Cyber Law and Outer Space (Activities): Legal and Regulatory Challenges

*Rada Popova**

Abstract

Cyber security opens a new dimension in the discussion on human activities in outer space. The part of the law pertaining to cyberspace which is of interest for this paper is the regulation related to cyber activities in outer space.
Space activities are not immune from malicious cyber activities as transmission signals are vulnerable to cyber access. The range of threats is very wide and can include the loss of control, the disruption of services and the modification or loss of data. While it is clear that the malicious uses of cyberspace constitute a large spectrum of threats for space operations, the legal rules applicable to cyber operations have still to be determined.
This paper will first tackle definitional matters in order to describe the technical nature of cyberspace and to address the question on how cyber law may touch upon outer space activities. Then, questions of the applicability of international law and space law to cyber activities as well as measures to address the consequences of cyber threats to the space infrastructure will be addressed.

1. Definitional Matters

Before an assessment of the role and the importance of cyber regulation for outer space activities can be undertaken, some definitional issues must be addressed. First of all, the notions 'cyberspace', 'cyber activities' and 'cyber law' must be defined in order to clarify what the relation and the interdependence between outer space and cyber activities are and what role does cyber law play in terms of regulation.

* Teaching and Research Fellow and PhD candidate at the Institute of Air Law, Space Law and Cyber Law (University of Cologne); (Mag. iur) Law Master's Degree (University of Vienna); Researcher at the 2017 Centre for Studies and Research (Hague Academy of International Law). Institute of Air Law, Space Law and Cyber Law, University of Cologne, Germany, rada.popova@uni-koeln.de.

1.1. Cyberspace, Cyber Activities and Cyber Law

Absent a universal and legally binding definition, the notion *cyberspace* can be briefly defined as a globally accessible technological infrastructure of interconnected computers and networks which is used for the transmission of signals and data.[1]

Cyber activities are based on the exchange of digitized data and take place through the use of cyberspace infrastructure using the universal language of code.[2] *Cyber activities in outer space* can therefore be defined as all activities that involve the use of cyberspace in relation to the transmission of data between the different elements of the satellite infrastructure.[3]

Cyber law does not exist as a secluded legal domain. It comprises the legal issues pertaining to cyber activities in various fields, such as communications, finance, transportation and critical infrastructure. It is not yet an advanced, but rather an emerging field of law which is currently scattered in various national policies and regulations, regional sets of rules and, at least in an initial phase, in relevant norms of international law. At the same time, as interoperability allows for the global accessibility of cyberspace, this opens a new dimension of the discussion on human activities in an international and global domain.[4] The main subject of cyber law are non-lawful cyber

1 Compare, for example, the definitions provided by the Oxford Online Dictionary: "*The space of virtual reality; the notional environment within which electronic communication (esp. via the Internet) occurs*"; the definition formulated by the International Electrotechnical Commission in its Guidelines on Cybersecurity, ISO/IEC:2012: "*The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*"; the definition formulated in the Memorandum from the US Deputy Secretary of Defense from 2008: "*[the] global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers*" (quoted by Mudrinich, E. M. *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, The Air Force Law Review, Vol. 68 (2012), p. 174) as well as the definition used in the German Cyber Security Strategy of 2011: "*Cyberspace includes all information infrastructures accessible via the Internet beyond all territorial boundaries*".

2 As famously formulated by Lawrence Lessig two decades ago, "Code is Law". See Lessig, L., Code and Other Laws of Cyberspace, Basic Books, New York 1999.

3 Currently, there is a lack of definitional preciseness in the terms used with regard to harmful cyber activities and very often, the notion 'cyber attack' is used *en gros* which leads to an overall lack of precision in the legal debate. In this paper, the attempt will not be undertaken to define the term 'cyber attack' as this requires a dedicated definitional debate. Here, the more general term 'malicious cyber activities' is found to depict better the full scope of various levels of malicious cyber activities.

4 Feick, J., Werle, R., Regulation of Cyberspace, in: Baldwin/Cave/Lodge (Eds.), The Oxford Handbook of Regulation, Oxford University Press/Oxford Handbooks

activities, thus the norms of cyber law aim at enabling the safe co-usage of cyberspace and the prevention from malicious cyber activities.
In this paper, the focus will be put only on some of the most relevant issues in order to depict the relevance of cyber activities for outer space.

1.2. Delimitation Between Cyber Law and Internet Technology Law

An important distinction must be made between cyber law and internet technology law because, although are closely related, they govern different subjects and are not synonymous.
First, the application of cyber law is not restricted only to the uses of the internet. Generally, internet (technology) law covers the legal aspects of usage of the world wide web (WWW) as the most used service provided by the internet and provides the legal framework for the global dissemination of electronic information. While the internet is a part of cyberspace, cyberspace consists also of systems and networks which may be considered an 'isolated virtual space'[5] as they are not connected to the internet or interconnected with other networks and the wider network.[6] This is the case, for example, with networks which are part of the critical infrastructure of a State[7] and serve the national defense and security.
Second, the main subject to be regulated by internet technology law is the regulation of contents on the Internet, such as the information flow, the creation of websites, the use of domain names, intellectual property rights, e-commerce and privacy matters.[8] In contrast, cyber law is applicable primarily to the protection from the malicious uses of technological infrastructure.
Therefore, cyber law and internet technology law are not equal legal fields. Cyber law is applicable primarily to the protection from malicious uses of cyberspace, whereas internet (technology) law primarily applies to the content transmitted over the internet.

Online. Retrieved from http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199560219.001.0001/oxfordhb-9780199560219-e-21.

5 Cyber Security Strategy for Germany (2011). Retrieved from https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf; see also the "Internet Standards Process", RFC 2026 of the IETF, Revision 3, Network Working Group, October 1996, p. 2.

6 Herpig, S., Strategic Operations in the Cyber Domain and Their Implications for National Cyber Security 2015. Retrieved from https://subs.emis.de/LNI/Proceedings/Proceedings246/597.pdf, p. 598.

7 § 42 U.S.C. 5195 (c) - Critical infrastructures protection.

8 One of the most prominent examples for regulation relevant for the protection of personal data from recent times is the EU General Data Protection Regulation, (EU) 2016/670 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

2. Cyberspace and Outer Space: a Comparison

The role of cyber activities in outer space can be illustrated by comparing the legal nature and main characteristics of the two domains cyberspace and outer space. There are a few significant features which showcase that, first, certain naturally predisposed restrictions exist for the usability of these domains and second, that due to some similar characteristics, related legal principles might be applicable to both fields.

In terms of physical scope and accessibility, both cyberspace and outer space are internationally and globally accessible environments. With regard to cyberspace, this is predetermined by the interoperability of its network architecture and the universal 'language' of code. In outer space - by the natural laws of astrophysics such as orbital motion, gravity, perturbations etc. In both domains, there is detachment from or difficulties for the establishment of jurisdiction through territoriality.

Moreover, both domains serve as an environment for human activities - in man-made cyberspace through the interaction of persons, hardware, software and worldwide technological services based on protocols[9]; in nature-made outer space, mostly through the use of rocket and satellite technology and the transmission of data between Earth and outer space.

The access to both cyberspace and outer space is open in its nature and depends first and foremost on technological (i.e. computer-based and launching) as well as on financial capabilities. Moreover, both cyberspace and outer space are, to a different extent, *per se* free from physical borders and detached from sovereignty as territoriality has subordinate meaning in them.[10]

In terms of legal consequences, this means that both cyberspace and outer space are subject to international regulation as national regulation is restricted in its scope and effectiveness. Hence, concepts of general international law are applicable in both environments.

9 Feick, J., Werle, R., Regulation of Cyberspace, in: Baldwin/Cave/ Lodge (Eds.), The Oxford Handbook of Regulation, Oxford University Press/Oxford Handbooks Online. Retrieved from http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199560219.001.0001/oxfordhb-9780199560219-e-21.; Reidenberg, J., *Governing Networks and Rule-making in Cyberspace*, Emory Law Journal, Volume 45 (1996), p. 911.

10 The concept 'jurisdiction' is applicable to both domains, but in a rather weaker form due to the difficulties to establish a nexus between space objects and States, on the one hand, and between cyber activities and States, on the other hand, based on territoriality.

3. The Factual Background: Cyber Threats in Outer Space

3.1. Types and Addressees of Cyber Threats

Cybersecurity is becoming an increasingly relevant aspect of outer space activities. Since the beginning of the 'space age' six decades ago, space technology has not only experienced commercialization which has transformed the originally mostly state-owned and state-financed space infrastructure to a currently strongly privately-owned and to a large part also to a privately-financed market. Space applications have become relatively widely accessible and the impact of outer space technology in various fields of everyday life, critical infrastructure[11], defence systems and transportation is global. This transformation has inevitably led to an interweaving between outer space and cyberspace – because, as all other devices that are using internet-based networks, also space objects have become devices in the Internet of things (IoT).[12]

The risks for space missions[13] include, among others:

- the loss of availability of ground infrastructure:
- the (physical) loss of satellites;
- the degradation in the overall performance of the satellite;
- the partial degradation of system performance;
- the loss of mission availability for the end user;
- incorrect mission data received by the end user
- unauthorized access to data;
- unauthorized access to control.

They can originate from private hackers, or by governments[14] and be motivated by commercial or political reasons and may target each segment of space infrastructure. For example, they can be addressed at satellites in outer space, at ground stations as well as against the uplink or downlink

11 Falco G., Job One for Space Force: Space asset Cybersecurity, Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2018, p. 1.

12 Blount, P.J., *Satellites are Just Things on the Internet of Things*, Air and Space Law Vol. 42. No. 3 (2017), pp. 273-294.

13 See, for example, Muylaert, J./Del Monte, L., Cybersecurity of Space Missions, Presentation at the Workshop of the European Interparliamentary Space Conference, 14 May 2018.

14 Blount, P.J., Targeting in Outer Space: Legal Assets of Operational Military Actions in Space, Harvard national Security Journal, 2012, available online at http://harvardnsj.org/wp-content/uploads/2012/11/Targeting-in-Outer-Space-Blount-Final.pdf.

communication taking place between space and the ground infrastructure. The addressees of such malicious cyber activities can be satellite operators (private or governmental) as well as end users.
The purposes of these attacks can be manifold and usually are aimed at the impediment of operations, at stealing or modifying satellite data, at sending wrong information to the addressees. Although not yet feasible without considerable financial and technological capabilities, hacking satellites can even result in the overtaking of access and physical control over space objects.

3.2. The Vulnerability of Space Infrastructure vis-à-vis Malicious Cyber Activities

Certain measures can be undertaken to mitigate these risks.[15] However, full protection from malicious cyber activities addressed at space objects is not feasible. The problem is that these security controls and preventive actions remain always one step behind hackers due to the remoteness of satellites. The hardware and software, once the satellite has been launched, cannot be physically updated to meet new security challenges and 'wireless' updates from the ground station are not comprehensive enough to meet the challenges posed by hacks that are constantly being sophisticated. The fact that after launch the satellite can merely get substantial updates which are restricted to software only, underlines the significant advantage of hackers vis-à-vis the protection capabilities of the satellite operator.
The infrastructure on the basis of which data is transmitted between Earth and outer space the frequency spectrum – is open both for electronic as well as for cyber-based uses.[16] Through so-called jamming radiofrequency communications are interfered with through the creation of noise in the same frequency band.[17] Jamming can cause interference in both the downlink and uplink communication for the signal received by satellites as well within the

15 According to Muylaert/Del Monte (*supra note* 13), such cybersecurity measures may include the security in development and life cycle; signal protection; spacecraft resiliency; system access control; system monitoring, message and data protection, command protection.

16 Jamming is generally not considered a malicious cyber activity as radiofrequency interference does not necessarily involve cyberspace; spoofing, however, might be a mechanism to trigger cyber intrusions, for example by altering the output signal from the satellite or by simulating fake signals using software-defined spoofers. The first major GPS spoofing attack was reported by the US marine administration in 2017 against ships on the Black Sea, see Jones, M., "Spoofing in the Black Sea: What really Happened?", https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/.

17 Harrison, T./ Johnson, K./Roberts, T., Space Threat Assessment 2018, Aerospace Security, 11 April 2018, p. 4; available online at https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_SpaceThreatAssessment_FULL_WEB.pdf?w0Hlq5eiJvbk_7hPbqifSrBNUqZEDfca.

field of view of the receiving ground station.[18] Spoofing results in creating a fake signal produced by the attacker's device. Through spoofing, false or corrupted data may be broadcasted and received by the attacked object. This may even result in manipulating and taking over control over a satellite.[19] In result, any communication between Earth and space and between space objects through signals can be 'hacked' through malicious cyber activities. Thereby, access to data, signals and even physical control over space objects can be overtaken by the uses of cyberspace.

This process has been intensified through the emergence of NewSpace,[20] in particular through the development of small satellites and the projects for mega-constellations[21] as low-cost devices may be more vulnerable. This vulnerability is caused by the need to provide service at a competitive price which leads to a trade-off between security and price. However, there also other factors which contribute to the overall vulnerability of space infrastructure. As other technologies, also space technology has undergone a shift from being analogue to digitization.[22] Considering the number of single interconnected 'entry points' of a satellite system (ground mission segment, ground control segment, space segment, user segment, uplink and downlink communication) using the global language of internet protocols[23], the risks for intrusions using cyberspace are considerable.

Furthermore, the complexity of the problem is aggravated by the fact that unlike kinetic attacks directed against satellites, malicious cyber activities do not necessarily require substantial financial means. The large number of suppliers in the supply chain of the satellite infrastructure add up to the

18 Garino, B., Gibson, J., *Space System Threats,* in: Air Command Staff College. AU-18: Space Primer, 2nd ed., pp. 274-275.

19 Harrison, T./ Johnson, K./Roberts, T., Space Threat Assessment 2018, Aerospace Security, 11 April 2018, p. 4; available online at https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180823_Harrison_SpaceThreatAssessment_FULL_WEB.pdf?w0Hlq5eiJvbk_7hPbqifSrBNUqZEDfca.

20 See, for example "NewSpace: New Business Models at the Interface of the Space Industry and Digital Economy", Study Commissioned by the German Federal Ministry of Economy and Energy, SpaceTec Partners/BHO Legal, 2016. Full text in German available at https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/bericht-der-koordinatorin-lur.html.

21 See, generally, *Small Satellites and Large Satellite Constellations,* in: Jakhu/ Pelton (eds.), Global Space Governance: An International Study, Springer, 2017, pp. 357-378.

22 On the convergence and digitization of telecommunications, see Werbach. K, Breaking the Ice, *Rethinking Telecommunications Law for the Digital Age*, Journal of Telecommunications and High Technology Law, Vol. 4 (2005), pp. 59 et seq.

23 Blount, P.J., *Satellites are Just Things on the Internet of Things*, Air and Space Law Vol. 42. No. 3 (2017), p. 278.

probability that access is gained to vulnerable entry points.[24] Hacking the ground station from which control over a satellite is exercised, or hacking the battery power system on board a satellite, can be effected through sophisticated hacking, but does not require sophisticated technology.[25]

4. The Legal Framework Applicable to Cyber Activities in Space

4.1. The Legal Framework Applicable to Cyber Operations in Space

As has been argued above, cyber law is not a separated, 'autonomous' legal field, but it is much more integrated in different branches of law insofar as far as cyberspace has a relevance to the activities governed by the respective legal fields.

What is clear is that currently, there is no international cyber law that governs the global cyber infrastructure. Apart from one international agreement - the 2001 Budapest Convention,[26] and some regional[27] and national efforts[28], States have not yet come up with an international agreement on the regulation of cyberspace.

Cyber activities have been extensively discussed in the context of *jus ad bellum* in order to establish whether, and under which circumstances, cyber 'attacks' may be qualified as use of force as set out in the UN Charter in its Article 2 (4)[29] and whether the right to self-defence might be applicable in cases of hostile cyber acts.[30] It is not yet clear whether and in how far malicious cyber activities fall under the applicability of international law regulating conflicts (e.g. whether a cyber attack can constitute use of force). However, as some interventions might be combined with a certain element of force or a physical effect, one may argue that these cases constitute a violation of the prohibition of intervention and that certain cyber activities

24 Falco G., Job One for Space Force: Space asset Cybersecurity, Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2018, p. 5.

25 *Ibid.*

26 Convention on Cybercrime, Council of Europe, CETS No. 185, concluded on 23 November 2001, entered into force on 7 January 2004.

27 These regional efforts include mainly policy documents of the European Parliament and the Council of the EU, the most recent of which is the so-called 'cybersecurity package' to improve the EU cyber resilience and response. See European Commission, Digital Single Market, Cybersecurity, available online at: https://ec.europa.eu/digital-single-market/en/cyber-security.

28 See, for examples, the national cyber strategies and cyber-related laws of Canada, Germany, China, Israel, Russia, USA.

29 Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI.

30 *Ibid.*, Article 51.

can indeed amount to the use of force in the sense of Art. 2 (4) of the UN Charter.[31]

In the specific context of space activities, according to Article III of the Outer Space Treaty[32] international law applies to outer space activities, unless a specific provision has been established in the treaties on space law.[33] Thereby, it remains to be seen under which conditions international law and space law are applicable to cyber activities in outer space. It can be argued that cyber operations conducted from or through outer space or aimed against space objects, are subject of space law.[34] Thus, space law is *lex specialis* with regard to cyber activities that are based on space assets.[35] Thereby, the milestone provisions setting the legal framework for human activities in outer space are applicable to cyber operations directed to or originating from outer space which are not merely transmitted through outer space. Therefore, according to Article IV OST, cyber activities in outer space must fulfill the requirement to be conducted for "peaceful purposes".[36] Moreover, cyber operations in

31 There is extensive literature on the discussion on whether certain malicious cyber activities can violate the prohibition on the use of force. See, among others, M. N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017 pp. 330-339; Waxman, M. C., *Cyber Attacks and the Use of Force: Back to the Future of Article 2(4)*, Yale Journal of International Law Vol. 36 Issue 2 (2011), pp. 421-459; Petras, C.M., *The Use of Force in Response to Cyber-Attack on Commercial Space Systems - Reexamining Self-Defense in Outer Space in Light of the Convergence of U.S. Military and Commercial Space Activities*, Journal of Air Law and Commerce, Vol. 64, Issue 4 (2002), pp. 1214-1268.

32 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 610 UNTS 205, adopted on 27 January 1967, entered into force on 10 October 1967.

33 In this sense, space law is a *lex specialis* to general international law, see Simma, B., Pulkowski, D., *Of Planets and the Universe: Self-contained Regimes in International Law*, European Journal of International Law Vol. 17 (2006), pp. 483 et seq.

34 For a diverging opinion, see Mejia-Kaiser, Martha, Space Law and Unauthorized Cyber Activities, in: Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace, NATO Cooperative Cyber Defence/Centre of Excellence, Tallinn, 2013, p. 360.

35 See the chapter "Space law" in M. Schmitt (Ed.), Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations, pp. 270 et seq. to which Hobe/Popova had contributed as experts throughout 2015. There, a distinction is undertaken between "space-enabled cyber operations" and "cyber-enabled space operations" whereby the latter involve either the operation of space assets or the conduct of space operations by cyber means.

36 For an extensive account, see Schmitt (Ed.), Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations, Cambridge, Cambridge University Press, 2017, pp. 273-277.

outer space must not impede the exercise of jurisdiction and control over space objects as this would amount to violation of sovereignty.[37] According to the rather vaguely formulated principles of due regard and non-interference stipulated in Article IX Outer Space Treaty,[38] cyber activities in outer space may not harm and damage the activities of other States. Another obligation for States results from Article VI Outer Space Treaty which requires that any space activity, thus including cyber activities, must be authorized and supervised. Non-compliance with this obligation may result in state responsibility.[39]

It is questionable whether the liability regime of space law[40] is applicable in cases where the damage caused by a space object results from a cyber activity.[41] Here, it can be stated that the law of State responsibility is generally applicable to cyber activities in outer space and the specific liability regime for damages caused by space objects should be applicable as *lex*

37 Lafferranderie, G., *Jurisdiction and Control of Space Objects and the Case of an International Intergovernmental Organisation (ESA),* Zeitschrift für Luft- und Weltraumrecht (German Journal of Air and Space Law) Vol. 54 (2005), pp. 229–242.

38 On the meaning of the 'due regard' and 'co-operation' principles, see S. Marchisio, "Article IX", in: Hobe/Schmidt-Tedd/Schrogl (eds.), Cologne Commentary on Space Law Vol. I, Cologne, Heymanns, 2009, mn. 19 *et seq*.

39 As codified in the Articles on Responsibility of States for Internationally Wrongful Acts, International Law Commission, November 2001, adopted by the International Law Commission at its fifty-third session (2001), available with commentaries at: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Merits, Judgment of 27 June 1986, 1986 ICJ Reports 14 and *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment of 26 February 2007, ICJ Reports 2007, p. 43.;

40 Art. VII Outer Space Treaty; Convention on International Liability for Damage Caused by Space Objects, 961 UNTS 187, adopted on 29 March 1972, entered into force on 1 September 1972 (Liability convention).

41 Applying the criterion of kinetic effects to argue that cyber activities are not to be considered space activities, Mejia-Kaiser brings forward the argument that: "*[The Liability] Convention applies to damage which arises from the kinetic energy and other physical direct damages that unfold following a collision by the space object's body or parts thereof. For that reason, damages directly caused by unauthorised cyber activities to a space object are not covered by the Liability Convention per se. Unauthorised cyber activities against space systems can also not be considered as space activity under Outer Space Treaty Articles III and VI",* Mejia-Kaiser. M, Space Law and Unauthorized Cyber Activities, in: Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace, NATO Cooperative Cyber Defence/Centre of Excellence, Tallinn, 2013, p. 360.

specialis.[42] For example, if resulting from a cyber activity, a space object causes damage in outer space, fault-based liability should be invoked.[43] More problematic is the case where absolute liability should be applicable, namely in cases where the space object, as a result from an intentional cyber activity, causes damage to aircraft in flight or on the surface of the Earth as in these cases, both the rules on absolute liability as well as state responsibility may be applicable.

4.2. The Problem of Attributability as the Main Issue for Imposing Any Legal Consequence

One of the most challenging issues related to the regulation of cyber activities is attributability.

Prevention is not enough to counteract cyber threats and intrusions. So far, the issue of attribution to States of malicious cyber activities, which would amount to an internationally wrongful act, has not been extensively addressed by international law and no agreement has been reached on the issue of whether it suffices for a cyber activity to originate from a State's territory to presume State responsibility.[44] However, as the source of the attack can very rarely be traced back, very often the responsible persons cannot be prosecuted while the attacked person/organisation/state has to carry the costs for the consequences of the attack. The existing (customary) legal regime on state responsibility as codified in the Articles on the Responsibility of States for Internationally Wrongful Acts[45] makes it clear that the principle of due diligence is applicable in cyberspace and that States should not allow their territory to be used for malicious cyber activities against other States.[46]

This undoubtedly applies in all cases where the State knowingly allowed its territory to be used for malicious cyber activities and failed to undertake

42 Article VIII Outer Space Treaty; Differently, Mejia-Kaiser, *supra note 42*.

43 Article III Liability Convention

44 Pihelgas, M., Back-Tracing and Anonymity in Cyberspace, in: K. Tsiolkowski (ed.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, NATO Cooperative Cyber Defence Centre of Excellence, 2013, p. 31, 33; Antonopoulos, C., State Responsibility in Cyberspace, in: Tsagourias/Buchan (eds.), Research Handbook on International law and Cyberspace, Edward Elgar, 2015, p. 55, p. 62.

45 Responsibility of States for Internationally Wrongful Acts, GA Resolution 56/83, UN Doc. A/RES/56/83 (28 January 2002, adopted 12 December 2001) annex.

46 *Corfu Channel* (United Kingdom vs. Albania), Judgment, International Court of Justice, ICJ Rep. 4, 22.; Report of the Group of Intergovernmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (22 July 2015), 13 (c), 13 (f).

measures to prevent the occurrence of a violation of international law through cyber activities carried out from its territory.[47]

5. Conclusion

The analysis of the existing legal framework applicable to cyberspace, on the one hand, and to outer space activities, on the other, leaves many questions open. While certain legal concepts are common for both domains, many definitional delimitations remain disputable and various cross-sections between cyber activities and the use of space infrastructure remain outside the scope of the existing regulation.

It is to be expected, however, that with the raise in the awareness about the weak points in the various segments in the satellite (supply) chain and its components, more efforts on the national and regional, but also on the international level will be invested specifically with regard to cybersecurity in outer space.

47 Chircop, L., *A Due Diligence Standard of Attribution in Cyberspace*, International & Comparative Law Quarterly, Vol. 67, Issue 3, July 2018, pp. 643 – 668.