Journal of Contemporary Politics

ORIGINAL ARTICLE

Securing India's Space Assets: Navigating Non-Traditional Challenges in the Cyber Era

S S Adwaith[1], Ashika S Prasad[1*]

[1]*Research Scholar, Department of Political Science, University of Kerala, Kerala, India*

ARTICLE INFO

Article history:
Received 26-11-2025
Accepted 06-01-2026
Published 31-03-2026

* *Corresponding author.*
Ashika S Prasad
ashikasprasad@keralauniversity.ac.in

https://doi.org/10.53989/jcp.v5i1.25.111

ABSTRACT

The intensity, frequency and scale of cyber-attacks define the warfare of the 21st century, and this has triggered a series of economic, political and social adjustments from the local to the international arena. Cyber-attacks are an emerging threat to space security. With the growing reliance on automation, there is a high risk of external agencies interfering with the operation of the satellite, cutting off the communication system and trying to obtain confidential data from the satellite. This paper seeks to identify cyber threats to space assets and analyse their implications for India's security, applying a realist perspective and focusing on China's rise as a space-cyber power.

Keywords: Space Assets, Cyber Security, Space Security, India, China

INTRODUCTION

The 21st century is witnessing outer space as a theatre of competition as more nations and private players have established their stake in exploring outer space. A nation's dependence on its space assets for various purposes makes it a potentially attractive target for adversaries. Satellites are vital components across sectors such as telecommunications, navigation, resource mapping, weather forecasting, military applications, and research activities. Consequently, they are the prime targets for malicious actors aiming to disrupt operations, steal data, or obtain unauthorised access. The core concern revolves around the transmission of information across space infrastructures, mainly as the sector evolves from a space infrastructure economy to a space data economy. Safeguarding space infrastructures and data against cyber-attacks is now more critical than ever, given the integration of space applications into our daily lives and the imperative for the sustainable utilisation of outer space. This paper focuses on a specific dimension of space security: cyber threats as distinct from kinetic threats.

Ear et al., (2023) put forward an analysis of 72 cyber-attacks, which were categorised into 8 distinct groups. These included 25 instances of jamming, 17 incidents of Computer Network Exploitation (CNE), 16 cases of hijacking, 4 control-related incidents, 3 Denial-of-Service (DoS) attacks, 3 incidents of eavesdropping, 1 incident of theft-loss, and 3 incidents of spoofing. Additionally, the analysis revealed that a significant majority, 71% of the attacks, were attributed to three interrelated categories:

political motivations, state espionage, and criminal activities[1].

Incidents over the years demonstrate the vulnerability of space assets to cyber aggression and the difficulty of attributing such attacks. As early as late 1998, the failure of the joint U.S.-German-U.K. X-ray satellite, known as Röntgensatellit (RoSat), raised suspicions of deliberate sabotage by Russian hackers. Even though concrete evidence is lacking, it is confirmed that a cyber-intrusion occurred in the servers of NASA's Goddard Space Flight Centre around the same time as the damage to RoSat[2]. This incident highlights the potential vulnerability of space assets to cyber threats and the challenges in attributing such attacks to specific actors.

More recently, during the Russia-Ukraine war, in late February 2022, a cyber attack targeted Viasat's KA-SAT network, which remains the most prominent cyber-attack publicly acknowledged since Russia's invasion of Ukraine. U.S. Secretary of State Antony Blinken stated that the cyber-attack aimed to disrupt Ukrainian command and control during the invasion, with repercussions extending to other European countries[3].

These cases reveal a deeper pattern: cyber threats to space systems are no longer isolated incidents but systematic operations aligned with state strategy. China exemplifies this strategic integration. Unlike the U.S.-Soviet space competition, which remained separated from cyber operations, China has deliberately consolidated cyber and space capabilities through its various doctrines. For India, this is strategically significant because China has institutionalised cyberspace integration, while India's institutions remain separate. This institutional asymmetry creates a structural vulnerability that cannot be solved by technological fixes alone.

This study adopts a qualitative, exploratory approach based on open-source research and case analysis. The research draws on a range of secondary sources, including academic literature, government and industry reports, news articles, and technical studies, to identify and examine the cybersecurity threats to space assets. Through this literature-driven analysis, the paper applies a realist lens, focusing on state-centric security concerns to interpret how cyber threats to space systems create strategic challenges. Given the sensitivity of cyber operations in space, available information has limitations. Much of the data on cyber threats and incidents, especially regarding Chinese activities, comes from U.S. or allied governmental and corporate sources, and these accounts are often incomplete or prone to bias. Given these constraints, this paper adopts a structured analytical approach: (1) it characterises cyber threats to space systems technically (ground, space, and link segments); (2) it examines China's doctrinal approach to cyber-space integration through official documents and strategic studies; (3) it maps India's institutional response capacity and identifies gaps. The analysis applies neorealist theory to interpret state behaviour, treating space-cyber security as a state-centric strategic challenge.

CONCEPTUAL FRAMEWORK

In international politics, security can be interpreted differently depending on the perspective. For some, the absence of warfare may be considered a form of security, while others may view interdependence and integration as elements of security[4]. From a realist perspective, security often revolves around military capabilities relative to other actors, having sufficient deterrence capabilities, and forming alliances to balance power or threats.

The prevailing notion of security predominantly revolves around national or international security, where the state is the prominent actor and the primary focus is on the use of force, with external threats being the main concern[5]. Technological advancements in the 21st century, particularly in Information and Communication Technology (ICT), have facilitated the emergence of cyber-warfare and cyber-espionage, leading to a gradual shift of the battlefield from traditional domains like land, air, and sea to cyberspace[6].

The advent of cyberspace has forced economic, social, and political adjustments globally. It has re-elevated security as a key factor in statecraft: we stand on the threshold of what some call a 'cybered conflict' era, where warfare may be ambiguous, covert, prolonged, and involve surprise cyber-attacks on unprecedented scales and targets[7]. Identifying when such conflicts begin or end, who is behind them, and what their motives are can be extremely difficult. Adversaries might exploit cyberspace to weaken an opponent's society and critical systems long before overt hostilities.

Outer space has similarly become integral to national security. Space systems are now critical infrastructure for activities like disaster response, navigation, and military operations[8, 9]. The digitisation of space systems, the increasing relevance and criticality of space systems in military operations, and the growing integration of satellites into the digital infrastructure make them more vulnerable to cyber threats.

The integration of cyber and space vulnerabilities creates a new strategic challenge that traditional security theories partially miss. Space systems were historically protected by isolation, and satellites operated in controlled environments, difficult to access remotely. However, digitisation has collapsed this isolation. Modern satellites rely on digital command systems, networked ground

stations, and encrypted communications, all vulnerable to cyber exploitation. This convergence means an attacker no longer needs kinetic weapons (ASAT missiles) to disable satellites; remote cyber operations achieve the same effect. For strategic analysis, this matters because traditional deterrence theory (based on kinetic capabilities) becomes insufficient. A state with superior cyber capabilities but weaker kinetic ASAT weapons may achieve greater strategic effect than a state with advanced ASAT weapons but poor cyber defences.

No theory of international politics emphasises security more than neorealism, which posits that the quest for security (and ultimately survival) drives state behaviour[10]. Kenneth Waltz's neorealist framework identifies three mechanisms through which states enhance security: (1) internal balancing- developing military capabilities to offset adversary advantages; (2) external balancing- forming alliances to collectively deter threats; (3) strategic positioning- exploiting geographic, technological, or diplomatic advantages to shift relative power[11].

The space-cyber domain exhibits a particularly acute security dilemma. A state that develops cyber-capabilities to defend its space infrastructure (defensive intent) appears to be developing offensive cyber-warfare capabilities against adversaries. Conversely, another state's development of space-cyber offensive capabilities appears threatening to neighbours. This dynamic is more pronounced in space-cyber than terrestrial domains because: (1) cyber-attacks are covert and difficult to attribute, creating ambiguity about intent; (2) space-cyber capabilities are dual-use- serving civilian, commercial, and military purposes simultaneously, making pure 'defensive' development difficult to verify; (3) international norms for space-cyber conduct are weak or absent, unlike nuclear or chemical weapons regimes. Applying Waltz's neorealist framework, China's space-cyber integration represents an internal balancing move that triggers a security dilemma for India.

CYBER THREATS TO SPACE ASSETS

Understanding the technical landscape of cyber threats to space systems is essential for analysing why China's strategic integration of these capabilities poses particular challenges for India. Space vulnerabilities fall across three interconnected segments: the physical satellites, ground control infrastructure, and communication links between them. An attacker exploiting vulnerabilities in any segment can cascade effects across the entire system.

Each segment is vulnerable to different kinds of attack. The space segment includes the satellite's structure, its control and communication subsystems, and any mission-specific payloads (e.g. remote sensing instruments or military sensors). The ground segment involves facilities like control stations that monitor satellite health, send commands, and receive the satellite's data. Communication links connect everything: uplinks (signals sent from ground to satellite), downlinks (satellite to ground), crosslinks (satellite to satellite), and telemetry, tracking & command (TT&C) links that control the satellite's operations[12].

Threats to space assets or counter-space measures can be broadly classified into offensive and defensive. Defensive counter-space measures are implemented to protect one's own space assets from potential attacks. Offensive capabilities, however, possess a wide range of functions, enabling them to deceive, disrupt, deny, degrade, or destroy any component of a space system, be it satellites, ground systems, or communication links between them[13]. Kinetic anti-satellite (ASAT) weapons are offensive weapons capable of either destroying spacecraft outright or significantly impairing their ability to carry out their missions[14].

Non-kinetic methods of attack are also highly effective. These may include jamming uplinks and downlinks, using lasers to dazzle or partially blind sensors, and launching attacks with high-powered microwaves. Additionally, there's the deployment of radio frequency (RF) jamming equipment capable of interfering with space system links, along with laser systems intended to temporarily or permanently degrade or destroy satellite subsystems, thus impacting satellite mission performance. Moreover, electromagnetic pulse weapons are highlighted for their ability to degrade or destroy satellite and ground system electronics[15].

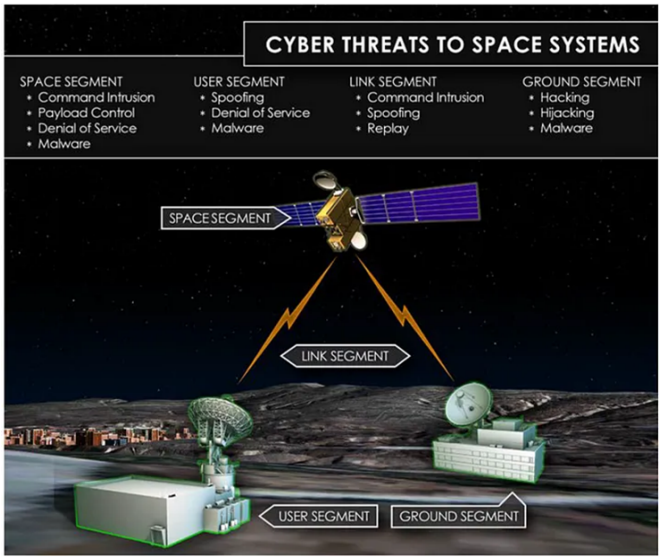

Fig. 1: Cyber threats to space systems. (*Source: National Air, Space, and Intelligence Centre (NASIC)*)

In the past, the majority of space infrastructure operated with custom fixed-function hardware and software, which reduced the possibilities for potential cyber-attacks. However, modern satellites increasingly incorporate off-the-shelf, programmable hardware and software components. As a result, they are now more prone to cyber-attacks than any other kind of kinetic or non-kinetic attacks. The term 'Cyber ASAT' is frequently used to underscore the escalating threat posed by cyber-attacks targeting space systems. Unlike traditional kinetic ASAT weapons that physically destroy satellites, Cyber ASAT operations leverage cyber capabilities to disrupt or manipulate satellite operations. The interconnected nature of civilian, military, and strategic systems amplifies the impact of such attacks, potentially disrupting communication, navigation, and military operations[16].

Numerous open-source reports indicate that nation-states and other entities are actively engaging in cyber intrusions targeting government spacecraft assets. Government assets are not the sole focus of such attacks; considering the military's dependence on commercial satellites to enhance bandwidth, cyber-attacks on commercial space systems also pose a significant concern[17].

Cyber-Attacks to Ground Segment:

Ground control stations are prime targets for cyber-attacks. The vulnerabilities present in ground systems or satellite data receivers can provide attackers with the opportunity to infiltrate the ground network and operate undetected. By compromising ground control stations, attackers could potentially manipulate satellite trajectories, disrupt communication links, or even cause physical damage to satellites, thereby posing significant risks to national security, communication systems, and other critical infrastructure reliant on space[18]. Ground segment cyber threats encompass a variety of malicious activities targeting ground systems and infrastructures supporting space operations, as well as user applications and interactions. These threats include cyber-attacks and intrusions aimed at exploiting misconfigurations and software vulnerabilities to gain unauthorised access to critical systems and networks. Malware injection into systems controlling space operations, as well as satellite data receivers and transmitters, poses a significant risk[19]. Phishing attacks are employed to obtain sensitive credentials, while the introduction of malware through the supply chain of ground station system components further exacerbates security concerns. This form of compromise can subsequently affect ground systems, posing risks at a later stage of operations. Physical attacks on ground station infrastructures add another layer of vulnerability, highlighting the multifaceted nature of cybersecurity challenges faced by the ground segment of space operations[20].

Cyber-Attacks to Space Segment:

Access to a satellite's controls presents a significant risk, as it could allow an attacker to inflict damage or potentially wreck the satellite. The attacker could exploit this access to deny, degrade, or manipulate the satellite's transmission, disrupting its intended functions. Additionally, gaining high-level access could provide the attacker with insights into the satellite's capabilities or other sensitive information, further exacerbating the security threat[21]. Adversaries use space situational awareness to detect the presence, location, and identity of satellites, enabling them to track and target attacks to deny strategic capabilities. This includes employing electromagnetic pulse actuators or radio frequency transmitters for jamming and spoofing attacks. For instance, attackers may use electromagnetic pulse actuators to cause failures in victim satellites or deploy radio frequency transmitters to disrupt communications or deceive satellite sensors. Additionally, adversaries may exploit any technology that facilitates a close approach to inspect and repair satellites for conducting attacks, potentially resulting in temporary or permanent damage to the targeted satellite[19]. The exploitation of software and hardware vulnerabilities in space assets is a prevalent threat, which could involve giving bad instructions to manipulate basic controls or maliciously controlling payload systems to execute denial of service attacks and overload systems[22]. Attackers may also introduce malware into satellite system components via the supply chain, compromising the integrity and functionality of space assets. Satellite hijacking, wherein attackers alter legitimate signals to repurpose satellites for alternative purposes, is another concerning cyber threat. Adversaries may exploit surveillance satellites to monitor and track military and other sensitive activities on Earth. Lastly, physical attacks against space assets, such as using space-based robotic arm technology for grappling with other satellites, further underscore the multifaceted nature of space segment cyber threats.

Cyber-Attacks on the Link Segment:

Link segment cyber threats encompass a range of adversarial tactics aimed at disrupting, denying, deceiving, or degrading space communications and services. Adversaries conduct attacks such as jamming to prevent users and other space assets from receiving intended signals. For instance, uplink jamming (orbital jamming), directed toward the satellite, impairs services for all users in the satellite reception area, while downlink jamming (terrestrial jamming), targeted at ground users, has a localised effect[23].

Orbital jamming disrupts the signal transmitted from a ground station to a satellite. The jamming device does not need to be in close proximity to the transmitter but can be

positioned anywhere within the satellite's receiving beam. This means that for certain types of satellites, the jamming device could be located anywhere within the satellite's coverage area on Earth, often referred to as its 'footprint.' The jamming signal effectively degrades the quality of the desired signal received by the satellite[24]. Spoofing is another tactic used to deceive the receiver by introducing a fake signal with erroneous information. However, attributing such attacks and distinguishing them from unintentional interferences can be challenging due to their sophisticated nature. Additionally, adversaries may engage in eavesdropping on satellite communications, particularly if the traffic is not encrypted[19]. This underscores the complexity and significance of link segment cyber threats in space cybersecurity.

CHINA'S CYBER AND COUNTERSPACE CAPABILITIES

China's military-strategic thinkers have increasingly emphasised cyberspace and outer space as critical domains of national power. The People's Liberation Army (PLA) first articulated a comprehensive cyber warfare doctrine in the 2013 edition of The Science of Military Strategy, an authoritative text by the PLA's Academy of Military Science. This document recognised cyberspace as a crucial domain of modern military struggle. Similarly, China's 2015 defence white paper (China's Military Strategy) explicitly discussed cybersecurity for the first time, calling cyberspace a new 'pillar' of economic and social development and a national security realm. Chinese analysts often equate the importance of cyber warfare in the information age with that of nuclear warfare in the 20th century, underscoring how decisive cyber operations could be in future conflicts[25].

By 2014, China initiated changes to its military policy to prepare for offensive cyber operations in combat. The 2013 edition of *The Science of Military Strategy* proposed strategies for achieving dominance in space and cyberspace. As early as 2012, it seems that China began deploying offensive cyber capabilities against political adversaries beyond its borders through targeted campaigns aimed at influencing and exploiting international social media platforms for propaganda[26].

The Guidelines on Joint Operations of the Chinese People's Liberation Army, adopted in 2020, emphasise the importance of modern warfare. The emergence of new technologies and battle domains necessitated the development of new types of joint campaigns, such as "Joint Cyber Campaigns" and those in the electro-magnetic spectrum[27]. The new guidelines highlight the significance of cyber and outer space domains.

The space-cyber nexus involves exploring both space and cyber domains bidirectionally, ensuring cybersecurity for space-based infrastructure and addressing space safety and security affected by cyber-driven spacecraft. China anticipates future trends in satellite constellations to emphasise the effective integration of various space-based functions. An example is the PNTRC (positioning, navigation, timing, remote sensing, and communication) satellite system, comprising numerous high-resolution remote sensing satellites, BeiDou navigation satellites, space-based satellite communication networks, and ground-based fifth- and sixth-generation mobile network and Wi-Fi technologies[28]. By developing the next generation of such systems, China aims to take a leading role in promoting the concept of "Internet+Space"[29].

China recognises the shift towards information technology-based warfare and the importance of integrated military combat operations. China's Strategic Support Force (SSF), established in 2015, consolidates space, electronic warfare, cyber, and psychological warfare capabilities to adapt to the evolving landscape of information technology-based warfare. The SSF's space component is primarily responsible for satellite launch and operations, enabling crucial functions like command and control, communications, and intelligence gathering. This force plays a pivotal role in China's strategic deterrence efforts, integrating capabilities across nuclear, conventional, space, counterspace, and cyber warfare. With its advanced C4ISR capabilities, the SSF facilitates joint operations and "system vs. system" warfare tactics, crucial in modern conflict scenarios[30, 31].

China also recognises the importance of joint military-civilian efforts in establishing an integrated space-to-Earth cyberspace infrastructure. Spacecraft launchers and platforms operate as cyber-physical systems, heavily reliant on secure cyber operations for their design and functioning. China closely monitors developments in cyber threats in space, particularly highlighted by cyber operations during the Russia-Ukraine crisis in 2022. These incidents underscore the pervasive, mature, and severe nature of cyber means in the space domain during military conflicts[28].

China's challenges to US and European security extend across various sectors, including reinterpretations of international law, subversion of liberal market economic practices, and cyber insurgencies targeting civilian and military entities. Asian allies face a dilemma similar to Europe regarding how closely to align with the US in countering Chinese threats. Cooperation with the US raises concerns about abandonment versus entrapment, particularly evident in US-China space and naval competition, where modern Chinese weapons undermine

US deterrence[32]. Australia plays a central role in the evolving US space and naval security agenda, expanding its capacity for communication and intelligence in outer space and integrating its space activity with US systems to deter potential adversaries. However, this integration also exposes Australia to threats such as advanced cyberattacks against jointly operated satellites[33]. Between 2016 and 2018, approximately 200 predominantly aerospace-related companies and research institutions, including the Japan Aerospace Exploration Agency, were subjected to significant cyberattacks believed to be associated with the Chinese military[34].

On the normative front, China's participation in international cyber- and space-governance forums remains limited. Although China is a member of many multilateral bodies, its transparency, commitment to rules-based behaviour and willingness to support binding norms in outer-space or cyberspace remain weak. This normative gap allows China to exploit dual-use technologies and grey-zone tactics with fewer normative constraints[35]. China is increasingly integrating artificial intelligence into satellite intelligence analysis and cyber-space workflows[36]. The combination of space-based sensors, automated data processing and cyber exploitation capability reduces decision-latency and strengthens China's ability to act rapidly in contested domains. Although detailed open-source documentation of PLA joint cyber-space drills is rare, think-tank reports note increased emphasis on integrated training of cyber, electronic warfare and space units, hinting at a doctrinal shift towards cross-domain operations[13, 37].

IMPLICATIONS FOR INDIA

China's aggressive pursuit of space weaponisation poses a significant challenge to India as it transforms space into another battleground. China could leverage its advanced cyber capabilities to target Indian space assets, denying New Delhi critical data acquired or received by its satellites and potentially conducting kinetic attacks to destroy them. India's national security space narrative is shaped by two key factors: the expanding infrastructure of China's space program and Pakistan's missile capability. These developments have tactical implications for India's border areas and underscore the need for robust defences and strategic responses to safeguard its space assets and national security interests[38].

China has heavily invested in and surpassed India in most domains controlled by the SSF. Over the past three decades, China has made significant strides in its space programs, achieving milestones such as launching an operational global satellite navigation system and nearly completing the Chinese Space Station. China has also been extensively involved in hacking computers and collecting personal data worldwide, leveraging successful hacking attempts to amass vast amounts of data for applications, particularly when combined with artificial intelligence. China's history of meddling with Indian servers dates back to at least 2008, when Chinese hackers attempted to breach servers belonging to the National Informatics Centre, the National Security Council, and the Ministry of External Affairs. One critical gap between the capabilities of the two Asian giants lies in India's lack of offensive systems. Since the Galwan Valley clash and subsequent stand-off along the Line of Actual Control (LAC), the number of cyber threats originating from China has only increased.

According to a report by the Singapore-based cybersecurity firm Cyfirma, there was a 200% surge in cyberattacks from China between May and June 2020. China's substantial intelligence, surveillance, and reconnaissance (ISR) capacity in border conflicts with India has driven India to advance its ISR capabilities and bolster command and control (C2) systems[7, 38, 39].

In a 2011 report by the US-China Economic and Security Review Commission, several attempts were revealed to breach a US Geological Survey Earth-imaging satellite, Landsat-7, and NASA climate change sensors, Terra AM-1. Though no damage occurred, cybercriminals could complete all steps necessary to command the satellites[24]. Similarly, a 2014 paper by IOActive, a US-based cybersecurity firm, reported vulnerabilities in existing satellite communication terminals used across commercial, government, and military operations, highlighting multiple potential hacker entry points. The report also indicated China's People's Liberation Army (PLA) continued to develop technologies aimed at 'blinding and deafening the enemy', including the capability to conduct cyberattacks on ground stations to control satellites. These revelations coincide with the 2020 standoff between India and China at the Line of Actual Control (LAC), with Indian security officials expressing a need for dedicated satellites to monitor Chinese activities. According to the US-based China Aerospace Studies Institute (CASI), China conducted numerous cyberattacks between 2007 and 2018, including attacks against Indian satellite communications in 2017. Despite acknowledging cyber-attacks, ISRO maintained that none of its systems were compromised. The report also highlighted China's counter-space technologies targeting space systems from geosynchronous orbit (GEO). Chinese hackers targeted power grids in northern India, particularly in proximity to the disputed India-China border in Ladakh, as reported by Secureworks, a US-based private cybersecurity firm[40, 41].

The significance of China's cyberspace integration lies not in individual capabilities but in their operational synthesis. China's Strategic Support Force creates 'cross-domain

synergy', cyber operations enhance space operations and vice versa. A cyber-attack on an Indian satellite ground station coincides with the jamming of uplinks, disabling multiple satellite functions simultaneously. This requires adversaries to defend across multiple domains with integrated responses. India's current institutional structure, with ISRO managing satellites independently and NCCC handling cyber separately, cannot generate equivalent cross-domain responses. More critically, China's doctrinal clarity (published guidelines, explicit strategic vision) creates strategic predictability. India's doctrinal silence, the 2023 Space Policy omits cyber security entirely, creates the opposite effect: ambiguity invites probing. For India, matching China's doctrinal clarity is as important as matching its technical capabilities.

India has made some initial strides: it established a tri-service Defence Space Agency in 2019 and conducted its own demonstration of ASAT capability (Mission Shakti) in 2019 to signal deterrence. On the cyber side, institutions such as the National Cyber Coordination Centre (NCCC) under the Ministry of Electronics and IT and the Indian Computer Emergency Response Team (CERT-In) have been working to improve national cybersecurity readiness. The NCCC provides real-time situational awareness of cyber threats and coordinates information sharing, while CERT-In handles incident response for cyber attacks and threats like hacking and phishing.

However, significant gaps remain. Notably, India's current draft National Cyber Security Strategy (formulated by the Data Security Council of India) does not explicitly address the protection of space infrastructure. This omission is critical: as India's space assets become more crucial to both civilian life and military operations, failing to plan for their cybersecurity leaves a door open for adversaries. Despite advanced space capabilities, India faces a structural asymmetry relative to China. First, institutional fragmentation: space operations are civilian (ISRO), cybersecurity is multi-agency (NCCC, CERT-In), and military space coordination is nascent (the Defence Space Agency was created only in 2019). When cyberattacks target satellites, no unified command structure coordinates response. China's Strategic Support Force consolidates all these functions under a single authority. Second, technical legacy: older ISRO satellites use legacy protocols vulnerable to spoofing and jamming. Unlike modern systems with encryption and intrusion detection, retrofitting orbital systems designed for 10-15 year lifespans is infeasible. A 2014 IOActive study documented zero-day vulnerabilities in Indian satellite communication terminals, persistent entry points for attacks. Third, doctrinal silence: China's 2015 and 2020 doctrinal statements articulate an explicit space-cyber integration doctrine. India's 2023 Space Policy emphasises commercialisation but contains no space cybersecurity provisions. This doctrinal gap signals neither strategic clarity nor deterrence intent. These three asymmetries reflect India's temporal disadvantage: China consolidated cyber-space integration in 2013-2015; India began in 2019. This 'second-mover disadvantage' is structural. Without institutional integration, India remains vulnerable despite technical competence.

Traditional cybersecurity measures, like IT network firewalls or access controls on terrestrial systems, may not be fully sufficient for satellites and space networks, which have unique constraints (latency, difficult-to-patch hardware in orbit, etc.). Space assets often have a higher threshold for failures or attacks, given the difficulty of repair and the outsized consequences (losing a satellite could cripple communications or intelligence over a large area). Thus, India's approach needs to be more specialised and proactive when it comes to space cybersecurity.

CONCLUSION

This paper has addressed four key issues. First, cyber-attacks have demonstrably become a defining feature of 21st century security competition. The evidence- 72 documented space system attacks[8], the RoSat incident, the Viasat attack, and the 2017 attacks on Indian satellite communications- confirms that cyber operations are no longer peripheral to warfare but central to it. Second, the technological shift from traditional domains to cyberspace is complete. Space systems, previously isolated from cyber threats, are now digitised, networked, and vulnerable to remote exploitation. Third, China's rise as an integrated space-cyber power is documented through its Strategic Support Force consolidation, 2015 and 2020 doctrinal statements, and operational demonstrations against allied aerospace targets. This rise creates acute implications for India. Fourth, automation and digital integration in satellites create systemic vulnerability- legacy satellites cannot be patched, ground stations rely on networked protocols, and command-and-control systems depend on digital infrastructure.

For India specifically, three implications follow: (1) Institutional fragmentation- space under ISRO, cyber under NCCC/CERT-In, military coordination under Defence Space Agency- creates coordination failures when attacks occur. China's unified Strategic Support Force has no Indian equivalent. (2) Technical vulnerability- older ISRO satellites lack cyber defences, ground stations use vulnerable protocols, and there is no integrated space cybersecurity strategy despite the 2023 Space Policy. (3) Temporal asymmetry- China began integrating cyberspace capabilities in 2013; India only created the Defence Space Agency in 2019. This creates a second-mover disadvantage.

These vulnerabilities are not theoretical. They manifest in documented attacks: 2008 breaches of Indian government

servers, 2017 cyberattacks on Indian satellite communications, and 2020 Ladakh crisis cyber escalations. India must address them through two responses: First, integrate space and cyber command structures under the Defence Space Agency authority, formalising coordination protocols between ISRO and military cyber commands. Second, prioritise cyber-hardening of critical satellites (navigation, communications, reconnaissance) through retrofitting where possible and designing new systems with cyber-resilience as an architectural requirement.

Without these changes, India faces escalating risk. China's doctrine explicitly targets space-cyber integration; India's strategy remains silent on it. As India's dependency on space infrastructure deepens- navigation, communications, military operations- the stakes increase. Securing India's space assets against cyber threats is not optional; it is a prerequisite for strategic autonomy.

REFERENCES

1. Ear E, Remy JLC, Feffer A, Xu S. Characterizing Cyber Attacks against Space Systems with Missing Data: Framework and Case Study. *2023 IEEE Conference on Communications and Network Security (CNS)*. 2023; :1-9 . Available from: https://doi.org/10.1109/cns59707.2023.10289045
2. Wess M. (2021, February 1). *ASAT Goes Cyber*. U.S. Naval Institute. https://www.usni.org/magazines/proceedings/2021/february/asat-goes-cyber
3. Pearson J. (2022). Russia downed satellite internet in Ukraine -Western officials. *Reuters*. https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10/
4. Bhattacharya S. (2016). Explaining the Conceptualisation of Security in Mainstream International Relations Theory. *The Indian Journal of Political Science*, 77(1), 77–84. https://www.jstor.org/stable/26575669
5. Attinà F. Traditional Security Issues. *China, the European Union, and the International Politics of Global Governance*. 2016; :175-193 . Available from: https://doi.org/10.1057/9781137514004_10
6. Srikanth D. (2014). Non-Traditional Security Threats In The 21st Century: A Review. *International Journal of Development and Conflict*, 4, 60–68.
7. Kremer JF, Müller B. Cyberspace and International Relations: Theory, Prospects and Challenges. 2014; . Available from: https://doi.org/10.1007/978-3-642-37481-4
8. Rajagopalan RP. (2019). *Electronic and Cyber Warfare in Outer Space*. https://unidir.org/publication/electronic-and-cyber-warfare-in-outer-space/
9. CCSDS. (2022). *Security Threats Against Space Missions*. https://ccsds.org/Pubs/350x1g3.pdf
10. Baldwin DA. The concept of security. *Review of International Studies*. 1997; 23 (1) :5-26 . Available from: https://doi.org/10.1017/s0260210597000053
11. Waltz KN. (1997). *Theory of international politics (Reiss)*. Waveland Press
12. Khan SK, Shiwakoti N, Diro A, Molla A, Gondal I, Warren M. Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions. *International Journal of Critical Infrastructure Protection*. 2024; 47 :100724 . Available from: https://doi.org/10.1016/j.ijcip.2024.100724
13. Shabbir Z, Sarosh A. Counterspace Operations and Nascent Space Powers. *Astropolitics*. 2018; 16 (2) :119-140 . Available from: https://doi.org/10.1080/14777622.2018.1486792
14. Partlow RG. (2010). *Space System Vulnerabilities and Defenses [Air Command and Staff College, Air University]*. https://apps.dtic.mil/sti/pdfs/AD1019732.pdf
15. Yates H, Grimaila MR. (2008). *A Systematic Approach for Securing our Space Assets. Faculty Publications*. https://scholar.afit.edu/facpub/160
16. Khan A. (2020, August 1). *Cyber ASAT-Capabilities and South Asia. Modern Diplomacy*. https://moderndiplomacy.eu/2020/08/01/cyber-asat-capabilities-and-south-asia/
17. Bailey B, Speelman RJ, Doshi PA, Cohen NC, Wheeler WA. (2019). Defending Spacecraft in the Cyber Domain. *The Centre for Space Policy and Strategy, The Aerospace Corporation*. https://aerospace.org/sites/default/files/201911/Bailey_DefendingSpacecraft_11052019.pdf
18. Nichols PRK, Carter CM, Ii JVD, Farcot M, Hood CJP, Jackson DMJ, *et al.* (2023). *Cyber-Human Systems, Space Technologies, and Threats*. New Prairie Press.
19. Varadharajan V, Suri N. Security challenges when space merges with cyberspace. *Space Policy*. 2024; 67 :101600 . Available from: https://doi.org/10.1016/j.spacepol.2023.101600
20. Li D. Cyber-attacks on Space Activities: Revisiting the Responsibility Regime of Article VI of the Outer Space Treaty. *Space Policy*. 2023; 63 :101522 . Available from: https://doi.org/10.1016/j.spacepol.2022.101522
21. Robinson J. (2016). The Space Review: Governance challenges at the intersection of space and cyber security. The Space Review. https://www.thespacereview.com/article/2923/1
22. Martin AS. Outer Space, the Final Frontier of Cyberspace: Regulating Cybersecurity Issues in Two Interwoven Domains. *Astropolitics*. 2023; 21 (1) :1-22 . Available from: https://doi.org/10.1080/14777622.2023.2195101
23. King M, Goguichvili S. (2020). *Cybersecurity Threats in Space: A Roadmap for Future Policy*. Wilson Centre. https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy
24. Livingstone D, Lewis P. (2016). *Space, the Final Frontier for Cybersecurity?* The Royal Institute of International Affairs, Chatham House. https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf
25. Jinghua L. (2019, March 22). *What Are China's Cyber Capabilities and Intentions?* International Peace Institute. https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/
26. The International Institute for Strategic Studies. (2022). *China's Cyber Influencing and Interference*. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2022/02/great-power-offensive-cyber-campaigns_04-china.pdf
27. Finkelstein DM. (2021). *The PLA's New Joint Doctrine: The Capstone of the New Era Operations Regulations System*. CNA. https://www.cna.org/reports/2021/09/The-PLAs-New-Joint-Doctrine.pdf
28. Yuan Y. (2023, January 29). Chinese Thinking on the Space-Cyber Nexus. *Centre for International Governance Innovation*.
29. Yu J. (2020). *Satellite Internet, bringing the 'Base Station' to Space (New Technology, New Progress)*. People.Cn. http://scitech.people.com.cn/n1/2020/0810/c1007-31815964.html.
30. Chopra A. (2021). People's Liberation Army Stratgic Support Force: Implications and Options for India. *Air Power*, 16(3). https://capsindia.org/wp-content/uploads/2022/01/Anil-Chopra.pdf
31. Pollpeter K, Chase M, Heginbotham E. (2017). *The creation of the PLA Strategic Support Force and its implications for Chinese military space operations*. RAND Corporation.
32. Levite A, Jinghua L, Perkovich G, Chuanying L, Manshu X, Bin L, *et al.* (2021). *China-U.S. Cyber-Nuclear C3 Stability. Carnegie Endowment for International Peace*. https://carnegieendowment.org/files/Levite_et_all_C3_Stability.pdf

33. Odgaard L. NATO's China Role: Defending Cyber and Outer Space. *The Washington Quarterly*. 2022; 45 (1) :167-183 . Available from: https://doi.org/10.1080/0163660x.2022.2059145

34. Kashiwagi R. (2021). *Japan aerospace cyberattacks show link to Chinese military: Police*. Nikkei Asia. https://asia.nikkei.com/Business/Technology/Japan-aerospace-cyberattacks-show-link-to-Chinese-military-police

35. Lee Y. (2022). Cyberspace governance in China: Evolution, features and future trends. *Institut Français des Relations Internationales (Ifri)*. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/lee_cyberspace_governance_china_2022.pdf

36. U.S.-China Economic and Security Review Commission. (2025). *Artificial eyes: Generative AI in China's military intelligence (Insikt Group Report)*. Recorded Future. https://assets.recordedfuture.com/insikt-report-pdfs/2025/ta-cn-2025-0617.pdf

37. The PLA goes back to school: Mapping new developments in China's military cyber education system. (2025, September 25). *Margin Research*. https://margin.re/2025/09/the-pla-goes-back-to-school-mapping-new-developments-in-chinas-military-cyber-education-system/

38. Simon T. (2023, January 29). Cyberproofing India's Space Assets. *Centre for International Governance Innovation*. https://www.cigionline.org/articles/cyberproofing-indias-space-assets/

39. Gill P. (2021, April 9). The Chinese cyber threat is real, and India's best defence right now is to keep its outage time limited. *Business Insider*. 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

40. The Defense Post. (2022, April 8). *India Claims It Foiled Chinese Cyber-Attack on Disputed Border*. https://www.thedefensepost.com/2022/04/08/india-chinese-cyber-attack/

41. Uppal R. (2023, February 14). *With Rising threat in Space domain from Electronic to Cyber Warfare, Space agencies enhancing Cyber security measures*. IDST, English.