SUPREMO AMICUS

VOLUME 20 ISSN 2456-9704

CYBER-ATTACKS IN OUTER SPACE: A STUDY

By *Vasudha Krishnamurthy*

ABSTRACT

Space infrastructure, today, is relevant in almost all national and international spheres. These space systems function with the help of cyber technologies, and because of this symbiotic relationship shared between the internet and the outer space, Cyber-attacks has become a growing concern in outer space. Much of the world's critical infrastructure – such as communications, air transport, maritime trade, financial and other business services, weather and environmental monitoring and defence systems – depends on the space infrastructure, including satellites, ground stations and data links at national, regional and international levels.[1] In the present era of outer space activities, it is important that we have an efficient and effective cybersecurity regime that extends not only to the Earth, but beyond as well. We can protect the space system if we understand the cyber vulnerabilities and its effect on such systems.Cyberattacks on satellites can include jamming, spoofing and hacking attacks on communication networks; targeting control systems or mission packages; and attacks on the ground infrastructure such as satellite control centres.[2]Regulating cyber attacks is a challenge to us, especially since we lack a strong enough cyber law and space law regime to tackle the said issue. This paper attempts to analyse the legal regime relating to increase in the militarization and commercialization of outer space in the era where we can witness increased cyber-attacks on space systems. It also attempts to highlight the concept of cyber attacks in outer space, and highlight the inadequacies of the present law in dealing with such instances.It addresses the need to craft a legislation to exclusively deal with such commercial space activities. It further addresses the issue of state responsibility for such cyber attacks and also the response of the states to such attacks. Countries have managed to co-operate with each other by agreeing upon peaceful uses of outer space and banning weapons of mass destruction and the same must be followed by various private players and governmental organizations. They must collaborate on the issue of outer space cyber security policies to arrive on a comprehensive strategy. This paper, finally suggests a proposed framework to govern cyber attacks in the outer space.

1. INTRODUCTION

Space infrastructure, today, is significant in almost all national and international spheres. They function with the support of cyber technologies, and because of this symbiotic relationship shared between the internet and the outer space, Cyber-attacks, which take place either on or through the cyberspace has become a growing concern in space. Much of the world's critical infrastructure – such as communications, air transport, maritime trade, financial and other business services, weather and environmental monitoring and defense systems – depends on the space

[1] Chatham House, The Royal institute of International affairs: Space, the Final Frontier for Cybersecurity?, para 1.

[2] Synergia Foundation:China-based hacking group targets satellites, para 3

infrastructure, including satellites, ground stations and data links at national, regional and international levels.[3] The problem with cyber-attacks is tracing the source of the attack and attributing territorial sovereignty to it, considering absenteeism of physical boundaries. Kristen E, has mentioned the three generations of sovereignty in her paper.[4]The first, where sovereignty over the Internet belonged to its users, not to governments. The second, where scholars argued that states should regulate the Internet and the third where emphasis was given on how cyber governance cannot be solved by or within a single state and needs international coordination. We are presently at the situation where regulation of cyberspace activities needs global attention and not just domestic legislations. The most crucial concern about such an attack is attribution of responsibility to the perpetrator of the attack, whether it is the state or an individual. Another important aspect is to extend the existing legal regime to these attacks in outer space in an era of space haves and have nots, where states with technological dominance are trying to control activities of the other states. Cyberspace and Outer space cannot be regulated in separate spheres, particularly in this era where they exhibit a symbiotic relationship. All cyber activities are based on space enabled communications and the Space activities rely on internet based communication networks. This paper in part IV would analyse whether the cyber-attacks in outer space can be treated at par with the concept of global commons and how can it be regulated under the present legal regime. Part V of this paper would throw light on the State responsibility for such attacks and Part VI would highlight the legal lacunae and suggest a proposed framework to regulate the issue on hand._Based on the above mentioned issues, the paper examines three main aspects of cyber-attacks In the Outer space- First, it deals with whether the present legal regime governing cyberspace and Outer space can be extended to address the concern of cyber-attacks in outer space, secondly, the issue of state responsibility for such an act and Thirdly, it suggests a proposed framework to govern cyber-attacks in outer space. This essay exclusively deals with cyber-attacks on outer space from a state responsibility, and extending the present legal regime to govern the same point of view. It does not examine the technical aspects of cyber-attacks and how it can be prevented from a cyber-security point of view.

2. BACKGROUND OF CYBER-ATTACKS IN OUTER SPACE

Cyberspace is 'the space of virtual reality; the notional environment within which electronic communication (esp. via the Internet) occurs'.[5] It is the virtual realm that enables communication

amongst various computer devices and thus enables us to utilize the internet. The International Organization for Standardization defines cyberspace as the complex environment resulting from the interaction of people, software and services on the Internet by means of technology

[3] David Livingstone Mbe Dsc, Dr Patricia Lewis,'Space, The Final Frontier For Cybersecurity?' (Chatham House, The Royal Institute Of International Affairs, Sept 22 2016) <Https://Www.Chathamhouse.Org/Publication/Space-Final-Frontier-Cybersecurity> Accessed On 25 October 2018

[4] Kristen E. Eichensehr,'The Cyber-Law Of Nations' , 2015(103) Geo. L.J. 317, 347 Accessed 3 November 2018.

[5] Oxford English Dictionary,3rd Ed. 2000 [Online] <Http://Www.Oed.Com/View/Entry/248411?Rskey > Accessed 1 Nov. 2018

devices and networks connected to it, which does not exist in any physical form.[6] Cyber-attacks refer to interference with the cyberspace or through it so as to harm another system. In the present era of outer space activities, it is important that we have an efficient and effective cyber security regime that extends not only to the Earth, but beyond as well. There are various space weapons that are being used to create attacks on space systems. Some of them are- kinetic anti-satellite operations, which are lethal space weapons that enable the other systems to trace the target satellite which is communicating data to the interceptor vehicle and the same is directed on the satellite. It damages or compromises the target satellite, damages the environment on the Earth and the activities based on the data received and moreover such destruction of the satellite creates space debris. If the event occurs at altitudes greater than the lower end of low earth orbit, may be expected to create a cloud of debris that is unlikely to leave orbit for the foreseeable future.[7] Further, we have the Jamming of missile defense systems which is likely to deteriorate the system's performance capacity. Jamming of navigation, communication and GPS systems cause such services to be interrupted and they either fail to deliver the required data or deliver faulty data and signaling. Other cyber tools to attack space systems are hacking or spoofing of communication and GPS networks that compromise the data or signals sent and received to such systems, attacking the ground infrastructure like the satellite control centres either by ground based lasers or by interrupting their servers, sending of worms or trojans to the space systems, etc. Regulating cyber-attacks is a challenge to us, especially since we lack a strong enough cyber law and space law regime to tackle the said issue.

3. THREATS POSED BY CYBER-ATTACKS IN OUTER SPACE

Communications with outer space via satellites occurs exclusively through the use of the electromagnetic spectrum, a fundamental building block of cyberspace. And as the dependence of critical computerized systems – whether space-based or land-based – on satellite communications grows, so does their common vulnerability to threat vectors in cyberspace.[8]

It is, therefore important to understand the threats posed by cyber-attacks in outer space, considering the substantial and ever increasing reliance of society on satellite technologies for navigation, communications, remote sensing, monitoring and the myriad associated applications.[9]Cyber-attacks usually are targeted at the data or the system that provides the data such as ground stations, antennas of satellites or the landlines that connect to terrestrial networks. Cyber-attacks can be used to monitor data traffic patterns, to monitor the data itself, or to insert false or

[6] Kristen E. Eichensehr,'The Cyber-Law Of Nations' , 2015(103) Geo. L.J. 317, 325 Accessed 1 November 2018.

[7] Bill Boothby,'Space Weapons And The Law' , 2017 (93) Int'l L. Stud. Ser. Us Naval War Col. 179, 207 , Accessed 3 November 2018

[8] Adv. Deborah Housen-Couriel, 'Cybersecurity And Outer Space: Connected Challenges' (Israel Defence, 2 Feb 2017) <Https://Cyberregstrategies.Com/Wp-Content/Uploads/2017/02/Cybersecurity-And-Outer-Space_-Connected-Challengesisrael-Defense.Pdf>Accessed 6 November 2018

[9] Pavan Duggal, 'Cyber Security Law, Its Regulation And Relevance For Outer Space' (International Conference On Cyberlaw, Cybercrime & Cyber Security , New Delhi, November 2017)

corrupted data in the system.[10] When a space system is subjected to such an attack, the data may be compromised or lost, or the satellite itself might be destroyed. If the attacker gains control over a satellite in outer space, he could manipulate or shut down all communications and permanently damage the satellite system by damaging its sensors, solar panels, transponders or communication subsystems. Communication faces a grave disruption if satellites and space systems are targeted. China has alleged to have initiated attacks against a remote sensing satellite, Landsat-7 of the US Geological survey department, causing interference with the ground station communications for about 12 minutes. In these attacks, the hackers "achieved all steps required to command the satellite but did not issue commands."[11] Such cyber-attacks can be used to steal high priority government data. For instance, in 2007, a Russian-speaking group of hackers, likely linked to the Russian government, has stolen satellite data used by government groups, militaries, and embassies around the world. They had perpetrated this attack by means of a malware called Turla. The data gotten by the attackers was highly confidential in nature, affecting critical national infrastructure. Analysing the intersection between cyber and space security is essential to understanding this non-traditional, evolving security threat.[12] Cyber-attacks in space can disrupt enemy missile defense activities, aircrafts, logistic operations and command and control links. This interception can be in form of inducing corrupt information which eventually causes physical damage to the spacecraft.

...On the civilian side, satellites enable many of the communications (phone, text, email, internet, television) and banking operations (credit card purchases, ATMs) that have become the primary modes of social interaction and the lifeblood of the world's economy. Global Positioning System ("GPS") satellites guide and track cars, airplanes, and, soon, drones that will deliver household packages. Earth Monitoring spacecraft enable farmers to supervise their crops, foresters to direct firefighters, and flood control authorities to anticipate river flows. Satellites help save lives by supporting disaster relief and search and rescue missions.[13] This excessive mutual dependence of the internet and space has given rise to various vulnerabilities in outer space.

4. EXTENDING THE PRESENT LEGAL REGIME TO CYBER-ATTACKS IN OUTER SPACE.

4.1 Cyber-attacks and Territorial Sovereignty

Attribution of territorial sovereignty to Cyber space is tedious, merely because cyber borders are not like physical borders. Territorial sovereignty is wholly based on physical location and such demarcation is not possible with Cyberspace. Many thinkers opine that the physical hardware supporting cyber is located within territorial sovereigns and often owned by private parties, and they regard these facts as fundamentally problematic for the commons conception of

[10] Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts , 'Space Threat Assessment;A Report Of The Csis Aerospace Security Project, Center For Strategic And International Studies, 2018

[11] Ibid 8

[12] Pavan Duggal, (N 6)

[13] David A. Koplow, 'The Fault Is Not In Our Stars: Avoiding An Arms Race In Outer Space', 2018 (59) Harv. Int'l L.J. 331, 334 Accessed 29 October 2018

cyber.[14] A single sovereign can regulate some aspects of the internet like the physical hardware, but cannot exercise control over the cross-border communication networks, domains and activities. Cyber cannot be treated as a domestic issue, it has to be the very nature of the activities it is capable of performing, has to be regulated under international law principles. These principles limit a country’s authority to exercise jurisdiction in cases that involve interests or activities of non-residents, such as in case of a cyber-attack in space involving various parties from various states. Preventing such international transit would require local hosting of websites and storage of data, which is contrary to how the Internet currently functions, though some countries have considered such requirements in the wake of surveillance disclosures. Relatedly, sovereign states' ability to control cyberspace is further undermined by states' inability seal their cyber borders. The fact that states cannot retreat behind cyber borders,' but still want and need to access the cyber domain, creates the demand for inter sovereign interaction to address cyber issues.[15]

4.2 Cyber-attacks and Global commons

Cyber-attacks in outer space have two contrasting approaches to it. one, to attribute territorial sovereignty as it is done with Airspace and the other, by treating this at par with any other extraterritorial spaces such as the High seas, Antarctica and Outer Space, at par with global commons. I.e. common resources that are open for use by anyone, but use by one person reduces other people's ability to use it. This ‘use’ is limited to ‘peaceful purposes’ as followed under the legal regime for High seas, Antarctica and Outer space. Cyber-attacks in outer space, if treated at par with the global commons concept, will also be subject to the UNGA resolution on the peaceful uses of Outer space and allow for outer space activities only if they fall within the ambit of Peaceful purposes’. There are other legal regimes that are being used to regulate activities in the outer space. By extending the same to cyber-attacks, we can regulate and impose liability as well on the perpetrators of such attacks. They have been discussed below.

4.3 CYBER-ATTACKS AND THE EXISTING LEGAL REGIME

4.3.1 UN Charter

Article 2(4) of the U.N. Charter prohibits the threat or use of force against another state. This provision would undoubtedly be applicable to attacks committed by one state upon the space systems of another state via cyberspace. Further, Article 51 of the charter would also be applicable in case of cyber-attacks. This article empowers individual or collective self-defense in event of an armed attack. The same provision will be applicable to an attack that takes place via internet as well. For instance, If a state attacks the satellite of another state by intentionally sending a worm to it, then the state attacked has the right of self-defense against the state perpetrating the attack. -

4.3.2 Committee on the Peaceful Uses of Outer Space

In December 1958, the U.N. General Assembly adopted a resolution on "the peaceful use of outer space," which recognized ‘the common aim that outer space should be used for peaceful purposes

[14] Kristen E. Eichensehr,’The Cyber-Law Of Nations’ , (2015)103 Geo. L.J. 317, 338 Accessed 1 November 2018

[15] Ibid 12

only.' The UN, in 1959 established a Committee on the Peaceful Uses of Outer Space, to prevent state rivals from entering and using this new domain as a battle ground. According to this resolution, Outer space and celestial bodies are free for exploration and use by all States in conformity with international law and are not subject to national appropriation. A cyber-attack such as jamming, spoofing/hacking attacks on communication networks, targeting control systems or mission packages or attacks on the ground infrastructure definitely don't fall within the ambit of 'peaceful use'. They are catastrophic in nature, aimed at causing a disruption to a state's system, network or obtaining data or documents from another state without their identity or activities being detected. The internet must be used only to the extent that it allows for the peaceful use and conduct of activities by various space systems in the outer space and definitely not for such misuse of technology.

4.3.3 Outer Space Treaty

The Outer Space Treaty, 1967 proclaims that outer space, the moon and other celestial bodies, are not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means, and that space activities shall be conducted in accordance with international law. It prohibits states from placing in orbit, installing on celestial bodies or stationing in outer space nuclear weapons or other weapons of mass destruction. It also prohibits military installations, and military maneuvers on celestial bodies. These provisions can be extended to the cyber-attacks in outer space too. Art IX of the treaty is applicable as it makes it illegal for a state to interfere with the exploration of outer space but a nation may destroy a satellite in orbit if that satellite is being used for military purposes. This is applicable for all cyber-attacks such as hacking of the satellite of another state, jamming or spoofing of communication networks being sent or received by that particular satellite in outer space. The treaty assigns states international responsibility for their governmental and nongovernmental activities in outer space and renders the launching state liable for damage caused in air or space or on Earth by a launched object. This provision should not only be applicable in case of a physical object, but also to a software attack. A state launching a spoof communication network so as to intercept the communications of a satellite by another state must be attributed the liability at par as what would be if it was a damage caused by a physical object launched.

4.3.4 Moon Treaty

The Moon treaty, 1979 specifies that the activities on the moon and other celestial bodies must be "carried out in accordance with international law, in particular the Charter of the United Nations. It explicitly restricts use of the moon to "peaceful purposes," and prohibits any threat or use of force or any other hostile act or threat of hostile act on the moon" or use of the moon to threaten or engage in hostile acts with respect to "the earth, the moon, spacecraft, the personnel of spacecraft or man-made space objects.[16] It further prohibits placing or using nuclear or other weapons of mass destruction on or in orbit around the moon, establishing military bases, or conducting weapons tests on the moon. This treaty will be applicable in case of a cyber-attack on any

[16] See The Unga Resolution For Details, Unga Res 34/68 (*5 December 1979*) <Http://Www.Unoosa.Org/Oosa/En/Ourwork/Spacelaw/Treaties/Moon-Agreement.Html> Accessed On 6 Nov 2018

spacecraft, rover or satellites installed on the moon or any other celestial body by a state or an individual actor via the internet.

4.3.5 International Aviation law conventions

The Chicago convention, 1944 prohibits the use of weapons against civil aircrafts[17] and Article I of the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,1971 prohibits interference with a plane's operating system if such interference would render the plane incapable of flight. It also prohibits disrupting or destroying the navigation facilities that allow for flight if said interference would endanger any aircraft in flight, which could have an effect on the targets that nations consider when planning a cyber-attack.[18] The same principles should be applicable to an attack that is beyond airspace, ie. To the outer space. An attack via internet that aims at compromising the operating system of the spacecraft or interference that causes disturbances in the space systems must also be treated in the same manner as unlawful acts are against civil aircrafts.

4.3.6 NATO'S Policy,2011

In 2011, the NATO issues a policy on cyber defense which says that NATO will defend its territory and populations against all threats, including emerging security challenges such as cyber defense" and that NATO will provide assistance if its members suffer a cyber attack and also clarified that international law, including international humanitarian law and the UN Charter, applies in cyberspace. The NATO has recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea.[19]

5. ATTRIBUTION OF STATE RESPONSIBILITY IN EVENT OF A CYBER ATTACK IN OUTER SPACE

5.1 Unearthing cyber-attacks

Due to the difficulties in tracing a cyber-attack and revealing the attackers identity and intention to perpetrate the attack, we have to consider how this tracing can be effective and what standards can be adopted to attribute responsibility on the individual/state.

An IP packet can be intercepted or spoofed mid-route, making it impossible to trace. Thus, while in theory it is possible to trace the IP addresses of cyber attackers and use that information to locate them, "sophisticated hackers are able to re-route or confuse programs designed to locate them.", Similarly, if a hacker uses a botnet to carry out attacks, the process of tracing IP packets becomes more time and resource intensive.[20]Cyber-attacks are linked to nearly

[17] See Convention On International Civil Aviation , (7 December 1944) < Https://Www.Icao.Int/Publications/Documents/7300_Orig.Pdf> Accessed 3 Nov 2018

[18] Convention For The Suppression Of Unlawful Acts Against The Safety Of Civil Aviation (Adopted 23 September 1971, Entered Into Force 26 January 1973) 974 Unts 178 <Https://Treaties.Un.Org/Doc/Publication/Unts/Volume%20974/Volume-974-I-14118-English.Pdf> Accessed On 4 Nov 2018

[19]Klara Jordan, 'Nato's Cyber Domain Concept Shows Increased Maturity In Understanding Of Cyber Threats' (Atlantic Council Blog, 21 Aug 2017)<Http://Www.Atlanticcouncil.Org/Blogs/New-Atlanticist/Nato-S-Cyber-Domain-Concept-Shows-Increased-Maturity-In-Understanding-Of-Cyber-Threats> Accessed On 7 November 2018

[20]Scott J. Shackelford; Richard B. Andres, 'State Responsibility For Cyber-attacks: Competing Standards For A Growing Problem' , (2011) 42 Geo. J. Int'l L. 971, 982 Accessed 3 November 2018

every field of activity, whether a connection exists or if the connection is very feeble. One of which is the Outer space – where the connection between cyber terrorism threats and actual damage to space-borne assets is very direct.[21] Such attacks are usually staged against the base stations that control the satellite and the space system that is in outer space is compromised. It is difficult to trace the identity of the attacker who has perpetrated an attack on the satellite, the intention with which he has done it, whether the attack has been done under the direction and control of the state and the magnitude of damage done to the space infrastructure.

5.2 ATTRIBUTION OF LIABILITY- EFFECTIVE CONTROL VERSUS OVERALL CONTROL STANDARD.

The problem with a cyber-attack as opposed to any kinetic attack is that it is difficult to figure out when the attack was initiated, the identity and intention of the attacker and the possible circumstances of the attack. Identity is the most important aspect of a cyber-attack as it is the deciding factor on basis of which an appropriate response is made, i.e the response would vary if the attacker is an individual, a state or a terrorist group. There are two types of standards of control to be looked into for attributing responsibility for such an attack- The effective control standard and the overall control standard.

The *effective control* standard recognizes a country's control over paramilitaries or other non-State actors only if the actors in question act in "complete dependence" on the State.

An act of a non-state actor is attributable to a state if the state exercises “effective control” over the operation during which the act occurred under the “effective control” standard, private conduct that is merely supported, financed, planned, or carried out on behalf of the state is not attributable unless the state also exercises a high-level of control “in respect of each operation in which the alleged violations occurred.[22] Further, Article VIII of the International Law Commission's Draft Articles on the Responsibility of States for International Wrongful Acts says that the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.[23]

On the other hand, we have the *overall control* doctrine, from the ICTY Tadic case according to which when a State has a role in organizing, coordinating, and providing support for a group, the group's acts are attributable to the -State.[24] Under this test, it has to be proved that the group or the individual performing a cyber-attack is doing so under the control of the state.[25]The state

[21] Adv. Deborah Housen-Couriel, ‘Cybersecurity And Outer Space: Connected Challenges’ (Israel Defence, 2 Feb 2017) <Https://Www.Israeldefense.Co.Il/En/Node/28413> Accessed 6 November 2018

[22] Emily Chertoff, Lara Domínguez, Zak Manfredi, And Peter Tzeng, J.D, ‘State Responsibility For Non-State Actors That Detain In The Course Of A Niac, (A Report Of The Center For Global Legal Challenges, Yale Law School, 7 Dec 2015) Accessed 7 November 2018

[23] Responsibility Of States For Internationally Wrongful Acts 2001, Article 8

[24] Lawerence L. Muir, Jr, ‘The Case Against An International Cyber Warfare Convention’ (Wakeforest Law Review, 9 Dec 2017)<Http://Legal.Un.Org/Ilc/Texts/Instruments/English/Draft_Articles/9_6_2001.Pdf> Accessed 5 November 2018

[25] Bosnia And Herzegovina V Serbia And Montenegro [2007] Icj 2, [404]

must exercise control not only by equipping and financing the group, but also by coordinating or helping in the planning of its military activity. By the two tests mentioned, we can attribute responsibility to the states that either directly or indirectly perpetrate such cyber-attacks against the space crafts or space systems belonging to another state. Further, by virtue of Article 8, an individual whose conduct engages state liability cannot enjoy the benefit of acting on behalf of that state without prior permission. An individual will have to prove that he acted under the direction of the state for the responsibility to be attributed to the state. However, in cases where the individual attacker has not acted under the aid, direction or control of the state, the situation is different. According to James Crawford, the power structures within the international system are such that sovereignty and statehood remain the basic units of currency, but it is no longer possible to deny that individuals may have rights and duties in international law".[26] The individual perpetrating the cyber-attack, is therefore attributed with Individual criminal responsibility under Art 7 of ICTY for extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly.[27]

6. LEGAL LACUNAE AND THE ROAD AHEAD.

Although various legal regimes can be extended to address this issue, we need to understand that in absence of a comprehensive strategy and regime exclusively for cyber-attacks in outer space, this issue cannot be solved. The first lacuna being that in spite of having various International treaties and conventions that can be extended to this issue, implementation of the same is very difficult due to the lack of an international body or organization entrusted with the same.

Further, the lack of national and international policies to regulate the cyber and space arenas. There needs to be in place international policies and dialogue between states regarding the comprehensive policy to regulate cyber-attacks in outer space. Such policies must address issues of attribution of responsibility, response of states and ensure a strong cyber security regime as well. This lack of international cooperation and lack of international agreements between states is why we are unable to address this issue effectively. Another important legal concern is the attribution of responsibility to non-state actors, who have typically been motivated by financial gains and ideologies. According to the *effective control* standard, a state is liable for the acts performed by the non-state actors only if the actors in question acted in complete dependence of the State. Under the overall control test, if a State has a role in organizing, coordinating, and providing support for a group, the group's acts are attributable to the State. The laws are however unclear as to what happens and what is the discourse to be taken if neither of these situations are applicable and if the attack has been perpetrated by a non-state actor, independent of the state's direction or control. The next part of this paper suggests a proposed framework to deal with the

[26] Kristen E. Eichensehr,(N 12)

[27]Statute Of The International Criminal Tribunal For The Former Yugoslavia, Un Security Council Resolution As Amended 29 September 2008 By Resolution 1837, Art 3(B) <Http://Www.Icty.Org/X/File/Legal%20library/Statute/Statute_Sept09_En.Pdf> Accessed 11 Nov 2018

present situation. There are various cyber-attacks being carried out in the outer space such as anti-satellite (ASAT) operations Jamming of missile defense systems, hacking or spoofing of communication and GPS networks, attacking the ground infrastructure like the satellite control centres, sending of worms or trojans to the space systems, etc. These attacks can be regulated and controlled by employing various legal and technical measures. Few technical responses that can be adopted to safeguard the space systems from attacks are- restricting the proxy servers so that the attackers don't gain control over the system, ensuring encryption to prevent jamming and spoofing, ensuring that the networks or utilities are traceable and that the infrastructure doesn't support anonymity. Furthermore, tests must be added for immunity to such attacks as an integral part of the tests satellites undergo during the manufacturing process, before being launched into space. It should mutually be decided about the role of the governments, how security can be maintained in the space community and whether this security regime must be a regional or an international one. It is essential that the symptoms of the attack are identified and preventive measures are taken against it. It is essential that we invest in new 'hack-proof' or 'hack-resistant' technologies, including blue-sky approaches such as quantum technologies for communication.[28] The satellite layout must be managed and be equipped enough to tackle a cyber-threat. It is important that awareness is created amongst the members of the space community to understand these cyber vulnerabilities and the legal regime regulating the same.

The need of the hour is to promote international co-operation amongst states and to develop a space cyber security regime to address all the concerns relating to cyber-attacks in space. This comprehensive space cyber security regime must be designed in a way that it suits the needs of various stakeholders such as the Governments, the Military groups, the technicians and the interests of the society at large. To align across and within all sectors, one approach is to adopt a single focus such as the provision of assured broadband via space – and make that the driving force, organizing all other initiatives around it. [29] In absence of a relevant international organization to regulate and implement the policies, what can be done is to resort to dialogues between two or more states such as the 2015 US–China cyber agreement, bilateral treaties or multilateral treaties such as The United States which has signed a Memorandum of Understanding with India on the issue of cyber-attacks and has added an extension to the existing Australia and New Zealand.[30], contacting the NATO cyber emergency response team or the INTERPOL, etc. Further, the same frameworks resorted to for other space related concerns such as those under the Outer space treaty, The Moon treaty, UN charter, etc must be resorted to

[28] David Livingstone And Patricia Lewis International Security Department, 'Space, The Final Frontier For Cybersecurity?' (2016) Chatham House <Https://Www.Chathamhouse.Org/Sites/Default/Files/Publications/Research/2016-09-22-Space-Final-Frontier-Cybersecurity-Livingstone-Lewis.Pdf> Accessed 11 November 2018

[29] Ibid 26

[30] Munish Sharma, 'India : Us :: China : Us – Cyber And Bilateral Visits' (Institute For Defence Studies And Analyses, 9 Jun 2016) <Https://Idsa.In/Idsacomments/India-Us-China-Us-Cyber-And-Bilateral-Visits_Msharma_090616> Last Accessed 5 November 2018

until we design an exclusive regime for cyber-attacks in outer space. The solution to the problem of attribution, further, is to allow for states to pool their resources and databases so as to figure out where the cyber-attack originated and which state must be attributed the liability for the same. We must set up the required infrastructure for the current and the future requirements for cyber security in outer space.

1. CONCLUSION

In conclusion, the author would like to stress on the fact that we are living in an era where the internet and space activities are highly dependent on each other and it this interdependence that has become a part of our daily lives. At the moment, with the possibility of cyber-attacks being perpetrated beyond Earth, all the way up to the Outer space, it is important for this issue to be given attention at the International level. Although we have various legal regimes dealing with this aspect, there is none that exclusively does. Until a Comprehensive international strategy is framed to address the issue, States must indulge in dialogues and enter into bilateral and multilateral treaties to govern the same. We currently lack an adequate cyber and Space security regime, thus making it essential for the International community joining hands to address the issue at hand.

*****