CENJOWS

ISSUE BRIEF
IB/13/24

ANALYSING INFORMATION SUPPORT FORCE (ISF) OF CHINA AND ITS IMPACT ON INDIA

MR UJJAWAL UPADHYAY

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

ANALYSING INFORMATION SUPPORT FORCE (ISF) OF CHINA AND ITS IMPACT ON INDIA

Mr Ujjawal Upadhyay is a Research Intern at CENJOWS, New Delhi.

Abstract

Cyber Warfare and Information warfare are the two most employed tools within the spectrum of gray zone warfare[1] that allows a country to target another country's critical infrastructure, break up communication lines, take vital and private company data, organise it for their gain, or use it as leverage whenever and wherever they choose. This process is characterized by ambiguity, which the enemy uses to increase deterrence. The Gulf War of 1990s has been considered "Information War" primarily due to the coalition forces' deployment of cutting-edge information technologies for armament, intelligence gathering, supply, and analysis and the widespread belief that these tools significantly reduced coalition losses. In the same era, cautious planners started considering safeguarding the armed forces as they grew more reliant on sophisticated technology and information networks. These tactics developed by the United States were closely monitored by the strategists and top leadership of China's People's Liberation Army (PLA). The following years saw a major shift in the tactics of the PLA, the reforms it underwent in 2015 which led to the raising of the Strategic Support Force (SSF) and the People's Liberation Army Rocket Force (PLARF). The recent development on 19th April 2024, in which the SSF was reorganised into three separate wings (Cyberspace Force, Aerospace Force and Information Support Force)

raises questions about why such a decision was taken by the Chinese government. With this background, this issue brief aims to analyse China's newly carved-out Information Support Force (ISF) from the erstwhile Strategic Support Force (SSF) and the threats they pose to India.

Introduction

The discussions on Information Warfare and the rising relevance of the cyber and space domain have gained substantial relevance and are much talked about today. However, the use of information as a means to cause disruption in the enemy's forces has been prevalent for ages. Stratagems like Chanakya and Sun Tzu in their books "Chanakya-Neeti" and "The Art of War" respectively talk about how to cause chaos among the adversarial armies even before contact to deceive them through various means and methods to break their morale. The tactics of Information Warfare got refined and more complex with the advances in the fields of information technology and cyber warfare. This was duly supported by the wide use of social media and widespread digitisation, to gather information and use that information to control public opinions.[2]

In the 2013 edition of "The Science of Military Strategy," a paper of the Academy of Military Science[3], the Chinese military discussed cyberwarfare from a comprehensive perspective in public. It highlighted that, in the modern world, cyberspace has emerged as a brand-new and crucial theatre of armed conflict. The Ministry of National Defence's 2015 report, "China's Military Strategy," carried a tone similar to the previous paper.[4] Since then, there have been plenty of news reports about rising cyber threats emerging from China. The majority of them support the idea that China is using its cyber power to gain worldwide dominance and that the Chinese government is involved in several destructive cyber activities behind the scenes.

A few inferences can be drawn about China's cyberspace policy and national security strategy based on the above approach. These are: Firstly, China has not created its cyber capabilities overnight. Since the US and Russia have been refining and adopting their respective cyber warfare strategies and tactics, the leadership in China is to ponder upon the future of warfare and henceforth develop its capabilities. The second is that China's military policy has been modified to meet the country's security environment, internal circumstances, and foreign military activity and is in line with the government's beliefs regarding cyber warfare.

The Chinese Strategic Support Force (SSF), founded in 2015, as a fifth and independent service of the People's Liberation Army (PLA), the Chinese Strategic Support Force (SSF) marked a significant advancement in China's military doctrine. The integration and advancement of capabilities in the cyber, electronic warfare, and space domains were the responsibilities of this specialist branch. China's pursuit of informationised warfare, which aims to establish control in the information domain essential for contemporary combat, heavily relies on the SSF.

The SSF’s responsibilities were to develop offensive capabilities to counter adversaries' cyber operations while simultaneously working on shielding Chinese networks from cyber assaults. All things considered, the SSF's creation highlighted China's dedication to reforming its armed forces and realigning them to the arising security threats. As part of China's overarching military policy, the SSF enhanced its ability to conduct operations across various domains by combining space, cyber, and electronic warfare into a single force that may change the course of future conflicts. In April 2024, the SSF was split into the Information Support Force, the Cyberspace Force, and the Aerospace Force.[5] The former SSF components will now be directly supervised by the Central Military Commission (CMC), working alongside the Joint Logistics Support Force (JLSF), which was established in 2016. This further establishes the efforts the Chinese have been making to continuously evolve their military and be up to date with the latest trends in warfighting.

Chinese Military Reforms Made under President Xi

The two significant displays of U.S. military might in the CCP's hemisphere during the 1990s namely, the Gulf War and the Taiwan Strait Crisis were significant turning points as the American forces adequately displayed the use of technology in ISR to overwhelm the enemy with superiority in information. Chinese military leadership along with the political class were taken aback and to some extent intimidated by the skill of American forces, admitted that their country lacked the means to fight a contemporary war and keep other countries from interfering in the area. When President Xi Jinping took office in 2012, there was a significant push from his side to reform the Chinese military into a world-class fighting force and shift from defensive roles to more expeditionary roles. Xi has pushed military changes more than his predecessors, championing what he terms the "Chinese Dream," an agenda to reinstate China as a major force at the global level.[6] Some of the major reforms included, new unified theatre commands, considerable manpower reductions, enhanced military-civilian cooperation and the establishment of new services such as the Rocket Force, Strategic Support Force, (SSF) Joint Logistics Support Force (JLSF). He worked to make the PLA(N) a significant maritime power rather than a primarily territorial force. Together with these significant reforms, there was also the creation of the Strategic Support Force.

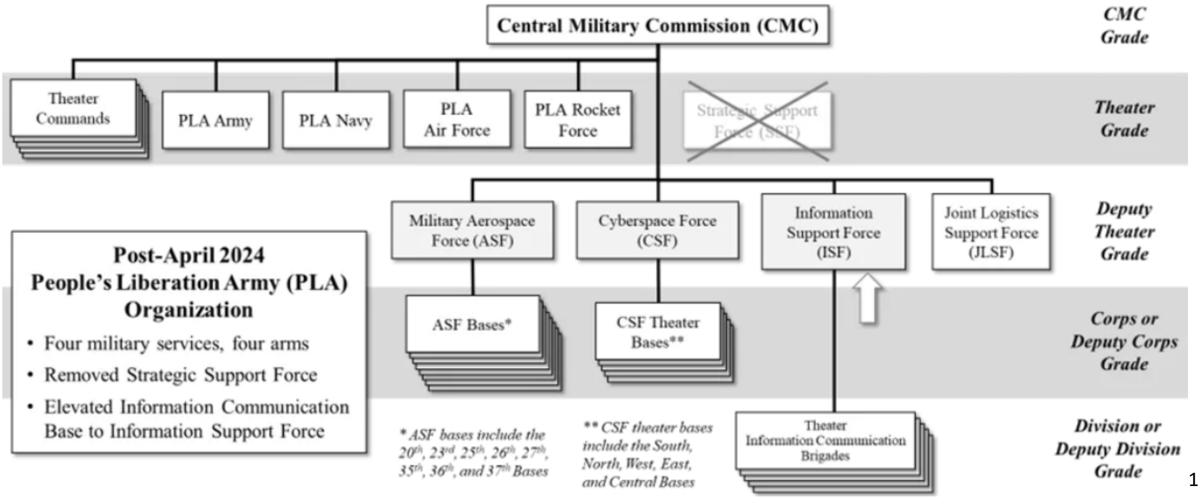
Information Support Force (ISF)

In the domains of Information Warfare, as discussed above, one component of the SSF was restructured into the Information Support Force or the ISF.[7] The ISF is based on Xi's '*wǎngluò xìnxī xìtǒng'* [网络信息体系], which when loosely translated, refers to 'internet information system'. Though there is no concrete definition of this term, experts suggest that it means that the forces need to be modernised and informationalised to fight the wars of the modern era and gives due recognition to cyberspace as a separate domain of modern warfighting and that the cyber forces no longer operate as a support arm. These reforms have been implemented in the SSF to weaponize them and deviate from their custom of providing PLA units with superior information and intelligence.

The PLA disbanded the SSF highlighting an altered strategy given the requirement of contemporary warfare's. According to reports, its broad scope has compromised its fullest efficacy, which prompted the latest restructure. Disregarding speculation of corruption, the communications network, cyberspace, and aircraft components all carried out their distinct tasks somewhat autonomously from the SSF personnel[8]. Hence, the removal of the SSF can be attributed to the PLA's increasing emphasis on battlespace information governance in multi-domain coordinated joint operations and enhancing strategic data-driven assets[9].

Organisational Reforms of PLA

The People's Liberation Army (PLA) is currently undergoing organisational reforms to maintain four domain-focused services, four strategic/functional forces, and five regionally focused theatre commands (comprising the "triple matrix" organisation) which can be seen in Fig 1. Even though it was unable to create long-lasting synergies between the various forces involved in information warfare and support, the SSF from the beginning was intended to be a transitional force structure rather than a permanent one[10]. It served a useful purpose in initiating and guiding more extensive military reforms as demonstrated in Fig 2 which we is witnessed as of now. The SSF had a dual role as a holding institution by consolidating critical strategic capabilities and removing them from the erstwhile General Staff and General Armament Departments.[11]


Central Military Commission (CMC)
CMC Grade
Theater Commands
PLA Army
PLA Navy
PLA Air Force
PLA Rocket Force
Strategic Support Force (SSF)
Theater Grade
Military Aerospace Force (ASF)
Cyberspace Force (CSF)
Information Support Force (ISF)
Joint Logistics Support Force (JLSF)
Deputy Theater Grade
Post-April 2024
People's Liberation Army (PLA) Organization
• Four military services, four arms
• Removed Strategic Support Force
• Elevated Information Communication Base to Information Support Force
ASF Bases*
CSF Theater Bases**
Corps or Deputy Corps Grade
* ASF bases include the 20th, 23rd, 25th, 26th, 27th, 35th, 36th, and 37th Bases
** CSF theater bases include the South, North, West, East, and Central Bases
Theater Information Communication Brigades
Division or Deputy Division Grade

[12]

Fig 1: The organisation of PLA forces post-reorganisation

(source: Jamestown)

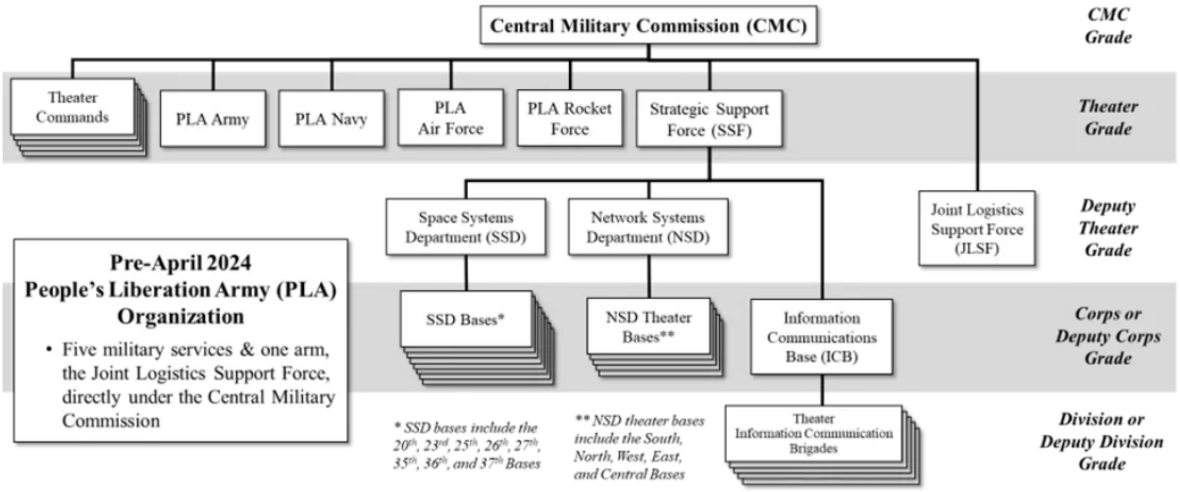

Central Military Commission (CMC)
CMC Grade
Theater Commands
PLA Army
PLA Navy
PLA Air Force
PLA Rocket Force
Strategic Support Force (SSF)
Theater Grade
Space Systems Department (SSD)
Network Systems Department (NSD)
Joint Logistics Support Force (JLSF)
Deputy Theater Grade
Pre-April 2024 People's Liberation Army (PLA) Organization
• Five military services & one arm, the Joint Logistics Support Force, directly under the Central Military Commission
SSD Bases*
NSD Theater Bases**
Information Communications Base (ICB)
Corps or Deputy Corps Grade
* SSD bases include the 20th, 23rd, 25th, 26th, 27th, 35th, 36th, and 37th Bases
** NSD theater bases include the South, North, West, East, and Central Bases
Theater Information Communication Brigades
Division or Deputy Division Grade

Fig 2: The organisation of PLA forces pre-reorganisation

(source: Jamestown) [13]

Major Attacks on Indian systems by the Chinese – Attack; impact, method/type, countermeasures

As per the Cyber Emergency Response Team (CERT), India faced 5 billion cyber-attacks in 2023[14]. Both private and government institutions were targeted by various entities. The threat was to the extent that the systems of the Prime Minister's Office were compromised too in February of 2024 as per CERT.[15] The files were extracted and uploaded on an open domain called GitHub for other hackers to exploit and attack the systems. A similar attack was conducted by the Chinese entities on the servers of the Employees' Provident Fund Organisation (EPFO) recently[16] and a similar type of strategy was adopted where the data was uploaded in the open domain exposing the vulnerabilities of the Indian systems for everybody to exploit[17].

The Chinese have been engaging in acts of cyber espionage and attacks on Indian critical infrastructure since 2020. They have been targeting power grids in major Indian metropolitan cities as well and a few attempts were made to attack the power grids in Ladakh though they were unsuccessful[18]. Some of the recent successful attempts by the Chinese include the following incidents-

- Reports allude to the crashing of the Sukhoi 30 plane near the India-China border on May 23, 2017, cyberattack[19]. The Indian Air Force has concluded that cyber weapons, possibly from China, were used to bring down their Sukhoi fighter.[20]

- In October 2020, during the COVID-19 pandemic, the Indian and Chinese forces were locked on the Line of Actual Control (LAC). To warn India not to push its border claims, China launched a cyberattack against India. It was to cause a massive power outage in Mumbai. [21]

- Following the October 2020 Mumbai power outage, Chinese state-sponsored hacker organisations launched cyberattacks against two seaports (VOC, Tuticorin and Jawaharlal Nehru Port, Mumbai)[22] and at least ten strategically significant nodes in India's power infrastructure. Including the vaccine manufacturing systems of Serum Institute and Bharat Biotech, two Indian companies.[23w]

To carry out and accomplish these attacks, the Chinese state is sponsoring various hacker groups and tasking them to find and exploit various vulnerabilities in Indian cyber networks[24]. Some Chinese hacker groups and their actions directed towards India-

- Red Echo and Shadow Pad, proxy groups backed by Chinese MSS have targeted Indian power sectors repeatedly along with twelve critical infra to steal confidential data and disrupt Indian supply chain networks.[25] Further, against the backdrop of the Galwan skirmish, these groups had also temporarily set up internet access to advance Chinese strategic ambitions.
- APT41, notorious for its surveillance capabilities and ransom attacks, has carried out multiple phishing attacks, and compromised data linked to recent tax regulations and SARS Cov-19 within Indian soil[26] disguised as part of the government agencies.
- Emissary Panda(APT27) has been actively involved in carrying out phishing attempts against military and security agencies.[27] Apart from targeting private firms, they have further attempted to dissipate malware into systems to collect plans and layouts concerning India’s strategic interests and armed forces
- APT-C-0 along with Stone Panda (APT10), has been connected to cyberespionage efforts aimed against vital infrastructure, defence contractors, and Indian government institutions.[28] They have a reputation for utilising sophisticated malware and spear-phishing schemes to obtain unauthorised access to private data. APT 10 on the other hand has mostly carried out operations involving spear-phishing and theft of software

vulnerabilities. It has concentrated on obtaining patents and confidential data from a variety of businesses, particularly aviation, healthcare, and manufacturing.

Tactics adopted by Chinese against the backdrop of Russia-Ukraine War

The Chinese are closely watching the conflict and are drawing lessons out of it while trying to evolve their tactics and implement these against their adversaries.[29] It is important to analyse how cyber tactics are evolving in the current conflicts that are redefining the current geopolitics and will shape the future of warfighting. The battle has clearly illustrated how conventional military tactics and cyber operations can be combined to create a hybrid warfare strategy. In addition to using conventional military assets, cyberattacks were employed to interfere with Ukrainian forces' command structures, intelligence collection, and communications. The targeting of vital infrastructure, including financial systems, telecommunication networks, and power grids, highlighted how susceptible these services are to cyberattacks while their impact on a country's functioning is impeccable. As per the Royal Military state officials, China initiated strikes on Ukrainian armed forces, establishments and nuclear facilities soon before the Russian attack. The UK forces also reported claiming over six hundred sites, involving Ukraine's military service, were exposed to numerous malware attacks orchestrated by China. Most of the PLA units have been assigned to obtain information on the Ukraine crisis.[30]

These assaults were aimed at sabotaging operations, spreading chaos among the public, and creating mistrust among the people and the government. Disinformation campaigns using cyber operations were used to generate confusion, spread propaganda, and change public opinion intended to undermine morale, sway public opinion abroad, and advance military goals. The conflict made it clear how critical cyber resilience and preparedness are for governments and enterprises. In order to mitigate the effects of cyberattacks, it emphasized the necessity of strong cybersecurity plans, incident response skills, and continuous investment in cyber defences. A comprehensive look at China's efforts and build-up indicates that the country has been increasing the number of attacks it launches on the critical infrastructure of the target nations, while also putting more of an emphasis on enhancing the capabilities of its cyber forces and state-sponsored hacker groups.

Impact of Cyber Threats on India

Being the fifth largest economy, India’s rise digitally via platforms and services has been commendable. However, the nation faces sophisticated and persistent cyber threats from state-sponsored and non-state actors. Given that the nation’s cybersecurity policies and infrastructure are still evolving, it makes it easy for hackers to exploit the gaps and weaknesses in the system. Some of the notable challenges due to cyber-attacks in India are as follows -

- Data breach and privacy concerns regarding data on the internet - With increased digitisation and with more and more data being stored online on servers, hackers have been making efforts to access these databases and leaking them on public platforms where others can exploit them. This puts individuals and organisations both at risk hence securing personal data online is the biggest issue the enterprises and government face.
- Threat to Financial Institutions - The Indian banking industry is at great risk of cyberattacks from hackers looking to benefit from theft and extortion. Attacks against banks, financial institutions, and online payment systems have resulted in huge financial losses. The Indian Cybercrime Coordination Centre recently said that digital financial scams cost ₹1.25 lakh crore[31] in the past three years.
- Critical infrastructure vulnerability - Vital installations such as the power grids, lines of communications and transportation systems are at great risk of being compromised by hackers which will cause major disruptions and lead to even serious law and order situations too.
- Cyber Espionage - Cyber espionage is the use of cyberattacks to spy on or undermine the interests of other governments or organisations. Like other countries, India is a target for cyber espionage operations designed to acquire secret information and gain a strategic advantage. Cyber espionage may impact India's national security, foreign policy, and economic growth.
- Advanced Persistent Threats (APTs) - APTs are complicated and long-lasting cyber-attacks carried out by well-resourced and competent teams on a country or a particular cyber system. These assaults are intended to penetrate the target's network and remain concealed for an extended period of time, allowing them to steal, manipulate, or cause harm. APTs are difficult to identify and counter because they utilise sophisticated strategies and tools to circumvent security safeguards.

Recommendations

In the past few years, the Indian government has come up with a few measures that were crucial towards the goal of achieving a robust cyber defence mechanism.

- The Joint Doctrine for Cyberspace Operations released in June 2024 provides the blueprint for assisting senior leadership to take informed actions with carrying out cyber activities in the modern-day combat operational environment.[32] Yet, India is still lagging in delegating agencies to put in a centralised effort towards national cyber security[33]. More emphasis must also be placed on achieving offensive capabilities to disrupt adversarial network systems and deter future attacks. Agencies like the Defence Cyber Agency (DCyA) must be allocated more resources to arm it to the teeth by additionally strengthening the human and tech talent pool, steering Cyber Security Centres of Excellences (CyCoE) and streamlining a zero-trust ecosystem for addressing security issues and weaknesses.
- A nodal ministry needs to be appointed to coordinate all the efforts towards strengthening the national cyber security framework. Currently, all the agencies be it civil or military are more or less working in silos, therefore more emphasis must be laid on jointness and having clear-cut mandates for all of the agencies to reduce redundancies. An apex Cyber Security Board should be set up consisting of experts from PSUs and private players to address the issue and bring in the state-of-the-art technology to mitigate all the redundancies.
- The government should organise hackathons and actively seek for exceptional youngsters to be trained as cyber warriors. Establishing a strong network infrastructure also entails performing bug-hunting exercises across government agencies and ministries to find vulnerabilities and address them before they are taken advantage of by an outside party. Additionally, to empower hacker organisations to launch targeted attacks against adversarial network systems, the government should develop models in which they take over and support hacker groups operating within the nation.
- It is time that India should identify that cyber offence is just as important and necessary as cyber defence. Our current strategy seems to be more defensive and reactive hence, India must likewise invest in more aggressive cyber tools. Offensive cyber capabilities also need to be complimented by structural and policy reforms to clearly roles and areas of operations of various government

agencies along with a nodal ministry that is in charge and at the helm of all cyber-related operations and makes all policy-related decisions.

- Also, the government should start laying more emphasis on developing offensive capabilities to deter the Chinese and ensure that through cyber power projection regularly a loud and clear message is delivered that any action by them will lead to a response serious in nature. Additionally, it is imperative that we critically analyse our systems and identify the vulnerabilities that can be exploited by the Chinese army along with state-sponsored hacker groups.

Conclusion

The Chinese have been probing for weaknesses in India’s cyber networks for a long time. The attacks on power grids, ports, banks and other critical infrastructure should not be viewed in isolation as single incidents but should be perceived as a dry test run for something bigger in the future that can impale the country to a large extent.
The current world conflicts have demonstrated that cyber-attacks are a crucial tactic in the book of hybrid warfare as they enable the conventional forces to proceed with ease once the critical infrastructure is critically impacted and the lines of communication are down.

The attacks on Indian power grids in Ladakh may have been averted but the situation on borders is still volatile with both sides massing troops. With these recent reforms in the PLA SSF, India should be on high alert as the Chinese might be planning to launch a fresh wave of belligerent actions at the borders backed by the newly formed ISF causing serious financial losses along with disrupting economic activities. Data breaches and uploading of the compromised data on open platforms such as GitHub point towards serious threats that the ISF and state-sponsored hacker groups pose to India in the future.

Beijing currently believes that cyber weapons will remain its preferred weapon and that there is no real inherent risk that the Chinese state will face following a cyberattack or cyber espionage activity that would result in any serious retaliation. Cyber as a weapon is very cost-effective whereas a successful attack has severe implications on the victim nation which has compelled the PRC to invest more in these tools. Therefore, it is critical that India analyses the gaps in its strategy and identifies its gaps and vulnerabilities, rectifying them before the enemy attempts to exploit them causing serious disruption and chaos. The way forward is only through adopting adequate measures to equip our forces and agencies to fight this battle of the future.

DISCLAIMER

The paper is author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Endnotes

[1] Forward Defense Experts. 2022. "Today's Wars Are Fought in the 'Gray Zone.' Here's Everything You Need to Know about It." Atlantic Council. February 23, 2022. https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/.

[2] Greenwald, et al. 2017. "NSA Prism Program Taps into User Data of Apple, Google and Others." *The Guardian*, December 29, 2017. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[3] DESJARDINS, RICHARD. 2007. The Science of Military Strategy. EDITED BY PENG GUANGQIAN AND YAO YOUZHI. Beijing: Military Science Publishing House, 2005. 504 pp.

[4]"What Are China's Cyber Capabilities and Intentions?" n.d. Carnegieendowment.org. https://carnegieendowment.org/posts/2019/04/what-are-chinas-cyber-capabilities-and-intentions?lang=en.

[5] Bruzzese, Matt, and Peter W. Singer. 2024. "Farewell to China's Strategic Support Force. Let's Meet Its Replacements." Defense One. April 28, 2024. https://www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143/.

[6] Maizland, Lindsay. 2020. "China's Modernizing Military." Council on Foreign Relations. February 5, 2020. https://www.cfr.org/backgrounder/chinas-modernizing-military.

[7] "RIP, SSF: Unpacking the PLA's Latest Restructuring." n.d. Thediplomat.com. https://thediplomat.com/2024/04/rip-ssf-unpacking-the-plas-latest-restructuring/.

[8] Air University (AU). 2024. "The PLA's New Information Support Force." April 22, 2024. https://www.airuniversity.af.edu/CASI/Display/Article/3749754/the-plas-new-information-support-force/.

[9] "China Security Report 2022." 2022. NIDS. 2022. https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2022_A01.pdf.

[10] "Planned Obsolescence: The Strategic Support Force in Memoriam (2015-2024) - Jamestown." 2024. Jamestown. May 6, 2024. https://jamestown.org/program/planned-obsolescence-the-strategic-support-force-in-memoriam-2015-2024/.

[11] Costello, John, Joe McReynolds, Center for the Study of Chinese Military Affairs, Institute for National Strategic Studies, and China Cyber and Intelligence Studies Institute. 2018. "China's Strategic Support Force: A Force for a New Era." *China Strategic Perspectives*. Vol. No. 13. National Defense University

Press. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

[12] "A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force." 2024. Jamestown. April 26, 2024. https://jamestown.org/program/a-disturbance-in-the-force-the-reorganization-of-peoples-liberation-army-command-and-elimination-of-chinas-strategic-support-force/.

[13] "A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force." 2024. Jamestown. April 26, 2024. https://jamestown.org/program/a-disturbance-in-the-force-the-reorganization-of-peoples-liberation-army-command-and-elimination-of-chinas-strategic-support-force/.4

[14] DSCI, and Vinayak Godse. 2023. "India Cyber Security Domestic Market 2023." https://www.dsci.in/files/content/knowledge-centre/2023/India%20Cybersecurity%20Domestic%20Market%202023%20Report.pdf.

[15] Livemint. 2024. "Data Breaches at PMO and EPFO, In-Cert Officials Brought in to Probe Allegations." Mint. mint. February 21, 2024. https://www.livemint.com/news/india/data-breaches-at-pmo-and-epfo-in-cert-officials-brought-in-to-probe-allegations-11708500221463.html.

[16] Aryan, et al. 2024. "EPFO, PMO Data Breach: Centre Says Aware of Reports, Cert-In Looking Into Details." *The Economic Times*, February 21, 2024. https://economictimes.indiatimes.com/tech/technology/epfo-pmo-data-breach-centre-says-aware-of-reports-cert-in-looking-into-details/articleshow/107870171.cms?from=mdr.

[17] "The massive data leak from a Chinese cybersecurity agency, whose targets include India." 2024. The Indian Express. February 2024. https://indianexpress.com/article/explained/china-data-leak-surveillance-india-github-9175313/.

[18] "Chinese Hackers Targeted 7 Indian Power Hubs, Govt Says Ops Failed." 2022. Hindustan Times. April 8, 2022. https://www.hindustantimes.com/india-news/chinese-hackers-targeted-7-indian-power-hubs-govt-says-ops-failed-101649356540330.html.

[19] Mishra, Abhinandan. 2018. "Concerns Deepen About Cyber Attack on Su 30, IAF Starts Inquiry - the Sunday Guardian Live." The Sunday Guardian Live. April 25, 2018. https://sundayguardianlive.com/investigation/9670-concerns-deepen-about-cyber-attack-su-30-iaf-starts-inquiry.

[20] Goud, Naveen. 2017. "China Cyber Attacks Indian SUKHOI 30 Jet Fighters!" Cybersecurity Insiders. June 5, 2017. https://www.cybersecurity-insiders.com/china-cyber-attacks-indian-sukhoi-30-jet-fighters/.

[21] "Did Chinese Hackers Cause Mumbai's Power Failure in October?" n.d. The Wire. https://thewire.in/world/india-china-hackers-border-tension-power-grid-malware-recorded-future.

[22] "China hackers targeted power grids near Ladakh, says report." 2022. The Indian Express. April 8, 2022. https://indianexpress.com/article/india/chinese-hackers-electricity-distribution-centres-ladakh-minister-rk-singh-7858001/.

[23] Staff, Scroll. 2021. "Chinese Hackers Still Targeting One Indian Port, Says US Cyber Security Firm: Bloomberg." Scroll.in. March 3, 2021. https://scroll.in/latest/988464/chinese-hackers-still-targeting-one-indian-port-says-us-cyber-security-firm-bloomberg.

[24] M, Sarvesh. 2024. "China State-backed Hacking Groups Reportedly Targeted India and Other Countries; Here'S What We Don'T Know." MEDIANAMA. February 23, 2024. https://www.medianama.com/2024/02/223-china-state-backed-hacking-groups-india/.

[25] George, P.J. 2021. "Explained | Red Echo, ShadowPad, and the Targeting of India's Power Grid." The Hindu. March 7, 2021. https://www.thehindu.com/sci-tech/technology/red-echo-over-india/article34008299.ece.

[26] Starks, Tim. 2021. “Suspected Chinese Hackers Masqueraded as Indian Government to Send COVID-19 Phishing Emails.” *CyberScoop*, October 5, 2021. https://cyberscoop.com/apt41-india-blackberry-china/.

[27] Sharma, Ankur. 2021. “China Aggressively Trying to Hack Indian Cyberspace.” *Rediff*, March 3, 2021. https://www.rediff.com/news/report/china-aggressively-trying-to-hack-indian-cyberspace/20210303.htm.

[28] CYFIRMA. 2020. “INDIA THREAT LANDSCAPE REPORT 2020.” https://www.cyfirma.com/media/2020/11/India-Threat-Landscape-Report_14-Oct-2020-compressed-1.pdf.

[29] “Beyond Cyber Fires and Ukraine: PLASSF Impact on a Sino-Indian Conventional War.” n.d. Orfonline.org. https://www.orfonline.org/research/beyond-cyber-fires-and-ukraine.

[30] Goujard, Clothilde. 2023. “EU Warns China on Ukraine Disinformation and Cyberattacks.” *POLITICO*, September 19, 2023. https://www.politico.eu/article/european-union-china-ukraine-disinformation-cyberattacks-war-russia/.

[31] Reddy, Bharat. 2024. “Digital Financial Frauds in India: A Call for Improved Investigation Strategies.” The Hindu. March 25, 2024. https://www.thehindu.com/sci-tech/technology/digital-financial-frauds-in-india-a-call-for-improved-investigation-strategies/article67988607.ece#:~:text=A%20recent%20report%20by%20the,over%20the%20last%20three%20years.

[32] “CDS Gen Anil Chauhan Releases Joint Doctrine for Cyberspace Operations.” n.d. https://pib.gov.in/PressReleaseIframePage.aspx?

[33] Ciso, Et. 2024. “Legal Gaps and Concerns Abound as Cybercrime Rises Unabated in India.” *ETCISO.In*, January 1, 2024. https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/legal-gaps-and-concerns-abound-as-cybercrime-rises-unabated-in-india/106434980.