NAVIGATING CYBER RISKS: FORTIFYING INDIA'S SPACE INFRASTRUCTURE

BISWAJIT BARICK AND GOPAL BHUSHAN

INTRODUCTION

On January 16, 2025, India created history with a successful Space Docking Experiment (SpaDex), entered into the elite group of nations and became the fourth nation to achieve this technological feat. This mission has showcased Indian technological prowess in spacecraft docking, undocking and rendezvous—a critical capability for future space operations.[1] In the year 2023, India's Chandrayaan-3 also comprised a mission which has been achieved by only three nations in space history. During all these missions, data is transferred from multiple locations across the globe, and the coordination and the command and control of satellites worldwide create vulnerable and

Lieutenant Colonel **Biswajit Barick** is a PhD Scholar at Amity Institute of Defence & Strategic Studies, Amity University.

Dr. **Gopal Bhushan** is Deputy Director General, Amity Directorate of Science & Innovation, Amity University.

1. Santosh Kumar, Gouri S, and Vatsla Srivastava. "SpaDeX Mission: Revolutionising Space Exploration," Press Information Bureau (PIB), January 16, 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2093369. Accessed on February 13, 2025.

easy targets to any space-faring nation if the cyber security of space assets is not addressed.

Modern society depends heavily on the space infrastructure, thus, the space infrastructure, on which services are essential for the smooth functioning of our societies, economies and security, becomes critical. It has to be protected and the protection of such assets from cyber threats is becoming a challenge. There are many examples in the past of cyber attacks on satellites viz. the Russian attack on Ukraine's Viasat KA-SAT network in 2022 to create communication outages during the commencement of the Russian invasion; the hacking and jamming of the Starlink network[2]; and the introduction of malware to a host of satellite terminals in 2023 which rendered communications offline.[3] The cyber threat to satellites is a reality today.

The paper examines the emerging cyber security threats to space assets, with a focus on the increasing vulnerability of space systems resulting from technological advancements and the commercialisation of the space sector. India's achievements in space exploration, such as the successful SpaDex, Chandrayaan-3 and future space ambitions call for robust cyber security measures to protect critical space assets which are essential to our nation for smooth functioning in contemporary scenarios. Cyber threats, including malware, social engineering, supply chain attacks, and denial-of-service attacks, pose significant risks to space missions and infrastructure. The paper analyses recent cyber attacks targeting space systems and suggests mitigation strategies, including comprehensive cyber security solutions, international cooperation, cyber security training, and rigorous security testing protocols.

As per the Department for Promotion of Industry and Internal Trade (DPIIT) Start-Up India Portal, the number of space start-ups has increased from just 1 in the year 2014 to 189 in 2023. The investment in space start-ups in India has increased to $ 124.7 million

2. "Russian Satellite Internet Downed via Attackers Claiming Ties to Wagner Group," *Darkreading.com* (Dark Reading Staff, 2023), https://www.darkreading.com/cyberattacks-data-breaches/hackers-claiming-wagner-group-ties-down-russian-satellite-internet-comms-. Accessed on February 13, 2025.
3 Robert Lemos, "India Needs Better Cybersecurity for Space Systems," *Cyware Labs*, September 11, 2024, https://social.cyware.com/news/india-needs-better-cybersecurity-for-space-systems-7e3add13. Accessed on February 15, 2025.

in 2023.[4] "India's space economy currently accounts for around 2 per cent of the global space economy, but it has the potential to reach $44 billion by 2033, with about 8 per cent of the global share,"[5] as per Space Economy Trends analysis details. The rapid development in the space sector makes India a growing target of cyber attacks on its space assets. The future missions in space as released by the Press Information Bureau are shown in Fig 1.[6] The increasing complexity and commercialisation of space systems require further strengthening of security measures to address emerging cyber threats effectively.

Fig 1: Indian Missions in Space

Source: "SpaDeX Mission: Revolutionising Space Exploration", PIB, January 16, 2025.

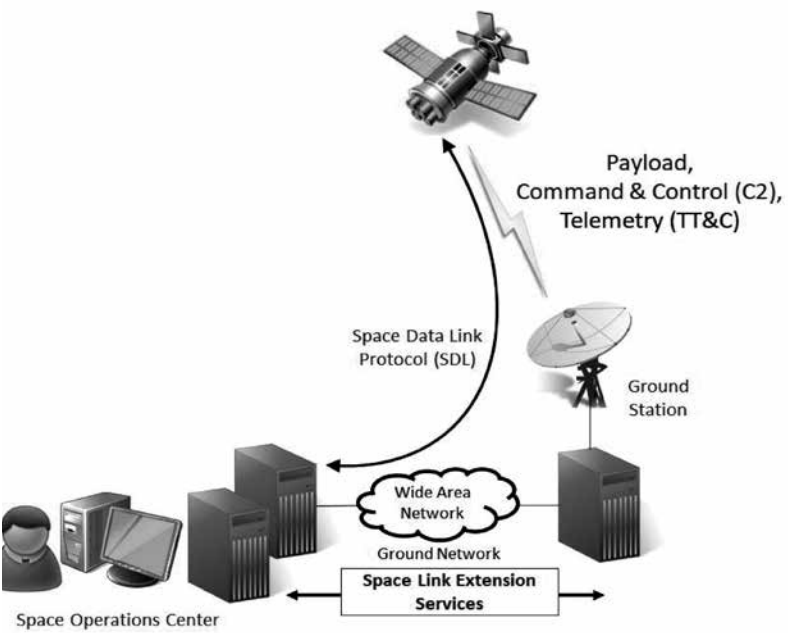
CYBER SECURITY LANDSCAPE IN SPACE SYSTEMS

Space Systems: The term "space systems" includes all the systems and equipment involved in space activities, from ground to orbit,

4. "The Next Frontier: Analyzing India's Focus on Space Technology," Investindia, April 23, 2024. https://www.investindia.gov.in/blogs/next-frontier-analyzing-indias-focus-space-technology. Accessed on February 16, 2025.
5. "Space Economy in India: Trends, Innovations, and Future Prospects - PWOnlyIAS," April 11, 2024. https://pwonlyias.com/editorial-analysis/space-economy-india/. Accessed on February 13, 2025.
6. Kumar, et. al., n. 1.

space operations centre and sensors to signal data and payloads. The same is given in Fig 2. This also includes critical technologies such as global positioning systems, communication and imagery systems and economic activities.[7] The two major roles of space systems are in national security and economic development, however, both are at risk of disruption today.

Fig 2: Space Systems Threat Spectrum



Source: François Quiquet, "Description of the Elements of a Satellite Command and Control System," Space & Cybersecurity Info, May 18, 2020, https://www.spacesecurity.info/en/description-of-the-elements-of-a-satellite-command-and-control-system/.

The challenge in the space systems lies in the long-term functionality of the hardware and software of the space assets. These systems remain unchanged for up to 10-15 years due to a difficulty

7. RADM Frank Cilluffo (Retd.), Mark Montgomery, Sharon Cardash, and Kelsey Shields, "Time to Designate Space Systems as Critical Infrastructure," April 2023. Accessed on February 15, 2025.

in upgradation. Thus, they become easy targets for cyber threats as technology is advancing rapidly in the cyber domain.

Hack of United Kingdom's Ministry of Defence Satellites:[8] In 2023, a cyber attack compromised systems in the UK Ministry of Defence, including systems related to satellite control and communications. It was part of a broader series of state-sponsored attacks on critical infrastructure. While specific details remain classified, the breach raised alarms about the vulnerability of satellite communications and defence systems. This was one of the incidents that became news but thousands of such cyber attacks occur across the globe on a daily basis. The space systems are not devoid of such attacks. With the enhancement of technology and the reduced launch cost, the assets in space are increasing day by day and so are the threats.

The Indian Computer Emergency Response Team (CERT-In) has recently issued a stark warning about the increasing cyber threats to satellite communications, cautioning that "each new satellite added to this intricate network is both an engineering marvel and a potential target for cyber threats".[9] CERT-In issued an advisory on February 4, 2025, stating, "With satellites now deeply integrated into essential daily operations—from navigation to transaction synchronization—any disruption can lead to widespread repercussions."

Threat Spectrum: The space systems function on the 'system of systems' concept, i.e., damage to one system will have a cascading effect on multiple systems. The threat spectrum to the systems is multiplying manifold due to the rapid development in this field and the collusive interplay of the public and private players in recent times. First, the vulnerability to space systems from the adversary is due to its vast importance for a nation. Second, the commercialisation of the space sector has enhanced the threat level owing to the lowering

8. Akshay Joshi. "UK Military in Major Data Breach, and Other Cybersecurity News to Know This Month," World Economic Forum, May 21, 2024, https://www.weforum.org/stories/2024/05/cybersecurity-news-lockbit-scattered-spider/. Accessed on February 13, 2025.
9. "CERT-In Warns of Cyber Threats to Satellites, Says Each New Satellite Is a 'Potential Target: Advisories'", n.d., https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2025-007#:~:text=Satellite%20communications%20play%20a%20crucial,between%20satellites%20and%20ground%20stations. Accessed on February 16, 2025.

cost of space launch and utilisation of Commercial Off-The-Shelf (COTS) components in satellites, especially Cubesat. Also, the entry of smaller teams in the space operations' innovative technological demonstrations has added to the threats.[10] Third, the main means of communication between space objects and ground stations are through the vast numbers of interconnected networks of computers. The uplink and downlink data of the systems are not always encrypted. Thus, the adversary has the opportunity for data manipulation, distortion and disruption. Fourth, the vast volume of data collected, handled and communicated by satellites every day offers countless vulnerabilities that can be exploited by any cyber attack.

The Risks: Any cyber attack aims to minimise the exposure and maximise the impact. In view of the ever-increasing vulnerabilities in space systems, the risks accompanying cyber attacks are as follows:

- Taking control of satellites physically and manoeuvring them to collide and destroy.
- Altering the orbits of the satellites will render them incapable of performing the designated tasks.
- Deliberately lowering the orbit so that these satellites reenter the atmosphere and get destroyed. In addition, by using cyber attacks, the control systems of the satellites are altered and cause irreparable damage.
- Jamming, spoofing and hacking of communication networks to target the mission packages. Jamming, however, is not a typical cyber threat but spoofing is a major cause of concern as the user or receiver of the satellite data is unaware of the manipulated data that is being received post-spoofing by any cyber attack.
- The cyber attackers can target the ground systems which control the satellites in space and destroy them.
- The risk to the space systems from cyber attacks can emerge from one state to another or from military actions. In addition, from a well-resourced and well-funded criminal element seeking financial gains or from anti-national elements to promote and publicise their cause or from hackers to gain publicity.

10. Matteo Calabrese. "Space Oddity: Space Cybersecurity Lessons from a Simulated OPS-SAT Attack", Johns Hopkins University, July 2, 2023. Accessed on February 16, 2025.

TYPES OF CYBER ATTACKS/THREATS TO SPACE ASSETS

In today's scenario, cyber attacks can get detected and there are policies to take suitable actions against the defaulters. However, deniability and ambiguity in pinpointing the perpetrator continue. If we reflect on history, "The Max Headroom hack remains the gold standard: its content was bizarre, its motives were mysterious, and its perpetrator was never caught".[11] The types of cyber attacks which occur in the typical Information Technology (IT) industry also affect space operations as the systems used are the same.

- **Malware Attack:** The most common type of cyber attack is a **malware** (acronym of malicious software) attack which includes viruses, trojans, worms, ransomware and spyware. The malware enters the space system through any link on an untrusted email, website or by downloading unauthorised software. Once it enters the computer system, it deploys on the target systems and starts collecting the sensitive data, blocks network components and disrupts the system functioning by switching off the entire system itself.[12]
- **Social Engineering Attack:** In today's world of social media, a social engineering attack is very common and involves deceiving users into providing an access point for malware. The user unknowingly gives out sensitive data or installs malware on the device as the attackers pose as genuine entities. The main types of social engineering attacks include phishing, baiting, pretexting, Voice Phishing (Vishing), SMS phishing (Smishing), Tailgating and Piggybacking.
- **Supply Chain Attack:** The supply chain attack is an innovative type of cyber threat to developers and vendors associated with space operations, as it infects genuine applications and dispenses malware by means of a source code and software update mechanisms. These attacks are dangerous as the compromised

11. Katie Serena, "The Story of America's Creepiest Unsolved TV Hack," *All That's Interesting*, May 25, 2021, https://allthatsinteresting.com/max-headroom-incident. Accessed on February 13, 2025.
12. Nitin Agarwala, "Cyber Attack Against Satellites," *Synergy*, vol 3, issue no. 1, May 29, 2024, pp. 71–95, https://www.researchgate.net/publication/380934638_Cyber_Attack_against_Satellites. Accessed on February 16, 2025.

applications are certified by trusted vendors. The entire supply chain gets infected as the supplier of the systems is not aware that the application has been compromised since its inception. Such attacks include compromising the build tools and code signing procedures, and malicious codes generated during auto updates and embedded in the hardware/software.

- **Man in the Middle (MitM):** The MitM attack involves interference and interception of the communication between two ends such as the user and application. The attacker gets into the system and steals the sensitive data by impersonating, and eavesdropping on, the network. The means used are Wi-Fi eavesdropping, email hijacking, Internet Protocol, Hypertext Transfer Protocol Secure and Domain Name System (IP, HTTPS and DNS) spoofing.
- **Denial of Service (DoS):** In the DoS attack, the system gets overloaded with huge data traffic and its normal operations are stalled. If the DoS attack is involved in multiple devices, then it is known as Distributed DoS (DDoS). The techniques are SYN flood DDoS (TCP sequence), User Datagram Protocol (UDP) flood DDoS, HTTP flood DDoS and Network Time Protocol (NTP) DDoS.
- **Injection Attack*:*** An injection attack involves inserting malware into the code of a web application through the identified vulnerabilities. Once the attack is successful, the sensitive data is exposed, the DoS attack is executed, and the systems are then compromised. The methods of these kinds of attacks are Structured Query Language (SQL) injection, Code injection, Operating System injection, Lightweight Directory Access Protocol (LDAP) injection and Cross-site Scripting.

The list of cyber attacks on the space systems in the year 2024 is given in Table 1, as per one of the recent studies by the Centre for Security Studies at ETH Zurich that identified 124 cyber attacks against the space sector: DDoS attacks constituted 65 per cent, intrusion attacks were 11 per cent and 9 per cent were hacking and leak operations.

Table 1: Cyber Attacks on Space Systems in 2024

Month	Year	Type of target	Country targeted	Target	Attacker	Type of attack
February	2024	Company	Luxembourg	SES	Phoenix	DDoS
April	2024	Company	Russia	Astra	IT Army of Ukraine	DDoS
April	2024	Company	Russia	Altegrosky	IT Army of Ukraine	DDoS
March	2024	Company	Russia	Gazprom Space Systems	IT Army of Ukraine	Intrusion
March	2024	Company	Russia	RSCC	IT Army of Ukraine	Intrusion
January	2024	Agency	Russia	Far Eastern Scientific Research Center of Space	BO Team	Intrusion
March	2024	Company	Poland	Floris	No Name 057(16)	DDoS
July	2024	Company	Italy	Leonardo	Cyber Dragon	DDoS
January	2024	Company	Russia	Special Technology Center	GUR	Data breach
July	2024	Research	Russia	Military Training Center at BMSTU	Cyber Resistance	Data leak
June	2024	Research	Netherlands	SRON	62IXGROUP	DDoS
March	2024	Company	Ukraine	Unknown	Pharanos Cyber Army	Intrusion
January	2024	Company	Russia	GPSUpdate.ru	Anonymous Italia	DDoS

July	2024	Company	USA	TrafficView	LulzSec	DDoS
January	2024	Company	Russia	Sev-Sat	HimarsDDoS	DDoS
June	2024	Company	Ukraine	JSC Kyiv Radar Plant	No Name 057(16)	DDoS
July	2024	Company	Ukraine	JSC Kyiv Radar Plant	Cyber Army of Russia	DDoS
January	2024	Agency	Ukraine	UCRF	Cyber Army of Russia	DDoS
September	2024	Agency	USA	NOAA	CyberVolk	Data leak
April	2024	Company	USA	Starlink	Ukraine (unspecified)	Software cracking
May	2024	Company	Italy	Avio	No Name 057(16)	DDoS
September	2024	Company	France	Safran	JustEvil	Data leak
September	2024	Company	Ukraine	JSC Kyiv Radar Plant	No Name 057(16)	DDoS
September	2024	Company	Ukraine	JSC Kyiv Radar Plant	No Name 057(16)	DDoS
September	2024	Agency	USA	US Geological Survey	Cyber Volk	Data breach extorsion
September	2024	Company	Ukraine	Arsenal	No Name 057(16)	DDoS
September	2024	Company	Sweden	Hexagon	User1	Intrusion
September	2024	Unknown	Ukraine	Cell phones (GPS data)	Unknown	Malware

Source: Clémence Zürich, "Hacking the Cosmos: Cyber Operations Against the Space Sector a Case Study from the War in Ukraine," ETH Zurich, October 2024, https://doi.org/10.3929/ethz-b-000697348.

The Wiper malware used in the Via-sat hack was a unique type of attack—no other operation of that type had been observed so far. Thus, we can safely say that most operations against the space systems have been unsophisticated attacks, with temporary and recoverable

consequences.[13] This is just the beginning where the hacktivists are now taking sides in armed conflicts, which is evident not only in the Russo-Ukraine War but also in the Israel-Palestine conflict, to target the space systems. Recently, India announced the launch of multiple satellites to enhance the space-based surveillance programme. The sources in the military establishment told the leading newspapers during Aero India 2025, "The first lot of satellites under the third phase of the space-based surveillance (SBS-3) programme will be launched by 2027-28. A total of 52 satellites will be launched under the program".[14] If this is the case, the focus towards the cyber security aspects of the space system will gain more prominence in the future. This trend needs to be flagged and mitigation measures need to be implemented as it will have a great impact on future operations in the space sectors.

CYBER SECURITY CHALLENGES IN SPACE INDUSTRY

The concept of cyber security applies broadly to all systems that rely on digital and cyber resources, however, space systems have unique factors that differentiate them from terrestrial complements. Securing space systems against cyber threats poses extraordinary challenges due to operational constraints, environmental factors, and the critical nature of space-based assets. The major challenges are as follows:

- **Distance and Inaccessibility:** The satellites, once launched, are not easily accessible for upgradations physically. The regular maintenance and security enhancements undertaken for terrestrial systems are not possible due to their inaccessibility.
- **Simple Workforce Access Protocol (SWaP) Constraints and Legacy Systems:**[15] The space systems in orbit are highly controlled

13. Clémence Poirier, "Trawling Hacker Forums Uncovers Crucial Information on Space Cyber Attacks," *ViaSatellite*, October 30, 2024, https://interactive.satellitetoday.com/via/november-2024/trawling-hacker-forums-uncovers-crucial-information-on-space-cyber-attacks. Accessed on February 16, 2025.
14. Kalyan Ray,"Aero Show 2025: First Batch of Satellites Under New Space Surveillance Programme to be Launched by 2027-28," *Deccan Herald,* February 12, 2025, https://www.deccanherald.com/india/karnataka/bengaluru/aero-show-2025-first-batch-of-satellites-under-new-space-surveillance-programme-to-be-launched-by-2027-28-3402717. Accessed on February 16, 2025.
15. Syed Shahzad, et al., "Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers," *Systems*, 12, no. 10, October 15, 2024, https://doi.org/10.3390/systems12100434. Accessed on February 15, 2025.

by weight, size and power limitations which levy substantial design trade-offs. In terrestrial systems, robust hardware security modules can be incorporated. In addition, due to the requirements of lighter weight and low power solutions, the employment of legacy technology is selected which is susceptible to modern cyber threats.

- **The Lifespan of Satellites:** The average life of a satellite is 15-20 years, thus, it becomes difficult to keep pace with the ever-evolving cyber threats and cyber security standards.
- **Communication Distances:** Owing to the long-distance communication, the signals to and from the satellites are susceptible to interception, jamming and manipulation due to the shared nature of the Radio Frequency (RF) spectrum and the long communication paths. The shared nature of the RF spectrum allows both legitimate and malicious parties to access and potentially interfere with satellite communications. Additionally, the long distances involved in satellite communication introduce latency and can make it easier for attackers to intercept or manipulate signals.

GLOBAL STRATEGIES TO ADDRESS CYBER SECURITY CHALLENGES

An Executive Order (EO) was signed by President Biden on "Strengthening and Promoting Innovation in the Nation's Cybersecurity".[16] The order includes detailed measures to protect systems involved in space operations. Section 3, "Improving the Cyber Security of Federal Systems," and Section 8 "National Security Systems and Debilitating Impact Systems," of the EO, highlight the actions to be undertaken by the agencies towards cyber security measures to be adopted in the space systems, strict adherence to the cyber security protocols by the private players in space operations and implementation of cyber defences on government procured space national security systems. The North Atlantic Treaty Organisation's

16. Office of Space Commerce, USA "Cybersecurity Executive Order Includes Direction on Space Systems," January 17, 2025, https://space.commerce.gov/cybersecurity-executive-order-includes-direction-on-space-systems/. Accessed on February 13, 2025.

(NATO's) Cooperative Cyber Defence Centre of Excellence (CCDCOE) has invited experts to revise the Tallinn Manual "to review legal and policy challenges related to cyber war."[17] Thus, these global efforts emphasise the importance of an integrated approach to maintaining the security of space infrastructure amidst the ever-expanding cyber challenges.

A few strategies that are being implemented/explored to navigate through the challenges globally are:

- **Data and Signals Encryption**: All the agencies involved in space operations need to ensure that all data and signals transmitted to and from satellites are encrypted. This will enhance the protection from interception and tampering. This is akin to the existing model of using advanced encryption protocols in military satellites to secure communication channels.
- **Authentication and Access Control**: Implementation of strong authentication and access control mechanisms to prevent unauthorised access to space systems. These measures apply to both ground systems and assets in orbit.
- **Redundant and Fail-Safe Mechanism**: The process of building redundancy of space assets ensures that if one component is compromised, back-up systems will be available to take over, and this will minimise the downtime and impact.
- **Artificial Intelligence (AI)-Based Detection Systems:** Incorporation of Artificial Intelligence (AI) and Machine Learning (ML) in space assets to detect unusual activities, such as unauthorised access attempts or abnormal signal patterns that indicate a cyber threat.
- **Quantum Technology**: Quantum cryptography is an emerging technology with potential applications in satellite communication. This could enhance the encryption key standards that are theoretically impossible to intercept without detection.
- **Hardening Firmware and Software**: Inception of the launch cyber security measures pre-launch to include hardened firmware and

17. Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge: Cambridge University Press, 2013), pp. 13-14, https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE. Accessed on February 13, 2025.

software, helps protect satellites from malware. The option of remote updates and rigorous testing can avoid vulnerabilities.

- **International Collaboration and Policies:** Keeping in view the global nature of space, organisations such as the International Telecommunication Union (ITU), United Nations Office for Outer Space Affairs (UNOOSA), European Space Agency (ESA) and other space-faring nations play a crucial role in establishing cyber security standards and promoting collaboration.

INDIAN SPACE NAVIGATING THROUGH CYBER RISKS

In the space era before the year 2000, the space industry relied on security through obscurity, as the players in the sector were limited. However, the new space era has opened up to new players and technologies, thus, the previous approach to security needs to be revisited and revamped, keeping in view the ever-changing landscape in the cyber domain. Thus, it is clear that the threats to space systems exist, and at an appropriate level, the following questions must be asked and answered to arrive at critical security measures before the deployment of space systems that may have a nationwide impact in the long run.

1. Do the cyber security measures in the nation have collection assets, systems or networks to identify cyber attacks in space systems?
2. Could the disruptions to the critical space systems impact national security, economic security, public health or safety?
3. Do existing policies, mechanisms or governance structures address the defaulters once identified?
4. Do the systems involved in the space domain incorporate security measures from the inception stage?
5. Are the people handling the systems in the space domain adequately trained to avoid any kind of inadvertently major impact?

Existing Mitigation Measures: If we dwell on the above-mentioned questions, we would be led to the mitigation measures that should be incorporated by the agencies working in this field. The Indian Space Research Organisation (ISRO) has made significant

strides in space technology and gained worldwide recognition and acclaim. As we continue to make our mark in the global space arena, the necessity for robust cyber security measures becomes paramount. The cyber security aspect is taken very seriously at ISRO. The cyber security framework has been designed to be robust, adaptive, and in line with international best practices. It includes a combination of technical measures, policies, and the expertise of certified ethical hackers.[18]

Suggested Measures: The cyber security landscape changes faster than imagined. Thus, India as a nation needs to regularly assess the existing means to address the cyber threats to its space assets and in addition, incorporate the latest solutions available globally. The solutions which are relevant and can be adopted into the realm of cyber security of space systems in the Indian context are covered in the succeeding paragraphs.

- **Comprehensive Cyber Security Solutions:** These are the tools that any organisation/agency should incorporate into the systems to defend against cyber threats and accidental damage to sophisticated and sensitive systems. The security solution is available for Application, Network, Cloud and Endpoint devices. The Internet of Things (IoT) security and threat intelligence comprise the important aspects that need to be considered by the space systems.
- **International Collaborations:** No one country in isolation can effectively protect its space assets from the cyber security challenges emerging in contemporary scenarios. The United Nations Organisation for Outer Space Affairs (UNOOSA) has initiated a discussion on these aspects. All the nations, including India, can play a crucial role in collaborating and coordinating the existing measures and the futuristic means to face the challenges and mitigate the same. A successful example of international cooperation is the establishment of the Space Data Association (SDA), an international organisation that promotes the sharing

18. Ethical Hacker, "Safeguarding the Stars: A Deep Dive into ISRO into ISRO Cyber Security Measureser Security Measures," *Linkedin*, October 15, 2023, https://www.linkedin.com/pulse/safeguarding-stars-deep-dive-isro-cyber-security-giridaran-e. Accessed on February 15, 2025.

of data on the movement of space objects to prevent collisions, and to mitigate risks. The SDA's collaborative approach serves as a model for addressing cyber security threats, wherein sharing threat intelligence and best practices can enhance the collective security of space missions.[19]

- **Cyber Security Training:** The space industry needs cyber security training akin to any Information Technology (IT) industry. As of May 2023, a report published by the *Business Standard* newspaper claimed that the industry had about 40,000 open opportunities, indicating the growing demand for skilled cyber security professionals. However, the demand-supply gap stood at 30 per cent, projecting a major skill challenge in the industry, according to the study by the tech staffing firm TeamLease.[20] The *Atmanirbhar Bharat* mission should also focus on the training of youth and professionals working in the space domain to build an ecosystem of homegrown software and skilled cyber security workers. The number of skilled cyber security professionals has increased from one lakh in 2021 to three lakhs in 2023 but the scope is large as the gap is ever-increasing with the latest technologies that need to be plugged.
- **Rigorous Security Testing Protocols:** The software and hardware being developed or assembled in India should undergo rigorous security testing protocols before it is deployed in any system. Most of the space projects today are prototype projects that lack the required security protocols, being the novel prototypes. However, the same systems may be studied in detail by threat actors and utilised in the future against the target nations. Hence, all efforts at the apex level need to be initiated to address vulnerabilities. The same can be achieved by sharing existing technologies with novice players and interchanging technologies to build resilience in space systems to face cyber threats.

19. Antara Jha. "Cybersecurity in Space and the Challenges of International Regulation", *Defstrat.com*, September 4, 2024, https://www.defstrat.com/magazine_articles/cybersecurity-in-space-and-the-challenges-of-international-regulation/. Accessed on February 15, 2025.
20. Sourabh Lele, "India Suffering High Cybersecurity Skill Gap, 40K Open Positions: Report," *Business Standard*, June 21, 2023, https://www.business-standard.com/technology/tech-news/india-suffering-high-cybersecurity-skill-gap-40k-open-positions-report-123062100397_1.html. Accessed on February 15, 2025.

- **Zero Trust Security Architecture for Space Systems:** The Space Systems Command (SSC) in the US is partnering with industries to develop and integrate a zero trust security solution across the entire range of space assets, from ground systems to satellites and other related systems[21]. Implementation of zero trust security mechanisms by ISRO can significantly enhance the security and resilience of its space missions and infrastructure. It will help in protection of sensitive data, enhance network security and real-time threat detection, secure remote access and resilience against cyber attacks.
- **Quantum Technology and AI:** Quantum technology has emerged as a potential solution to address the ever-escalating cyber threats across the globe. ISRO has made significant strides in quantum communication, and employment of quantum key distribution for enhanced encryption will go a long way to mitigate the cyber threats to space systems. With the advent of AI and ML, new dimensions have been added to cyber security, calling for a collective effort from all arenas, including technology firms, academia, and cyber security experts. Thus, collaborative and cooperative measures, if undertaken, will be a formidable force to reckon with, which will be essential to safeguard India's space systems from cyber threats.

CONCLUSION

The cyber security for space systems in the future will be shaped by increasing reliance on satellite constellations and the accelerating speed of cyber threats. As the constellation grows, the threat complexity will grow exponentially which will require seamless coordination and collaboration of multiple agencies to mitigate the challenges. The autonomous solution to the future anticipated threats will take centre-stage.

Cyber security begins with improving encryption standards: encryption of the uplink and downlink communication between the

21. "Space Systems Security and Resilience Landscape: Zero Trust in the Space Environment," *Cybersecurity and Infrastructure Security Agency Report, April 2024*, June 1, 2024, https://www.cisa.gov/sites/default/files/2024-06/Space%20Systems%20Security%20and%20Resilience%20Landscape%20-%20Zero%20Trust%20in%20the%20Space%20Environment%20%28508%29.pdf. Accessed on January 15, 2025.

satellite and the ground stations; implementation of cryptographic techniques like quantum encryption and end-to-end protocols; and incorporation of multi-layer systems to ensure redundancy and difficulty for malicious actors. In addition, it requires a comprehensive relook into the training of the workforce dealing with the systems in space operations[22]. The legal framework in the cyber security-related aspects of space systems will require continuous review, not only by a particular nation but as a collaborative effort by all space-faring nations.

A study published by the Foundation for Defence of Democracies (April 2023) recommended that space systems be designated as a critical infrastructure sector, considering their enhanced utility in our everyday lives. However, in the same study, it was also brought out that even after having identified the threats in the space domain many years ago, the steps taken by the United States have been inadequate. To counter cyber threats in space, a combination of regulatory frameworks, technological advancements and operational strategies must be implemented by space-faring nations.

In the case of India, whose ambition in the space domain is taking a positive stride, it needs to identify threats and enhance collaboration with other space-faring nations to learn from their experiences and build a robust and resilient ecosystem to thwart cyber security challenges. In addition, the private players' involvement in the space domain is a welcome measure, but the protocols of cyber security should not be compromised at any cost. As the saying goes, today's solutions may become tomorrow's problems. The speed of development in space systems today should not impede our path of navigation in this glorious space journey tomorrow due to cyber security aspects.

22. Anna Ribeiro, "CSIS 2025 Space Threat Assessment: Cyberattacks on Space Systems Persist, Tracking Harder Amid Infrastructure Threats," *Industrial Cyber*, April 28, 2025, https://industrialcyber.co/reports/csis-2025-space-threat-assessment-cyberattacks-on-space-systems-persist-tracking-harder-amid-infrastructure-threats/. Accessed on April 16, 2025.