Winning the Legal Battle of Cyber Security in Space Systems

Khyati Singh

Laws have been the backbone of human civilisation as they have facilitated the curtailment of actions that may lead to disruption, or cause disharmony. Space, being free from continuous human presence, was also away from this human invention of laws. However, with the bombardment of space missions and endless gadgets in the orbits, it become more than necessary to have laws for protecting space.

The foundation of space laws was laid with the Outer Space Treaty in 1967, which outlined certain key principles for the security of space. The treaty was formally known as the 'Treaty on Principles Governing the Activities of States in Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.' Its key principles included non-appropriation, that is, outer space, along with the Moon, cannot be attributed to a single state. There is no claim of sovereignty. In addition, it called for peaceful use of space by all countries, with clearly defined lines to forestall the installation of weapons of mass destruction, or nuclear weapons in orbit or on station, or celestial bodies, thereby forbidding the testing of any kind of military weapons in space. The treaty also

Ms **Khyati Singh** is a Research Associate at the Centre for Air Power Studies, New Delhi.

touched upon the environmental protection aspect by mentioning that states should avoid harmful contamination. Moreover, it tried to forge cooperation for the safety of astronauts by treating missions as a collective effort for the good of humankind. The treaty was ratified by over 100 countries which included all important space-faring nations. Although it was a significant development of its time, it failed to include many modern challenges that are mounted against space exploration.[1]

This treaty evolved during the time of the Cold War with limited space available for the private sector. However, the contemporary times have seen the active engagement of private companies in space. The ambiguities in the laws become easy to exploit amidst numerous participants. Furthermore, the issue of space debris has surfaced over and over again but has not received any significant action. Despite prohibiting weapons of mass destruction, countries are often engaged in developing space-based weapons, which fosters the fear of an arms race in space. Most importantly, the treaty does not have a robust enforcement mechanism and relies only on diplomatic pressure and state compliance.

The most advanced level of threats in space emerges from the cyber frontier precisely because of the difficulty to physically access these systems for upgradation and maintenance. Space stations, satellites and various orbital assets are exposed to different cyber attacks like denial-of-service attacks, data interception and manipulation, signal jamming and spoofing, unauthorised access and control. While efforts are being made to deal with these challenges with better technologies, the legal framework to address them had not been completely developed.

1. United Nations Office for Outer Space Affairs, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies", unoosa.org. Accessed on July 9, 2024.

The current legal framework to deal with cyber attacks has at its disposal a few treaties and regulations. The first of which has been the Outer Space Treaty, but as pointed out earlier, it does not foresee cyber attacks as a case in point. The Budapest Convention, also called the 'The Convention on Cyber Crime' is a significant treaty that addresses the cause of cyber crime. Its main provisions include criminalisation of activities like copyright infringement, system interference, misuse of devices, and illegal access to computer systems, amongst other offences. It also has procedural laws in place that expedite the preservation of stored data, interception of content data, search, and seizure of computer data.[2]

Although it provides a guideline for countries to develop cyber crime legislation, it does not specifically address space-based satellite systems. Moreover, it does not account for new-age cyber crimes like cyber terrorism and is often labelled as an attack on sovereignty by nation-states. It is due to this mindset that only 68 states have ratified it, and major powers like Russia and China are not signatories. This makes it a half-baked cookie. While there has not been an explicit mention of space systems, the principles it has laid down can be deployed for cyber crimes for space-based systems with an additional framework that specialises in them.

In the absence of an all-encompassing international treaty, countries have, at their national level, some laws and regulations that try to tame the menace of cyber attacks in space systems.

UNITED STATES

National Space Policy 2020: This is a comprehensive document that has marked the principles, goals, and objectives pertaining to space. It explicitly mentions the need to strengthen the cyber security aspect of space systems. The objectives entail measures

2. Council of Europe, "The Budapest Convention (ETS No. 185) and its Protocols", European Union, Budapest Convention, Cybercrime, coe.int. Accessed on July 9, 2024.

to improve the detection and response to cyber threats and to build more resilient space infrastructure that can withstand cyber attacks and mitigate risks. Promoting information sharing amongst various government agencies on cyber threats, along with international allies and key private players, is also on the list. It further highlights the importance of ensuring the integrity of the supply chain to prevent any cyber vulnerabilities and developing a workforce that is capable of dealing with challenges emerging from cyber in space. It also calls upon the private sector to adopt the best cyber practices, and for the state to facilitate commercial cyber security efforts.[3]

Space Policy Directive-5 2020: This directive specifically focusses on the issue of cyber security in space systems and provides a detailed framework for the protection of space assets from cyber threats. It stresses the need for operators to develop and implement cyber security measures that protect space systems against unauthorised access to critical space vehicle functions, protection against malicious activities, jamming and spoofing, along with physical protection for ground systems. It demarcates the framework for both state and private sector operations in space with attempts to evolve best practices and adopt cyber hygiene.[4]

Cyber Security and Infrastructure Agency: This is a crucial component of the US Department of Homeland Security that focusses on infrastructure security, cyber security, and communications. Despite its broad domain, it has been increasingly focussing on the cyber security of space systems. Its key functions related to space cyber security involve risk assessment and analysis which include conducting assessments of the cyber security risk to

3. The White House, "National Space Policy", United States of America, National-Space-Policy.pdf, archives.gov. Accessed on July 9, 2024.
4. The White House, "Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems", United States of America, September 4, 2020, Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems – The White House, archives.gov. Accessed on July 9, 2024.

ground-based and space-based units of the system and analysing possible vulnerabilities in the satellites and other communication technologies. It also operates the National Cyber Security Integration Centre, offers incident response services, and works towards capacity building and critical infrastructure protection.[5]

EUROPEAN UNION (EU)

EU Cyber Security Strategy 2020: This is an all-encompassing plan to improve the EU's collective resilience against threats from cyber. It also covers aspects of cyber challenges in space with key objectives pointing towards critical infrastructure protection and stresses on expanding the scope of Network and Information Systems (NIS) to include more sectors and space-based entities. It also lays emphasis on security by design and addresses the issues of the impact of emerging technologies like quantum and Artificial Intelligence (AI) on space systems. It has tried to evolve cyber security certification, which would be relevant for private players in the space industry.[6]

European Space Policy: This policy guides the EU's approach to space exploration. Apart from a range of elements that focus on strategic autonomy, security, and cooperation, it has designated aspects for cyber security. It classifies space systems under critical infrastructure which requires robust cyber security measures.[7] It has initiated programmes like the EU Agency for the Space Programme (EUSPA) which looks after the security accreditation of EU space systems and the Galileo Security Monitoring Centre.[8] The European Space Security and Education Centre (ESSEC) focusses

5. "Cybersecurity and Infrastructure Security Agency (CISA)", | USAGov. Accessed on July 9, 2024.
6. European Council, "Cyber Security: How the EU Tackles Cyber Threats", Consilium, europa.eu. Accessed on July 9, 2024.
7. European Council, "EU Space Policy", Consilium, europa.eu. Accessed on July 9, 2024.
8. EUSPA, EU Agency for the Space Programme, europa.eu. Accessed on July 9, 2024.

on education and training in the security of space, including cyber security. The Space Situational Awareness (SSA) programme has a component for protecting space assets from cyber threats. The GovSatCom Initiative is another such programme that especially works to protect satellite communications for both institutional and governmental users.

European Union Agency for Cyber Security (ENISA): It is a key organisation under the ambit of the EU framework which focusses on safeguarding network and information security across the states. Its primary objective is to achieve cyber security at a common level, and it has undertaken several initiatives to secure satellites from cyber threats. These include publishing satellite cyber security reports, regularly updating the cyber threat landscape, and organising cyber security exercises along the lines of scenarios that involve cyber attacks on space systems. ENISA has tried to address key challenges like the cross-border nature of cyber threats, and sector diversity.[9]

RUSSIA

Russian Space Agency (Roscosmos): Known as the State Space Corporation, this is the agency responsible for space programmes and research in Russia. It does not give out many details about its missions and programmes in the public domain. It has been looking after the cyber security of space systems by implementing its own set of protocols that cover both ground-based and space-based systems. It particularly emphasises on information security. Furthermore, it has taken certain initiatives like cyber protection centres to protect digital infrastructure, and invests heavily in anti-jamming technologies.[10]

9. ENISA, europa.eu. Accessed on July 9, 2024.
10. Elizabeth Howell, "Roscosmos: Russia's Space Agency", Space.com, January 30, 2018, Roscosmos: Facts & Information About Russia's Space Agency | Space. Accessed on July 9, 2024.

CHINA

China National Space Administration (CNSA): This is the agency responsible for China's civilian space programmes and international cooperation. Much like the Russian space agency, it does not disclose all details about its cyber security measures. It works on a comprehensive security strategy that integrates cyber security with physical security and focusses on developing indigenous technology to reduce reliance on foreign systems and, therefore, mitigate vulnerabilities.[11] Its major initiatives and focus areas include investments in quantum communications, including launching the Micius, which is the world's first quantum communication satellite. It provides an uninterrupted communication channel for space assets. It cannot be hacked, and that makes it one of a kind.[12] It has also implemented measures for advanced cyber security, including the BeiDou which is a navigation system and looks after the growing satellite networks.[13] It is further exploring the use of machine learning and AI to enhance the cyber security of space systems.

JAPAN

Japan Aerospace Exploration Agency (JAXA): This is responsible for the protection of space assets, and satellites, against cyber threats. It has in the past collaborated with other international space agencies like the European Space Agency (ESA), National Aeronautics and Space Agency (NASA) and Roscosmos to enhance the cyber security of space systems. It has also established stringent cyber security policies that are in line with international

11. Elizabeth Howell, "China National Space Administration: Facts & Information", Space.com, May 25, 2016.
12. Karen Kwon, "China Reaches New Milestone in Space-Based Quantum Communications", *Scientific American,* June 25, 2020. Accessed on July 9, 2024.
13. Jun Lu, "Global Capabilities of BeiDou Navigation Satellite System", *Springer*, August 31, 2020, Full Text, springeropen.com. Accessed on July 9, 2024.

best practices for cyber security. It has tried to build systems that are more resilient and even if a unit of the system is compromised, the overall mission can continue with minimum disruption.[14]

National Cyber Security Strategy: This strategy document highlights the principal areas where the state is making advances in both research and policy. It entails measures for the protection of critical infrastructure, cyber defence capabilities, international cooperation, public-private partnership, and research and development. It has defined the policy framework to protect space systems, along with guidelines to develop and implement cyber security initiatives for space assets.[15]

INDIA

Draft Space Activities Bill: This Bill aims at regulating and promoting space activities domestically, along with the objective of fostering a sustainable space environment. It implicitly touches upon various factors of space operations that are under cyber threat. The key provisions touch upon the aspects of authorisation and licensing, regulation and supervision, and protection of space systems. In terms of cyber security, it mandates to ensure that space systems are designed and operated with proper cyber security measures intact. It also mandates risk assessment for all space missions, including cyber threat assessment. Moreover, entities are also required to implement risk mitigation practices and strategies to tackle potential cyber attacks. It has also established a protocol for incident response and management in the event of a cyber attack, along with ensuring that contingency plans and recovery strategies are in place to minimise the disruption.[16]

14. Japan Aerospace Exploration Agency (JAXA). Accessed on July 9, 2024.
15. Mihoko Matsubara, "Japan's Cybersecurity Strategy From the Olympics to the Indo-Pacific", *IFRI*, February 2021, matsubara_mochinaga_japan_cybersecurity_strategy_2021.pdf, ifri.org. Accessed on July 9, 2024.
16. PRS Legislative Research, Draft Space Activities Bill, 2017. Accessed on July 9, 2024.

Indian Space Research Organisation (ISRO): ISRO has in place various cyber security protocols. The components include network security through the deployment of firewalls and Intrusion Detection Systems (IDS) to monitor and secure all the networks from unauthorised access and cyber attacks. It also has in place the use of Virtual Private Networks (VPNs) to secure communications. Other measures like regular training programmes, phishing simulations, vendor assessments, role-based access control, and multi-factor authentication are in place.[17]

ALL GLITTER AND NO GOLD!?

While there has been a newfound awareness amongst states to protect their space systems from cyber threats, there is still a lack of an active legal ecosystem to deal with the challenges.

The primary reason for this lackadaisical approach is the absence of a robust regime and internationally accepted legal framework for space systems. Cyber, being a sub-section of this mammoth structure, often ends up in footnotes. This lack of harmonisation pushes states into silos, where they are bound to national legal frameworks.

While a majority of national frameworks are overlapping in their themes and objectives, they have not been able to tackle the issue of cyber security on legal grounds. This problem becomes further aggravated for countries that do not have a designated cyber policy for the nation as a whole. Moreover, attribution is the biggest challenge that countries face in the cyber domain. This further widens the gap which is exploited by state-sponsored cyber groups to engage in cyber crimes.

In addition, many space-based technologies have a dual use nature, that is, they have both military and civilian applications. Amidst this, the often-demarcated lines of law between civilians

17. Indian Space Research Organisation (ISRO), isro.gov.in. Accessed on July 9, 2024.

and the military become blurred. Hence, finding a middle ground between them becomes a tall order.

Furthermore, technologies advance faster than laws. Space and cyber thrive on the foundation of technological progress. Designing a legal framework for the same is time-consuming and cumbersome. By the time a framework is implemented, new technological challenges emerge. Therefore, more foresightedness is required in drafting laws for cyber space.

To conclude, while the space domain continues to expand, the laws that secure it must be equally adaptive. Their balanced nature is fundamental as a miscalculated law can prove regressive for the technological progress of a nation. Though various national and international efforts are providing some legal back-up for space operations, there is a dire need for more comprehensive and coordinated international action and legal mechanisms, provided space is a shared resource. Ensuring compliance will also be a challenge that the states would face if these treaties are not legally binding. Therefore, with the continuous advancement and achievement in space, states would be required to adopt practices that keep the race healthy and legally sound.