags-electronic-warfare-suite-deal-for-lca-tejas-118122600906_1.html. Accessed on June 30, 2021.

Indian Navy's Shivalik class frigates employ BEL Ellora EW Suite. P-17A Nilgiri-class frigates, will have a more advanced BEL Ajanta EW suite.[43] India needs Software Defined Radios for all its operational aircraft and surface systems. There are many other EW systems under development in India, but a lot more needs to be done on this score. The US Defense Department is planning to invest much more in electronic warfare capabilities, so as to achieve superiority in the electromagnetic spectrum.[44] India needs to do the same.

Finally, there is a need for India to integrate the various elements of space, cyber, information warfare and electronic warfare in its own way to increase operational efficiency.

43. Daily Hunt, "Project-17A: India's Trump Card against Chinese Ships in Indian Ocean", May 11, 2018, at https://m.dailyhunt.in/news/india/english/defence+lover-epaper-defence/project+17a+india+s+trump+card+against+chinese+ships+in+indian+ocean-newsid-87599948. Accessed on June 30, 2021.
44. Jon Harper, "Electronic Warfare Spending on the Rise", *National Defense*, July 23, 2019, at https://www.nationaldefensemagazine.org/articles/2019/7/23/electronic-warfare-spending-on-the-rise. Accessed on June 30, 2021.