The Outer Space and Cyber-Attacks: How India's Proposed National Space Law Deals with Cyber-Security

Ishita Das[*]

Abstract

The Draft Space Activities Bill, 2017, India's proposed national space law, can cover issues concerning the relationship between the cyberspace and outer space sectors. Lessons can be drawn from the European Union Directive on Security of Network and Information Systems and the United States Internet of Things Cybersecurity Improvement Act in this regard. This research paper aims to throw light on the proposed national space law and ascertain if it is adequate to deal with the challenges concerning this interface.

While Section 1 of the research paper explores the background to India's proposed national space law, Section 2 discusses the relevant laws or policies adopted by different countries to safeguard their space assets from cyber-attacks. Section 3 highlights the challenges and opportunities under the national space law as regards this interface, and finally, Section 4 provides the concluding remarks and suggestions.

Keywords: outer space, cyber-attacks, security, Draft Bill, India

1. Introduction

The relationship between outer space and cyberspace is one that the members of the international community cannot ignore. Cyber security is one of the most crucial challenges that requires the attention of policymakers across the world. Cyber-attacks can be detrimental to critical infrastructure such as power grids, financial systems, transportation networks, water supply systems, and even space assets.[1] Therefore, it is essential to focus on this

* NALSAR University of Law, Hyderabad.

1 Falco G., (2018, July 12) Job one for space force: space asset cybersecurity. Belfer Centre for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/job-one-space-force-space-asset-cybersecurity, (accessed 15 January 22).

interface that may have widespread repercussions for different states by designing appropriate technical solutions and adequate legal and policy frameworks. India has initiated the process of enacting its national space law, the Draft Space Activities Bill, 2017 [hereinafter referred to as the "Draft Bill"]. This Bill can serve as a document for helping the country, and possibly, other nations, deal with the linkage between cyber security and security of the outer space assets efficaciously.

The Draft Bill has been drafted keeping the best interests of the private sector in view and is aligned with India's goals to adhere to the international norms as stipulated in the Outer Space Treaty and other relevant instruments in this domain.[2] The Draft Bill deals with different aspects, including licensing requirements for authorisation of commercial space activities in the country, registration of space objects, liability in cases of damage, and offences and penalties. The Draft Bill makes a clear reference to the Model Law on National Space Legislation [hereinafter referred to as the "Model Law"] as submitted by the International Law Association to the United Nations [hereinafter referred to as the "UN"] Committee on Peaceful Uses of Outer Space [hereinafter referred to as "COPUOS"].[3]

The European Union Directive on Security of Network and Information Systems [hereinafter referred to as the "EU NIS Directive"] and the United States Internet of Things Cybersecurity Improvement Act [hereinafter referred to as the "US IoT Cybersecurity Improvement Act"] can also cover the interface between outer space and cyberspace. The European Union Directive is the first EU-wide directive that has been created to enhance cyber security across all EU members.[4] The US IoT Cybersecurity Improvement Act has been designed to ensure cyber security for all IoT devices.[5] While there are certain differences in how the interface between outer space and cyberspace could be possibly addressed under these three pieces of legislation, there are clear synergies that could contribute towards adopting a more uniform approach as regards addressing challenges associated with this interface. A comparative analysis has been adopted as a part of the next chapter to understand the distinctions and similarities.

It is pertinent for the members of the international community to note that effective space regulation is necessary not only at the international level but also at the domestic level, especially given the new developments in the field

2 Draft Space Activities Bill, 2017, para. 7.
3 Draft Space Activities Bill, 2017, para. 12.
4 European Union Agency for Cyber Security (ENISA). NIS Directive. https://www.enisa.europa.eu/topics/nis-directive, (accessed 15 January 22).
5 United States Congress (Congress.Gov.). HR 1668-Internet of Things Cybersecurity Improvement Act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668, (accessed 15 January 22).

of technology. If the laws cannot keep pace with technological advancements, the challenges will remain.

2. Addressing Cyber Threats: A Comparative Perspective

The EU NIS Directive and the US IoT Cybersecurity Improvement Act have been created to keep pace with the technological developments and deal with the potential challenges posed by cyber-attacks. Countries across the globe need to implement steps towards ensuring cyber security so that the other sectors that are dependent on cyber technologies can be safeguarded. The EU-wide directive was launched in 2016, and various members of the EU adopted it by 2018.[6] The US IoT Cybersecurity Improvement Act came into effect in 2020.[7] Therefore, both the EU NIS Directive and the US IoT Cybersecurity Improvement Act are very recent additions to the legal instruments concerning cyber security.

2.1. Aims of the EU NIS Directive and the US IoT Cybersecurity Improvement Act

The EU NIS Directive aims to address digital threats that the critical infrastructure could be exposed to in order to ensure that the physical safety of the assets is not compromised. The Directive has three major components: (a) *national capabilities*, that is, the different EU Member States must have national capacities to deal with threats arising from breaches of cyber security, by adopting national computer security incident response teams [hereinafter referred to as "CSIRT"], performing cyber exercises, among others, (b) *cross-border collaboration* that is focused on cooperation and collaboration with the other EU Member States, for example, through the EU CSIRT network, and the NIS cooperation group, and finally, (c) *national supervision of critical sectors*, including water supply systems, transportation networks, health, energy, and finance sectors, digital infrastructure, *inter alia*.[8]

Critical infrastructure sectors are no longer 'isolated environments' as, over time, they have become more integrated with technology, more specifically, the Internet.[9] Many of these sectors employ RFID systems, actuators and sensors, industrial equipment, video surveillance cameras, personal

6 European Union Agency for Cyber Security (ENISA). NIS Directive. https://www.enisa.europa.eu/topics/nis-directive, (accessed 15 January 22).

7 United States Congress (Congress.Gov.). HR 1668-Internet of Things Cybersecurity Improvement Act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668, (accessed 15 January 22).

8 European Union Agency for Cyber Security (ENISA). NIS Directive. https://www.enisa.europa.eu/topics/nis-directive, (accessed 15 January 22).

9 B. Genge, I. Kiss, P. Haller, A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures, International Journal of Critical Infrastructure Protection, 10 (2015) 3-17.

computers, and other networking devices.[10] Therefore, the advancement of technology can threaten the physical safety of the critical infrastructure sectors through targeted cyber-physical attacks. Such attacks can cause tremendous physical damage to the sector, having significant economic ramifications for the country concerned.[11] The EU NIS Directive is a significant step towards addressing cyber-security concerns at a regional level. It can play a vital role in ensuring the security of the critical infrastructure sectors reliant on cyber technologies.

The US IoT Cybersecurity Improvement Act aims to establish minimum standards for IoT devices, as owned or controlled by the Federal Government, and for other purposes. As per the law, the National Institute of Standards and Technology [hereinafter referred to as "NIST"] and the Office of Management and Budget [hereinafter referred to as "OMB"] are required to take active steps to improve cyber security in IoT devices. The terminology, 'IoT', refers to the extension of Internet connectivity to physical devices. While the NIST has to develop and review appropriate standards and guidelines, the OMB is stipulated to deal with the review and updating of information security policies and principles based on the NIST standards and guidelines.[12]

Further, as the US IoT Cybersecurity Improvement Act touches upon the interface of cyberspace and physical devices such as critical infrastructure, including smart power grids, transportation networks, and health services, cyber vulnerabilities can have an enormous impact on these IoT-enabled sectors. These sectors may often employ IoT technologies as a part of their critical back-end systems.[13] The IoT devices represent a globally integrated system or network, and therefore, cyber-attacks could be targeted towards critical infrastructure that use cyber technologies for crucial operations. Most IoT devices could be vulnerable to both internal and external attacks that could be very hard for the concerned countries to deal with due to their inherent characteristics. There could be resource constraints as regards IoT computational capabilities, memory, and battery power.[14]

10 B. Galloway, G. Hancke, Introduction to industrial control networks, IEEE Communications Surveys and Tutorials, 15:2 (2013) 860–880.

11 R. Kozik, M. Choras, Current cyber security threats and challenges in critical infrastructures protection, in: Informatics and Applications (ICIA), 2013 Second International Conference on IEEE, 2013, pp. 93–97.

12 United States Congress (Congress.Gov.). HR 1668-Internet of Things Cybersecurity Improvement Act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668, (accessed 15 January 22).

13 I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, J. Lopez, A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services, *IEEE Communications Surveys & Tutorials*, 20: 4 (2018) 3453-3495.

14 M. Abomhara, G. M. Køien, Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks, Journal of Cybersecurity and Mobility, 4:1 (2015) 65-88.

2.2. The EU NIS Directive and the Outer Space Sector

The EU NIS Directive notes at the very outset that with the advancements in technology, the vulnerabilities posed to critical infrastructure sectors have also increased rapidly. It states that such threats can cause significant economic damage to the EU. The Directive notes that the current nature of fragmented approaches among the EU Member States is not sufficient to deal with the challenges stemming from cyber threats. Therefore, a harmonised system could be highly beneficial to the Member States. The Directive imposes an obligation on both the operators of essential services and digital service providers.[15] Article 1 of the Directive unambiguously notes that the Member States are expected to adopt adequate measures to achieve a high uniform level of security of network and information systems.[16]

Article 7 of the EU NIS Directive states that the Member States should adopt appropriate national strategies on the security of network and information systems, focusing on all the sectors identified in Annex II and services covered under Annex III.[17] Annex II lists critical infrastructure sectors such as energy, transport, banking and financial markets, health, drinking water supply systems, and digital infrastructure. Annex III identifies online marketplace, online search engine, and cloud computing services as a part of the services that the Member States would have to focus upon. While outer space has not been recognised as one of the sectors under Annex II, it is vital to bear in mind that the traditional critical infrastructure sectors depend upon outer space assets such as satellites for diverse functions.[18]

For example, Global Positioning System [hereinafter referred to as "GPS"] can contribute towards navigation that is beneficial for the transportation sector, including air, road, rail, and marine transit.[19] The satellites can provide information pertaining to disease patterns that could be very useful for the health sector.[20] The communication sector relies on space infrastructure, and access to such infrastructure is vital for national security missions through the facilitation of command and control, missile guidance, early warning, reconnaissance, and intelligence activities.[21] The space assets

15 EU Directive, art. 5, 6, 7.
16 EU Directive, art. 1.
17 EU Directive, art. 7.
18 EU Directive, Annex II, Annex III.
19 United Nations Office for Outer Space Affairs (UNOOSA). Benefits of space: Transportation. https://www.unoosa.org/oosa/en/benefits-of-space/transportation.html, (accessed 15 January 22).
20 United Nations Office for Outer Space Affairs (UNOOSA). Benefits of space: Global health. https://www.unoosa.org/oosa/en/benefits-of-space/global-health.html, (accessed 15 January 22).
21 United Nations Office for Outer Space Affairs (UNOOSA). Benefits of space: Communication. https://www.unoosa.org/oosa/en/benefits-of-space/communication.html, (accessed 15 January 22).

could also provide information concerning weather patterns used for forecasting operations and could benefit the agricultural sector.[22] Therefore, most of the critical infrastructure sectors identified in Annex II could depend on the outer space assets for crucial functions. Hence, the security of the outer space assets, considering its deep linkage with critical infrastructure sectors, could also be covered by the EU NIS Directive.

An important feature of the EU NIS Directive is the NIS Cooperation Group created for collaborating and sharing information among the EU Member States regarding the implementation of the Directive in their respective territories. The Group is also mandated to provide strategic guidance to the EU CSIRT network. The members of the Group are representatives of relevant national ministries and national agencies in charge of cyber security.[23] The Directive notes that for the Group to be in a position to be effective, all the Member States must have in place basic capabilities to counter challenges associated with cyberspace. The operators of essential services and digital service providers have to adhere to certain security and notification requirements to advance a culture of risk management and reporting of serious instances.[24] The Group can also play a vital role in applying the Directive to outer space assets.

2.3. The US IoT Cybersecurity Improvement Act and Security of the Outer Space

The US IoT Cybersecurity Improvement Act stipulates that it is imperative to ensure the 'highest level of security' at agencies in the executive branch. It also emphasises that such a form of security can only be achieved by collaborating with other relevant sectors comprising industry and academia.[25] The positive benefits of digital technology can be harnessed if the cyber security concerns are addressed 'proactively', especially in relation to the acquisition and operation of IoT devices under the federal government's control. The Act provides that the Director of the NIST shall facilitate the development and publication of standards and guidelines pertaining to appropriate use and management of IoT devices, including specification of minimum information security requirements for managing cybersecurity threats in relation to these devices.[26]

The Director of the NIST should consider the relevant factors for giving effect to the mandate of the Institute under the Act, comprising secure development,

22 United Nations Office for Outer Space Affairs (UNOOSA). Benefits of space: Agriculture. https://www.unoosa.org/oosa/en/benefits-of-space/agriculture.html, (accessed 15 January 22).

23 European Union Agency for Cyber Security (ENISA). NIS Directive. https://www.enisa.europa.eu/topics/nis-directive, (accessed 15 January 22).

24 EU Directive, para. 4.

25 US IoT Cybersecurity Improvement Act, s. 2.

26 US IoT Cybersecurity Improvement Act, s. 4 (a).

identity management, patching, and configuration management of the IoT devices. The US IoT Cybersecurity Improvement Act also provides that the Director of the OMB should facilitate the review of agency information security policies and principles based on the standards and guidelines published by the NIST in connection with the IoT devices. While performing the functions under the Act, the Director of the OMB shall consult with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, *inter alia*.[27] Section 5 of the Act elaborates upon the disclosure requirements concerning security vulnerabilities associated with information systems, including the IoT devices.[28] This piece of legislation is an important addition to resolving the challenges stemming from the interface of the outer-space and cyberspace sectors.

The IoT systems and outer space assets such as satellites are getting increasingly interconnected, and cyber vulnerabilities associated with the IoT devices can pose challenges to such assets. The IoT systems have two major components, (a) system hardware and (b) system software. As hardware and software vulnerabilities could be tricky to fix owing to inherent design flaws, the impact of cyber threats could be very detrimental to such IoT devices. Further, the IoT devices could be more prone to physical attacks that could lead to the unauthorised physical control of the device, extraction of cryptographic information, modification of the programming, and replacement of the device with a malicious device under the control of the perpetrator.[29]

Satellites could be affected by the activities of the perpetrators through different means, and a 'back-door' entry by compromising the IoT devices could be an easy option for them.[30] Cyber-attacks targeted towards IoT devices could include threats involving unauthorised data access and denial of services attacks [hereinafter referred to as "DDOS attacks"].[31] Therefore, given the deep linkage with IoT systems, the US IoT Cybersecurity Improvement Act could potentially cover cyber challenges and how they relate to outer space assets. As satellites may deal with information pertaining to national security interests, it is crucial to frame adequate policy and legal frameworks catering to all the components of the puzzle, including the IoT devices.

27 US IoT Cybersecurity Improvement Act, s. 4 (b).

28 US IoT Cybersecurity Improvement Act, s. 5.

29 M. Abomhara, G. M. Køien, Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks, Journal of Cybersecurity and Mobility, 4:1 (2015) 65-88.

30 T. Stremlau, Safeguarding satellites for a generation, https://www.pipelinepub.com/IoT/satellite-cybersecurity, (accessed 15 January 22).

31 E. Bertino, L. D. Martino, F. Paci, A. C. Squicciarini, Web services threats, vulnerabilities, and countermeasures, in: Security for Web Services and Service-Oriented Architectures, Springer, 2010, pp. 25–44.

3. India's Draft National Space Law and Cyber Security

The Draft Space Activities Bill, 2017, is a remarkable step for India towards encouraging the participation of the private sector in outer space activities. The Department of Space [hereinafter referred to as "DOS"] has been the nodal agency as regards outer space activities in the country for more than five decades and has played an instrumental role in fulfilling India's space ambitions. The Indian Space Research Organization [hereinafter referred to as "ISRO"] was established earlier and was brought under the purview of the DOS later. The ISRO has played a crucial role in fulfilling India's space ambitions and maintains a large fleet of communication satellites and remote sensing satellites for different purposes such as fast and reliable communication and earth observation, respectively.

3.1. The Genesis of India's Space Programme and the Draft Bill

The space research activities in the country started around the 1960s, when the Tokyo Olympics exhibited the potential of space technologies. The founding father of the Indian space programme, Dr. Vikram Sarabhai, established the Indian National Committee for Space Research [hereinafter referred to as "INCOSPAR"] in 1962 under the Department of Atomic Energy. Under the guidance of the visionary Dr. Sarabhai, the INCOSPAR set up the Thumba Equatorial Rocket Launching Station in Thiruvananthapuram for upper atmospheric research. The ISRO was established in 1969 to further India's space-based services and promote the development of space technology for the benefit of the country.[32]

Subsequently, the Government of India constituted the Space Commission and established the DOS in June 1972. The ISRO was brought under the aegis of the DOS in September 1972. The ISRO, apart from dealing with communication and earth observation, deals with space-based applications concerning weather forecasting, disaster management, Geographic Information Systems [hereinafter referred to as "GIS"], cartography, telemedicine, dedicated distance education or learning, among others. Through the ISRO and its various research and development [hereinafter referred to as "R&D"] centres, the DOS has executed and launched satellites and launch vehicle projects. It has also conceptualised and created several space-based applications for the country's benefit.[33]

While the DOS has played a key role in the drafting of the policies such as the Satellite Communication [hereinafter referred to as "SATCOM"] and the Remote Sensing policies, there is no national space law that pertains to the regulation of space activities in the country. Therefore, the Draft Space

32 Indian Space Research Organization (ISRO). About ISRO, https://www.isro.gov.in/about-isro (accessed 15 January 22).

33 Indian Space Research Organization (ISRO). About ISRO, https://www.isro.gov.in/about-isro (accessed 15 January 22).

Activities Bill, 2017, was introduced by the DOS to enhance the growth of the space sector while aligning with India's obligations under the international space law instruments such as the UN treaties. The Bill makes a clear reference to the UN COPUOS and emphasises the role of the intergovernmental committee towards space governance at the international level.[34] The Draft Bill, if implemented as law in the near future, could change the regulatory landscape concerning the space sector in India.

3.2. Definitional Conundrum under the Draft Bill

The Draft Bill is a very concise piece of legislation, and hence, there are not many definitions in the current draft as available in the public domain. Some of the definitions covered under the Draft Bill include 'commercial space activity', 'licence', 'person', 'space activity', and 'space object'. 'Commercial space activity' refers to space activities that can generate profit or revenue.[35] Therefore, such activities cover space programmes that are of commercial nature. The stipulation of this definition is in synergy with the goals of the Draft Bill, wherein it seeks to encourage the participation and involvement of the private sector in outer space endeavours. Further, the definition of 'licence' refers to Clause 7 (1) of the Bill wherein persons engaged in commercial space activity may seek authorisation by way of licence from the Central Government.[36]

The definition of 'person' under the Bill includes an individual, company, trust, Hindu Undivided Family, partnership, limited liability partnership or any other entity established under any law for the time being in force.[37] It is interesting to note that Clause 6 (2) of the Bill allows the Central Government to grant exemptions from the specified licensing requirements to certain persons if it deems it fit that the requirements are not necessary to secure compliance with international obligations.[38] While more clarity pertaining to exemptions is desirable, this provision highlights India's intentions to adhere to the international norms governing the outer space sector.

Further, Clause 7 (2) emphasises that no licence would be granted if the space activity (a) could adversely affect public health, the safety of individuals or property, (b) is inconsistent with India's international obligations, and (c) compromises the sovereignty and integrity of India, security of State, defence of India, friendly relation with foreign States, public order, decency, or morality.[39] While Clause 7 (2) considers India's international obligations, it does not take into account those space activities that could be harmful to the

34 Draft Space Activities Bill, 2017, Explanatory Note, paragraph I.5.
35 Draft Space Activities Bill, 2017, clause 2 (a).
36 Draft Space Activities Bill, 2017, clause 7 (1).
37 Draft Space Activities Bill, 2017, clause 2 (d).
38 Draft Space Activities Bill, 2017, clause 6 (2).
39 Draft Space Activities Bill, 2017, clause 7 (2).

outer space environment expressly. Article IX of the Outer Space Treaty provides that the parties shall avoid the 'harmful contamination' of the outer space environment while conducting space activities.[40]

The definition of 'space activity' includes the launch, use, operation, guidance, and entry of space objects into and from outer space and all functions for performing these activities, including the procurement of the objects for such purposes.[41] While the definition of 'space activity' under the Draft Bill is fairly comprehensive, it could have covered other aspects such as 'use of territory or facility of India for any launch'. Lack of clarity concerning such important components could be problematic as any operator could use a foreign territory to launch a satellite without seeking due permission from India.[42] Therefore, it is crucial for India's national space law to provide the scope of application regarding territorial boundaries.

'Space object' under the Draft Bill, is used to refer to (i) launching of any object on an orbital trajectory around the earth or to a destination beyond the earth orbit or (ii) any device, the purpose of which is to launch a space object on a trajectory even when such a device is operated without payload for its development and validation phase.[43] This definition is aligned with the definition of 'space object' under the Liability Convention and the Registration Convention. It is interesting to note that while Clause 1 (2) of the Draft Bill refers to space objects of 'Indian origin'[44], it has not defined what constitutes 'Indian origin'. However, a major omission as regards definitions is 'damage' as provided under Article I of the Liability Convention.[45] The absence of the definition of 'damage' or 'loss' gives rise to a definitional conundrum as there is a lack of clarity as regards what these terminologies, as employed under Clause 12 of the Draft Bill, could cover.

3.3. Damage caused by Cyber-attacks can be covered under the Draft Bill

Clause 12 of the Draft Bill deals with liability for damage arising out of commercial space activities. It specifies that a licensee under the Bill must indemnify the Central Government for any claims brought against the Government in relation to damage or loss arising out of its commercial space activity or concerning a space object covered under the licence. The Central Government would determine the quantum of liability that would be imposed on the licensee.[46] Therefore, as the clause does not elaborate upon the nature of 'damage' or 'loss' that could be caused as a result of commercial

40 Outer Space Treaty, art. IX.
41 Draft Space Activities Bill, 2017, clause 2 (f).
42 U. Dasgupta, Do national space laws look beyond liability for damage? The case of India, International Institute of Space Law, 1 (2018).
43 Draft Space Activities Bill, 2017, clause 2 (g).
44 Draft Space Activities Bill, 2017, clause 1 (2).
45 Liability Convention, art. I (a).
46 Draft Space Activities Bill, 2017, clause 12.

space activities or in relation to a space object, it may cover damage or loss caused by cyber vulnerabilities. Further, the Draft Bill clearly emphasises that policies 'in the interests of national security' should be pursued.[47] As cyber security breaches may affect space assets, and in turn, national security, it may cover this interface within its scope.

Cyber-attacks can cause damage to a space asset over a spectrum, starting from minimal or no damage to extensive damage. They may manifest in the form of data interception or monitoring, data corruption, and even loss of control of the concerned space asset. While in the cases of data interception or corruption, there may be no collateral damage as regards the targeted space asset, if there is a seizure of control, it may render the target satellite disabled and uncontrollable.[48] Maximum damage can be caused if the perpetrator takes control of the satellite and uses that to collide with another functional satellite, which, in turn, would have very serious repercussions for the outer space environment.[49] Therefore, India must address challenges stemming from the interface between the outer space and cyberspace domains.

Clause 16 of the Draft Bill deals with punishment for causing damage or pollution to the environment. It provides that any person who causes damage or pollution to the outer space environment would be held accountable for the space activities that result in such damage.[50] This provision can include physical damage caused by space activities wherein the perpetrator uses cyber-attacks to gain control over a space asset and engage in the act of collision with another satellite, thereby causing damage to the outer space environment.[51] Once the Draft Bill is enacted and the different provisions are invoked, one would gain more clarity on how damage could be construed in the Indian scenario.

4. Conclusion

India's Draft Space Activities Bill, 2017, is still in its nascent stage, and the Bill was released into the public domain by the DOS for seeking public opinion from relevant experts in this field. Assuming that the DOS has

47 Draft Space Activities Bill, 2017, clause 3 (a).

48 T. Harrison, K. Johnson, T. G. Roberts, T. Way, M. Young, Space threat assessment 2020, March 2020, https://aerospace.csis.org/wp-content/uploads/2020/03/Harrison_SpaceThreatAssessment20_WEB_FINAL-min.pdf (accessed 15 January 22).

49 J. Kallberg. Designer satellite collisions from covert cyber war, Strategic Studies Quarterly (2012) 124-136.

50 Draft Space Activities Bill, 2017, clause 16.

51 I. Das, The outer space and cyber-attacks: Attributing responsibility under international space law, IAC-20-E7.4.7, 71st International Astronautical Congress, online, 2020, 12-14 October.

received comments from across the country, and possibly, from across the world, the new version of the Bill would hopefully take into account the feedback of the relevant stakeholders. Therefore, as the author has access to the original text of the Draft Bill, there could be a slight disconnect as regards analysis depending on how the new provisions and legal terms appear in the final text. However, as the Draft Bill is a work in progress, it should evolve for the benefit of the country with time.

The Draft Bill has immense potential for positioning India as one of the countries focused on effective space regulation at the domestic level, and if India incorporates and tries to address issues such as the impact of cyber-attacks on space assets and liability in this regard, under the Draft Bill, it could set an example for other countries. The author would like to take this opportunity to convey to the policymakers and the relevant experts associated with the Draft Space Activities Bill, 2017, to pave the way for addressing new forms of challenges that could face the outer space sector in India, including but not restricted to cyber threats.