The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2024
Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

CYBERSECURITY AND SPACE LAW IN INDIA

Introduction:

In the era of advanced technology, the intersection of cybersecurity and space law has become a crucial area of concern for all countries, but especially for a country like India. The delicate dance between protecting space assets and having safeguards against cyber threats takes center stage as the Indian Space Research Organisation (ISRO) steadily advances the country's space program to new and unprecedented heights. Cyberattacks might target satellites, spacecraft, and ground stations. An intrusion into the networks that manage these resources might lead to a loss of control, unauthorized entry, or even modification of orbital paths. Ergo, strong cybersecurity measures must be put in place.

India's inception and advancement into the celestial realm reaching new heights, (roughly 384,400 kilometers away, the distance from Earth to the Moon), has been nothing short of extraordinary. With missions like the Chandrayaan-3, Aditya-L1 and many more in the works, it has become more than essential to protect the infrastructure and technology crucial to carry out such feats. With the risk of cyberattacks being much higher in the field of rocket technology, the chairman of ISRO, S. Somanath has stated that around 100 cyberattacks are launched against India's space agency every day. [1]

Space technology, which includes telecommunications satellites, GPS, internet access, and weather tracking, is critical for worldwide communication and innovation. A cyber-attack on space infrastructure can have terrible consequences for everyone on the ground.

[1] ISRO fights over 100 cyber attacks every day, reveals chairman Somanath (2023) onmanorama. Available at: https://www.onmanorama.com/news/kerala/2023/10/07/cybersecurity-conference-isro-chief-somanath-on-cyber-attacks.html (Accessed: 24 Feb 2024).

History of the recent past

There have been several incidents in the past that have jeopardized the integrity of sensitive databases. In 2019, The Kudankulam Nuclear Power Plant (KNPP) and the Indian Space Research Organisation (ISRO) were reportedly targets of a cyber-attack or cyber espionage believed to originate from North Korea. The malware used is identified as 'DTrack', associated with the North Korean hacker group Lazarus. The attack raises concerns about the extent of the breach and potential consequences for India's nuclear energy and civilian space programs.[2]

Current Legislations:

The IT Rules and the Information Technology Act, 2000 (ITA) provide protection for private and sensitive data. The ITA comprises within it, the punishments for various cybercrimes. Recently, The Digital Personal Data Protection (DPDP) Act, was passed in August, 2023. Currently, the national organization in charge of handling cybersecurity issues is the Indian Computer Emergency Response Team, or CERT-In. It functions under the direction of the Ministry of Electronics and Information Technology (MeitY) and is essential to maintaining cyberspace security.

There are no thorough national laws controlling activities relating to space in India. Instead, a disjointed collection of policies addresses specific aspects, including satellite communication, remote sensing data, technology transfer, and geospatial policies. In addition, India is a signatory to various space policies, treaties and agreements.

The Indian National Space Promotion and Authorization Center (IN-SPACe) and NewSpace India Limited (NSIL) are two new organizations that are established by the Indian Space Policy 2023 (Space Policy), which also clearly defines ISRO's role as a body dedicated exclusively to research and development. The NSIL is a public sector enterprise in charge of commercializing space technology, whilst the IN-SPACe is intended to serve as a single-window clearing and authorization agency for space launches (by private parties). The Department of Space (DOS) is tasked under the Space Policy with supervising the policy's execution and establishing a procedure for resolving space disputes.

[2] mallik. p. (2019) Cyber attack on Kudankulam Nuclear Power Plant. Available at: https://www.vifindia.org/sites/default/files/cyber-attack-on-kudankulam-nuclear-power-plant.pdf(Accessed: 24 Feb 2024).

Need to establish proper laws and procedures

Cyberattacks and Cybercrime have become frequent and are a relevant issue of the times, especially due to all the rapid technological development in the last two decades. Satellites are more prone to risk than often perceived. It has become much easier to launch cyberattacks by means of malwares and other hacking tools made available on the dark web. Taking into consideration the ease and the geopolitical motivations which a group, organisation or any party may have against another, it becomes extremely crucial to have cyber security experts and a proper framework and procedure in place.

ISRO handles a lot of sensitive data, including mission plans, satellite designs, research results, and vital technical data. To stop data breaches, espionage, and intellectual property theft, it is imperative to guarantee the security, integrity, and availability of this data. Ransomware attacks, data breaches, and virus installation are examples of cyberattacks that affect space infrastructure. Global economies, supply chains, national security, internet access, and communications can all be affected by these assaults. Cyberattacks on space missions can potentially result in property devastation, astronaut injuries or deaths, and a halt to space exploration activities. India's potential to become a major global space power and its role in the Quadrilateral Security Dialogue (Quad) underline the urgency of establishing a robust domestic framework to regulate space activities and sustain momentum in the evolving space industry.

Countermeasures:

A key component of space cybersecurity is maintaining secure communications between space stations and the ground. Putting in place enhanced encryption methods and communication protocols guarantee a secure channel of communication, which is essential for the protection of astronauts, sensitive information, and technology.

Having Access Controls and Mechanisms for Authentication in place will guarantee that only individuals with permission may access vital infrastructure. Cyber threats must be recognized, isolated, and lessened by the infrastructure that is in place, according to intrusion prevention and detection systems. In order to prevent cyberattacks from causing any systemic harm, space missions must use active intrusion detection and threat intelligence.

Conclusion:

India's space law and cybersecurity confluence poses a serious problem that has to be addressed right now with solid answers. As India moves forward with ambitious space projects, it is becoming more and more clear that strict cybersecurity controls are necessary. The lack of a comprehensive legal framework presents difficulties, particularly in light of the prevalence of cyberthreats and the possible geopolitical undertones.