Outer Space and Cyber-Attacks

Attributing Responsibility under International Space Law

*Ishita Das**

Abstract

The linkages between the two domains of outer space and cyberspace are deepening with the commercialization of outer space and the deployment of an increasing number of satellites delivering communications, navigation, and military services. However, the vulnerabilities stemming from this relationship are yet to be addressed in a comprehensive manner. While there is no policy that specifically addresses this interface, International Space Law can deal with the problems arising in this regard.

Article VI of the Outer Space Treaty deals with 'international responsibility'. However, this relationship was not considered when the treaty was drafted back in the 1960s. Cyber-attacks may affect the space assets by interfering with (a) 'flight control' and (b) 'payload control'. While with regard to the former scenario, the launching state may be held responsible for activities that cause damage to the surface of the Earth, in relation to the latter, the provisions of the Outer Space Treaty and the Liability Convention cannot really be invoked.

The aim of this research paper is essentially fourfold: (1) provide a background to the interface of the outer space and cyberspace, especially in view of the rise in commercialization; (2) discuss how cyber-attacks affecting space assets may be dealt with under the Outer Space Treaty and the Liability Convention; (3) explore the challenges as regards determination of responsibility in the context of life cycles of the space assets and multiple parties and finally, (4) provide the concluding remarks and suggestions.

Keywords: outer space, cyber-attacks, responsibility, International Space Law

1. Introduction

The outer space and the cyberspace are intricately connected and the ability of the latter to adversely affect the former is enormous. Cyber-attacks on critical infrastructure sectors such as agriculture, defence, electrical grid,

* Ishita Das, NALSAR University of Law, Hyderabad, India.

financial services, transportation systems, and water networks can cause tremendous economic damage to the concerned state. This problem would only compound if the space systems, that several of these sectors depend upon, are compromised due to cyber interference. For instance, the agriculture sector relies on the weather and climate information from the satellites to make appropriate decisions, the defence sector uses the services rendered by the intelligence satellites, and the transportation sector utilises the information concerning the Global Positioning System ("GPS"), among others.

While the cybersecurity of critical infrastructure systems is given increasing priority, the same may not be true for the space systems. Further, as the complexity of ownership, management, and operations involving the space sector makes it difficult to attribute liability as far as cyber-attacks are concerned, it is imperative to come up with effective solutions to deal with the challenges that stem from the relationship between the outer space and cyberspace. While certain international legal frameworks and documents may assist the international community in navigating through the problems, the current instruments are not adequate to address the threats posed to space infrastructure due to cyber-attacks.

Cyber-attacks may cause damage not only to the satellite targeted by the perpetrators but also other satellites that it may collide with following the cyber interference. Cyber-attacks may affect the space assets by compromising the safety-related flight controls and also other non-safety systems such as payload control that may cause significant economic damage to the state concerned. For example, if the cyber-attacks interfere with the payload's communication and navigation functions, it may harm the on-board applications in the satellite. Therefore, the perpetrators could try to compromise the 'flight control' and/or 'payload control' of the satellite.

International Space Law has certain instruments such as the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies ("Outer Space Treaty") and the Convention on International Liability for Damage Caused by Space Objects ("Liability Convention") that contain provisions regarding international responsibility and liability for damage caused by space objects. Article VI of the Outer Space Treaty specifies that the state party bears international responsibility for activities carried out in the outer space, both governmental and non-governmental.[1] Further, Article II of the Liability Convention provides that the launching state would be liable for damage

1 United Nations Office for Outer Space Affairs (UNOOSA): Treaty on principles governing the activities of states in the exploration and use of outer space, including the moon and other celestial bodies ("Outer Space Treaty") 1966, art. VI. Https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html, (accessed 02.02.21).

caused to the surface of the Earth.[2] Therefore, due to attribution issues associated with cyber-attacks on space assets, an unfair burden may be placed on the launching state from whose satellite the damage is caused.
While certain non-binding documents may address the problems stemming from the relationship between the outer space and cyberspace such as the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations ["Tallinn Manual 2.0"] the focus of this research paper is on the international legal frameworks under International Space Law. The section below explores the inadequacy of the Outer Space Treaty and the Liability Convention to deal with the challenges arising from cyber interference with space assets.

2. The Inadequacy of the Existing International Legal Instruments Concerning the Outer Space

The main international legal instruments as regards the outer space comprise the Outer Space Treaty, the Liability Convention, the Convention on Registration of Objects Launched into Outer Space ("Registration Convention"), the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space ("Rescue Agreement"), and the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies ("Moon Agreement"). The United Nations Committee on the Peaceful Uses of the Outer Space ("UNCOPUOS") has concluded these five international instruments that deal with various issues including (a) the freedom of exploration of the outer space; (b) the non-appropriation of outer space by any nation; (c) liability for damage caused by 'space objects'; (d) arms control, and (e) prevention of 'harmful interference' with the space activities and the environment. These international instruments emphasise that the benefits stemming from space activities should be utilised for the well-being of humankind and for strengthening international cooperation.[3]
Cyber-attacks that are targeted to impair a state's ability as regards the provision of space services can violate the state's freedom of exploration and use of outer space for the benefit of its citizens. As the outer space is the broader domain that seeks to maintain environmental security, food security, and national security of the states, the security of the outer space services

2 United Nations Office for Outer Space Affairs (UNOOSA): Convention on International Liability for Damage Caused by Space Objects ("Liability Convention") 1971, art. II. Https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html, (accessed 02.02.21).

3 United Nations Office for Outer Space Affairs (UNOOSA). Space law treaties and principles. Https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html, (accessed 02.02.21).

sector is paramount.[4] Further, the outer space is not amenable to any claim of appropriation by any state.[5] However, each state exercises sovereignty over its space objects.[6] Therefore, will there be a breach of sovereignty upon intercepting or stealing of information from another state's satellite through cyber-attacks? This question demands more clarity regarding the interface between the outer space and cyberspace.

Both the Outer Space Treaty and the Liability Convention contain provisions that deal with damage caused by 'space objects'. However, what if a space asset is attacked remotely from Earth, without utilising any space object to cause damage? Therefore, it is imperative at this stage to understand the meaning of the term 'space object' as provided in the Liability Convention. Article I of the Convention stipulates that 'space object' essentially comprises the component parts of the space object and the launch vehicle.[7] A reading of this definition points out the clear definitional problem that exists in the current International Space Law instruments.

Article IX of the Outer Space Treaty specifies that the nations should refrain from causing 'harmful interference' with the space activities and the environment.[8] While Article IX, arguably, may never have been invoked formally for dealing with cyber-attacks on satellites or jamming of satellites,[9] the use of similar terms by the International Telecommunication Union ("ITU") in their Constitution, the Convention and the Radio Regulations could be useful in this regard. The ITU requires the states to respect each other's right to use the radio-frequency spectrum and to exercise this right without causing 'harmful interference' with the others. While this terminology is fairly clear and covers radio-communication satellites, the language employed by Article IX of the Outer Space Treaty is still quite vague. The relevant provisions concerning the relationship between the outer space and cyberspace, as contained in the Outer Space Treaty and the Liability Convention, have been discussed below in detail.

2.1. The Outer Space Treaty

Article IV of the Outer Space Treaty prohibits weaponisation of the outer space wherein nuclear weapons and weapons that are capable of mass

4 Gärtner, H., Duhamel, E., et al (2009) 2 Security. In: Schrogl, K.U., Mathieu, C., et al (eds.) Threats, risks and sustainability-answers by space: studies in space policy. Springer, Vienna, p.249; Rajagopalan RP & Porras DA (2015) Cyber arms race in space: exploring India's next steps. ORF Issue Brief 113:2.

5 Outer Space Treaty, art. II.

6 Outer Space Treaty, art. VIII.

7 Liability Convention, art. I.

8 Outer Space Treaty, art. IX.

9 Kallender, P.K., (2014) Waking up to a new threat: cyber threats and space. Transactions of the Japan Society for Aeronautical and Space Sciences, Aerospace Technology Japan 12(29):Tv_9.

destruction are not to be placed in the orbit around the Earth. The installation of such weapons on celestial bodies and the stationing of the same in outer space is also prohibited.[10] Most of the states regard these activities as illegal as they violate the basic principles of Public International Law, in general, and International Space Law, in particular.[11] However, with the advancement of technological innovation, especially cyberspace, several commentators have expressed fear about the possibility of weaponisation of outer space when cyber-attacks target certain space assets.[12]

Paragraph 2 of Article IV specifies that the states shall use the Moon and other celestial bodies only for 'peaceful purposes'. The testing of any type of weapon is prohibited on the celestial bodies. However, what about anti-satellite ("ASAT") operations that are conducted in the outer space? Many scholars argue that the Outer Space Treaty does not prohibit the military use of outer space, as long as weapons are not deployed.[13] Further, the term 'peaceful' should be interpreted to mean 'non-aggressive'.[14] Therefore, the deployment of non-nuclear based ASATs may not be prohibited.[15] As a result of this grey area, several states have conducted ASAT operations, affecting the space environment adversely.

This interpretative conundrum shows the gaps that exist in the Outer Space Treaty and how inadequate the international instrument is to deal with more advanced forms of technologies concerning the cyberspace. Further, the Outer Space Treaty has not defined 'space weapons'. Broadly, space weapons may include space systems that are capable of interfering with, destroying or damaging space assets,[16] and narrowly, they may include a space system that

10 Outer Space Treaty, art. IV.

11 Cheng, B., (1997) Studies in international space law. Clarendon Press, Oxford, p.515; Tronchetti, F., (2012) A soft law approach to prevent the weaponisation of outer space. In: Marboe, I., (ed.) Soft law in outer space: the function of non-binding norms in international space law. Böhlau Verlag Vienna, p.365.

12 Su, J., (2010) Use of outer space for peaceful purposes: non-militarization, non-aggression and prevention of weaponization. Journal of Space Law 36(1):265; Ness PV (2010) The time has come for a treaty to ban weapons in space. Asian Perspective 34(3):215.

13 Soucek, A., (2011) International law. In Brünner, C., Soucek, A., (eds.) Outer space in society, politics and law. Springer-Verlag Vienna, p.318; Sheehan, M.J., (2007) The international politics of space. Routledge Chapman and Hall New York, p.2.

14 Lyall, F., Larsen, P.B., (2009) Space law: a treatise. Ashgate, Surrey, p.524; Su, J., (2010) Use of outer space for peaceful purposes: non-militarization, non-aggression and prevention of weaponization. Journal of Space Law 36(1):260-265.

15 Cheng, B., (1997) Studies in international space law. Clarendon Press, Oxford, p.515.

16 Tronchetti, F., (2012) A soft law approach to prevent the weaponisation of outer space. In: Marboe, I., (ed.) Soft law in outer space: the function of non-binding norms in international space law. Böhlau Verlag Vienna, pp.363-364; Duberti, G.J., (2011) The legality of space weapons in international law. Proceedings of the International Institute of Space Law 81.

has a specific goal to target another space object.[17] Even though more inclusive definitions have been proposed that cover both terrestrial and space-based systems,[18] the definitional problem of a space weapon still exists.
Articles VI and VII of the Outer Space Treaty deal with 'international responsibility' and 'international liability', respectively, wherein the concerned state party is responsible or liable for the damage caused.[19] However, if the perpetrator has masked the geographical location and carried out the cyber-attack anonymously or launched the attack on the space asset from drone computer systems situated in another country,[20] how will the perpetrator be traced? Therefore, traceability and attribution are challenges that face the international community as regards cyberspace. The problem becomes more complicated when such cyber perpetrators target the space assets, especially the ones that perform vital functions for the respective states.

2.2. The Liability Convention

Article I of the Liability Convention provides some important definitions comprising 'damage' and 'launching state' apart from 'space object' that has been discussed earlier. The term 'damage' covers loss of human life, or injury to persons, or affects the health of humans adversely, or loss or damage caused to the property owned by natural persons, juridical persons, states, or international organisations. Perpetrators may use cyber-attacks to target critical infrastructures such as nuclear centrifuges, electric grids, water supply systems, aviation defence systems, commercial systems, transportation networks, the financial sector, and agriculture.[21] Therefore, physical damage can be caused by using cyberspace maliciously.[22] However, the treatment of the space sector as critical infrastructure is still unsettled.

17 Tronchetti, F., (2012) A soft law approach to prevent the weaponisation of outer space. In: Marboe, I., (ed.) Soft law in outer space: the function of non-binding norms in international space law. Böhlau Verlag Vienna, p.364; Su, J., (2010) Use of outer space for peaceful purposes: non-militarization, non-aggression and prevention of weaponization. Journal of Space Law 36(1):265.

18 Mineiro, M.C., (2008) The United States and the legality of outer space weaponization: a proposal for greater transparency and a dispute resolution mechanism. Annals of Air and Space Law 33:448.

19 Outer Space Treaty, arts VI and VII.

20 Yannakogeorgos, P.A., (2016) Strategies for resolving the cyber attribution challenge. Perspectives on Cyber Power. Air Force Research Institute, pp.12-15.

21 Hsieh, L., (2018, April 2) Insight: US insurers grapple with physical risks from cyberattacks. Reuters. Https://www.reuters.com/article/bc-finreg-cyber-risks-physical-risks/insight-u-s-insurers-grapple-with-physical-risks-from-cyber-attacks-idUSKCN1H 91EH, (accessed 02.02.21).

22 Hathaway, O.A., Crootof, R., et al (2012) The law of cyber-attack. California Law Review 100(4):817.

Most of the critical infrastructures identified above depend on space systems for a variety of operations such as global communications, scientific discovery, and intelligence information, inter alia. Therefore, if the space systems are compromised by cyber-attacks, it could create several challenges for these critical infrastructures by providing a 'backdoor' entry to their systems.[23] The United States ("US") and the European Union ("EU") have pushed for the development of critical infrastructure protection policy mechanisms for their space sectors.[24] While the policy instruments are not comprehensive, they reflect a rather urgent need to take action in this area more seriously.

Damage can also be caused by way of 'space debris'. If cyber-attacks are used to create a collision between two satellites, they may create debris that could potentially damage other healthy satellites, and endanger the lives of the persons working in the International Space Station ("ISS"). While the ISS has designed ways to protect its astronauts and cosmonauts if debris has been tracked close to the station,[25] while also engaging in manoeuvres to avoid being hit by the debris,[26] one cannot be certain about the safety of the human lives aboard the ISS. For instance, as Kessler explains, the ISS does manoeuvres if it feels that the space debris is too close for comfort. It cannot predict if there will be a collision with space debris.[27]

However, if the collision created by the cyber-attacks were to trigger the Kessler Syndrome, the damage could cause unprecedented problems for the space industry. The Kessler Syndrome, essentially, is the chain reaction that could be initiated when a high-velocity collision of satellites occurs.[28] This would also cause a serious impact on the outer space environment. There are currently no concrete laws as regards space debris and the international community still has their 'heads in the sand' regarding the safety of space

23 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 02.02.21).

24 Hesse, M., Hornung, M., (2015) Space as critical infrastructure. In: Schrogl, K.U., Hays, P., et al (eds.) Handbook of space security. Springer New York, p.187.

25 Khlystov, N., (2018, April 3) We have a space debris problem: here's how to solve it. World Economic Forum. Https://www.weforum.org/agenda/2018/04/we-have-a-space-debris-problem-heres-how-to-solve-it/, (accessed 02.02.21).

26 Hall, L., (2014) The history of space debris. Space Traffic Management Conference. Https://commons.erau.edu/cgi/viewcontent.cgi?article=1000&context=stm, (accessed 02.02.21).

27 Torbet, G., (2019, October 24) We're slowly trapping ourselves under an umbrella of space junk. Digital Trends. Https://www.digitaltrends.com/cool-tech/kessler-syndrome-space-junk-trap-earth/, (accessed 02.02.21).

28 Kessler, D.K., Cour-Palais, B.G., (1978) Collision frequency of artificial satellites: the creation of a debris belt. Journal of Geophysical Research 87:2637.

assets.[29] Therefore, the question of taking the interface of cyberspace and outer space seriously might seem ambitious, but it is necessary.

Another challenge that faces the international community relates to the issue of attributing liability. The sub-section above has already explored the relevant provisions stipulated in the Outer Space Treaty. As far as the Liability Convention is concerned, there is a problem with the definition of 'launching state'. Essentially, Articles II and III of the Convention provide for absolute and fault-based liability, respectively, if the damage is caused by the launching state's space object. However, this definition does not give due regard to the extraneous factors that may trigger damage to a particular country's space object. Given the complexity of tracing the actual perpetrator, an innocent launching state, whose space object has been compromised, maybe pinned with liability while the perpetrator escapes any form of attribution altogether.[30] Therefore, there exists the 'launching state' definitional problem. With the commercialisation of the space sector, the challenge of attributing liability would only get more complex. The next section explores the technical aspects concerning the attribution of liability upon cyber interference with space assets.

3. Technical Aspects Associated With Attributing Liability

Cyber activities may interfere with three segments of space operations: (a) space-based, (b) terrestrial-based, and (c) peripheral systems. The perpetrators may get unauthorised access to the space-based segment through the use of malware that affects the on-board computer systems. Further, they may retrieve information from the payload of a space object, interfere with the transmission of information, or manipulate its flight control in a manner that could be detrimental to the space object itself or other space objects. The perpetrators may affect the terrestrial-based systems by getting unauthorised access to the ground stations that maintain contact with the space objects from the Earth. They may affect the peripheral systems by interfering with the links with the various satellite integrators, space agencies, space debris databases, and conjunction assessment centres.[31]

29 Fidler, D., (2018, April 3) Cybersecurity and the new era of space activities. Council of Foreign Relations. Https://www.cfr.org/report/cybersecurity-and-new-era-space-activities, (accessed 02.02.21).

30 Kehrer, T., (2019) Closing the liability loophole: the liability convention and the future of conflict in space. Chicago Journal of International Law 20(1):192-195.

31 Kaiser, S.A., Mejia-Kaiser, M., (2015) Cyber security in air and space law. Zeitschrift für Luft- und Weltraumrecht German Journal of Air and Space Law 64(2):404-405.

3.1. 'Flight Control' and 'Payload Control'

Unauthorised cyber interference with a space object may be conducted in two ways: (1) affecting the 'flight control' and (2) affecting the 'payload control'. Unauthorised access to the 'flight control' of a space object may result from interference with the space-based, terrestrial-based, and peripheral systems. If this cyber interference causes damage on the surface of the Earth to the launching state or another launching state, the launching state could be held responsible under Article VI of the Outer Space Treaty and could be liable to pay compensation under the Liability Convention. Therefore, the launching state would have to bear the costs of the damage that were a result of cyber activities it never authorised.

Unauthorised access to the 'payload control' of a space object can take place by interfering with the payload information in the form of communication, navigation or remote sensing signals. However, unlike the 'flight control' that can be covered under the Outer Space Treaty and the Liability Convention, interference with the 'payload control' does not really fall within the scope of application of either the Outer Space Treaty or the Liability Convention. This is because the payload signals do not necessarily have a direct physical impact on the space object. Interference with the payload signals can cause significant damage to the state utilising the satellite's services, and therefore, it is a serious challenge that remains to be addressed effectively.

3.2. Recognising Space Assets as Part of Critical Infrastructure

The recognition of space assets as 'critical infrastructure' is still a very slow process and the complexity of the supply chains concerning the space assets makes it challenging to attribute responsibility. The life cycles of the space assets may rest with multiple parties such as the developers, the operators, the owners, and the users, making it extremely difficult to determine the operational and financial responsibility in those instances where cyber-attacks affect these assets. With the advancement of technology, the problems in this area are only going to compound and, therefore, it is imperative to focus on resolving these issues. Moreover, unlike other critical infrastructure sectors, the management of the space sector may not rest with the owners making it all the more crucial to recognise this as one of the critical infrastructure sectors.

For example, let us take a hypothetical scenario wherein P, the owner, commissions the development of the satellite to Q who assumes the cybersecurity responsibility, and Q further commissions the development of specific components of the satellite to R, S, and T who are in charge of the cybersecurity technologies in their components. After Q finishes the delivery of the satellite to the owner, another company, U, may then assume operational responsibility of the satellite including its cybersecurity. U, in turn, may hire V who takes charge of the launching of the satellite, comprising its cybersecurity operations.

V may have to get insurance cover for the launch that would be provided by the insurance firm, W. Once the satellite is launched, enters orbit and becomes operational, U would manage the operations of the satellite, including its cybersecurity operations. For economic interests, P may lease the use of bandwidth or processing to other stakeholders such as X, Y and Z. Therefore, the multi-party involvement as regards the space sector makes it difficult to attribute responsibility to just one stakeholder. As different stakeholders may take charge of cybersecurity at different stages of the satellite development, launch, and operation, this complex network may be exploited by the perpetrators to launch cyber-attacks on the satellite concerned.

Coupled with the above-mentioned challenge, the life cycle of technologies deployed in the space sector is very different from the technologies used in other critical infrastructure sectors. For instance, a satellite may have to serve a specific function for a decade or so, indicating that if the security issues are not addressed adequately it could lead to catastrophic outcomes upon its compromise.[32] If the technologies used in the satellite and the ground system become obsolete it would be more prone to cyber-attacks due to legacy problems. It would be very hard to keep the satellite safe from the cyber perpetrators whose attacks are only getting more nuanced with the rapid advancement of technological innovation. With more developing nations interested in launching space missions commercially, the costs of not investing enough in terms of cybersecurity could pose dangerous threats in the future.[33]

4. Conclusion

The author has explored the relationship between the two domains of cyberspace and outer space and explained how cyber-attacks can have an adverse impact on space assets. The international community has taken some huge strides as far as the outer space is concerned and designed legally-binding international instruments such as the Outer Space Treaty and the Liability Convention. However, due to the complexities associated with the cyber domain, the multilateral actions have not yielded similar results. There is no binding international legal instrument as regards the cyberspace.[34]

32 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 02.02.21).

33 Livingstone, D., Lewis, P., (2016, September 22) Space, the final frontier for cybersecurity?. Chatham House. Https://reader.chathamhouse.org/space-final-frontier-cybersecurity#, (accessed 02.02.21).

34 Legris, E., Walas, D., (2018) Regulation of cyberspace by international law: reflection on need and methods. ESIL Reflection. Https://esil-sedi.eu/fr/esil-reflection-regulation-of-cyberspace-by-international-law/, (accessed 02.02.21).

As the international legal instruments concerning outer space were drafted during the 1960s-70s, the threats that could be posed by cyberspace were unimaginable. Hence, the relevant provisions of the Outer Space Treaty and the Liability Convention are not adequate to deal with the unique nature of the problems presented by cyberspace. Further, while International Space Law has been found to be applicable to cyberspace, the relevant international legal instruments would not cover all aspects of the challenges posed by cyber operations. The Tallinn Manual 2.0 addresses the interface between cyber operations and the outer space explicitly but does not expound on detailed guidelines that would benefit the international community.

Therefore, there is a need to rethink the current international legal instruments that could assist in dealing with the challenges presented by cyber-attacks on space assets. It is imperative to come up with a binding international agreement that recognises the relationship between the outer space and cyberspace and provides solutions to address the problems that could result from unauthorised cyber interference on space assets. The new agreement, formulated under the supervision of the UNCOPUOS, would deal with the definitional problems regarding 'space weapon' and the 'launching state', provide for an effective liability system for cyber interference with space assets, and finally, recognise the space sector as one of the critical infrastructure sectors. This international legal framework is the need of the hour in the contemporary setting.