IAC-20-E9,2.D5.4,x59386

THE CHALLENGE OF PROTECTING SPACE-BASED ASSETS AGAINST CYBER THREATS

Antonio Carlo[a]*, Laetitia Zarkan[b], Lisa Lacroix[c]

[a] *Space Generation Advisory Council (SGAC), Italy,* antonio.carlo@spacegeneration.org
[b] *Space Generation Advisory Council (SGAC), Switzerland,* laetitiazarkan@gmail.com
[c] *Space Generation Advisory Council (SGAC), Germany,* lisa.lacroix@spacegeneration.org
* Corresponding Author

Abstract

After more than 60 years of space activities, society has become dependent on space based technologies. The proliferation of private actors in the last decade has resulted in an intense race, while States are showing a renewed interest in space by increasing their investments and supporting diverse types of operations. Access to space is no longer limited to big powers as there is an increasing number of countries and private actors that own and operate satellites for all types of uses, including sensitive military capabilities and vital civilian infrastructures. Policy gaps are plentiful regarding the application of cybersecurity to space-based assets. This relates to the lack of global consensus on a precise definition of a use of force and on a clear threshold for what constitutes a use of force in cyberspace. National and global cybersecurity policy are still cautious when addressing digital security threats. Applied to space-based assets, this policy landscape lacks precision. As a matter of fact, a cyber operation targeting critical infrastructures could be the easiest and the most efficient way to disrupt essential services by inserting malicious codes aiming at stealing information or hindering any command and control systems.

If not preempted, such attacks could become a serious threat to space missions. Additionally, even though signatures and codes gradually become easier to identify, States and commercial actors are not rushing to ameliorate the process of attribution regarding the identity of cyber attackers. However, protecting space missions would not only require resilient and flexible systems but also the identification of the potential cyber threats and exposed components within the whole infrastructure to mitigate the risks. In this context, establishing clear mechanisms related to space-based assets security in the cyber world is not only important to build long-term sustainability in outer space. This is also necessary due to the lack of accepted international norms concerning unacceptable behavior in cyberspace. This paper will first briefly review how cybersecurity is addressed at both national and international levels. It will then assess the most important shortfalls of the existing legal regimes and the need for mitigation measures. Finally, it will conclude with suggestions and best practices to strengthen the protection of space-based assets in the cyber world. Please note that the present abstract is submitted under the auspices of the Space Generation Advisory Council, as part of the activities of the Space and Cybersecurity Project Group.

Keywords: Space, Cyber Space, Cybersecurity, Space Operation, Cyber Threats

1. Introduction

In the last decade, the increasing use of cyber capabilities by space operators brought to the inevitable development of new threats. Nowadays, technologies such as communication infrastructures as well as navigation, positioning and timing depend on space assets through international transmission and connection. With many space operators performing a digital transformation, more and more satellites are controlled by digitised systems, carry digital payloads and use digital links and cyber capabilities to gather, store and transmit information. Hence space assets are not only vulnerable to physical threats, but also to cyber threats. Space sector witnesses the conduct of space activities by a multitude of both public and private actors. The race to launch and deploy satellites of one's own country has both security and defence purposes. This race is also strongly linked to the national impetus to deploy new capabilities to have an hegemony in the space field and to remain independent. Space activities support many activities on the ground as space assets have a global coverage to connect remote areas, to monitor large zones all over the world, or to offer an accurate timing and positioning for many essential activities. While space assets are becoming more valuable, some actors are somewhat developing new types of devices with the intention of neutralising or momentaneously invalidating the systems and the opposing capabilities in space. The neutralisation can be done in a various of manner however

the new technologies allow the use of the cyber world to inflict a decisive hit to the space sector. Satellites can be attacked directly when the space asset is targeted and indirectly when the supporting assets like ground bases are under an attack. In the event of such a malicious operation, cyber and space issues are, in most cases, addressed by national laws and policies. However, both cyber and space normative systems are contained in general public law, as well as in customary international law and non-binding legal principles. In this context and because of the evolution of cyber and space activities, developing laws and policies that would fit the challenges of covering all the issues stemming from these activities is a vain wish. Hence a developmental interpretation of general principles may apply to disputes relating to space operations using cyber capabilities. This paper will identify the vulnerabilities of space assets connected to the cyber world through digital links and onboard equipment. After a brief review of the threats targeting the surface of attack, the paper will describe the role and status of the different actors of cyber operations that may have an impact on space activities, both as the victim or as the attacker. Finally, the paper will address the questions regarding States' jurisdiction and sovereignty. It will also provide an overview of the legal rules applicable to space and cyber domains and will try to find a common agreement on what the thresholds of malicious activities should be.

2. Space Operation

All activities intended to be or carried out in outer space are considered space operations. To this end, operations carried on earth with the intention to reach outer space such as a launch, from a planning, training and mission control point of view, is considered a space operation even in the unlikely event of a failed launch. This definition helps identify from a legal and a technical point how to deal with specific events [1].

2.1 The three Segments

Every artificial satellite needs three fundamental operational components: Space Segment, Ground Segment and User. These components are interlinked as parts of a larger space ecosystem. Altogether, they form the surface of attack as they cooperate and coexist with each other.

2.1.1 Ground segments

Ground segments are composed of all the ground based elements of the system such as transmit and receive each station. Primary elements are ground station, operation centre, launch facilities and integration test facilities. All of these facilities need highly qualified personnel that provide and maintain the segment running. The ground segments are decentralised and placed around the globe for technical purposes. The ground segment infrastructure needs to be always in contact with the other two operational components otherwise this could result in a misinterpretation of commands and lead to catastrophic events.

The telecommunication infrastructure needs to be resilient and/or always operational. For this reason, there are numerous components worldwide in order to prevent blind spots in communication. These can be from different agencies or organisations. The European Space Agency (ESA) is using its telecommunication centre in the United Kingdom, national centres such as the Italian centre in Malindi (Base Broglio) and the French launching site in the French Guiana.

Nowadays cyber events are increasing in number and kind. For instance these events can be Distributed denial of service (DDoS), Ransomware, SQL Injection or Brute-force. The ground segment are easy targets due to the large number of personnel working in them and the vulnerability of infrastructures and equipment. This vulnerability is likely to spread to other segments. Therefore, these segments are critical for a strong defence because in case of a breakthrough the security can prevent any kind of threats to reach the space segments. Constant monitoring, mitigation measures, and training of the personnel are essential to prevent and contrast possible cyber and physical events.

2.1.2 User Segment

The user Segment consists of the customer terminals that lead the operation and give command to the control centre and receive the elaborated data that are going to be shared.

In the early years of the space era, the predominant users were the governments driven by military entities, later the market-gap allowed the access of private companies with ingent investments in the field.

2.1.3 Space Segment

The Space Segment includes the satellite and the ground facilities such as telemetry and command.

The space segments are all the infrastructure that are in or are intended to be launched in space. Through time these segments had some evolution in the arrangements and configuration in order to serve different purposes such as the launcher, rover, modules for the construction of Space labs and satellites.

Initially space segments consisted of a unique/single satellite, such as the Envisat, however with time and the advancing of technology these satellites often decreased in size and increased in number to arrive in our days with

entire constellations or mega constellations of private companies such as startlink of SpaceX.

Satellites can be of many different natures and purposes such as: earth-observation satellites, geo-location/navigation satellites; communications satellite; space exploration [2].

a) Earth-observation satellites: Consist of satellites that provides information services based on Earth Observation data. These information are used both by military and civilian purposes such as the Copernicus programme of the European Commission in collaboration with ESA [3].
b) Geo-location/navigation satellites: These satellites provided by space-based assets are essential for the prosecution of everyday life since they are used for precision targeting; tracking; provision of precise timing which is also vital for the function of economical and banking networks. Europe developed his own system such as the Galileo Programme. The need to address cyber-related challenges to these strategic space assets is critical as essential services are dependent on having strong security measures.
c) Communications satellite (SATCOM): Telecommunications satellite is one of the most widespread functions of satellites, either civilian or military. Earth stations transmit information to other earth stations or to a user by using relay satellites. A satellite can carry the information all over the world thanks to its wide range of transmission. SATCOM provides support to C2 through its multiple applications, such as the establishment of communications in regions with minimal or even non-existent infrastructure; transmission of intelligence; relay of messages and control of UVs [4].
d) Space exploration in outer space or on celestial bodies. With the development of new activities planned to be carried out on celestial bodies, a new trend is emerging. More and more automatic or autonomous systems are being built to operate without or with limited human interaction. The emergence of space mining may boost the space economy and subsequently, the systems may become ideal targets to disrupt another State's or company's activity.

Since everyday life and daily operations carried out in the air, on the sea or on the ground rely totally on space segments, these have become extremely sensible and fundamental. In this sense the loss of command and control of one or many of these segments/capabilities may lead to a failure of the integrity that can heavily impact the ground segments. These impacts may lead to great issues due to the fact that space assets are widely used in a multitudes of sectors such as finance, communication and navigation.

This led to the rise of new actors targeting this segment for economical, political or military purposes which will be analysed in the following chapter.

With the increasing numbers of artificial satellites launched in the different orbits and the new constellations, the number of entry points through which attackers may gain entry into the surface of attack and disrupt space infrastructure is more and more vulnerable to cyber operations.

2.2 Threats

The increase and wide spread of space activities lead the main space players to be targeted by new threats. These menace are carried by international and national actors with different means and objectives. To contrast and protect the targeted space operation, nations have been developing new countermeasures against hostile attacks. These menaces are carried by different entities such as Nation States, cybercriminals and cyber terrorists.

Space segments serve different purposes and therefore are targeted in different ways one to the other. Possible threats can be divided in two categories, hard-kill and soft-kill [5].

a) Hard-kill is based on the use of a projectile or other methods in order to achieve the kinetic destruction of the target. Due to the predictability of satellite orbits and their restricted maneuverability, satellites are particularly susceptible to such attacks.
b) Soft-kill relies on interfering with the satellite's sensors (via jamming, spoofing or blinding through the use of powerful lasers), or with the satellite's software (via cyberattack). These attacks can render a satellite defunct without destroying it. A tangible example can be the Intelligence, Surveillance and Reconnaissance (ISR). Space-based assets equipped with sophisticated sensors provide a host of services, such as intelligence gathering, including Signal Intelligence (SIGINT); target information and damage assessment; warning of attacks and situational awareness.

Satellites used for critical operations are under constant attacks with the objective to take control over these infrastructure. A strong security and defence in the matter of cyber and physical is not just important but essential for the running of the Space Operations.

3. Actors liability and compensation

Questioning liability and compensation in the case of a cyber event requires defining actors involved and their legal status. Admitting a simplified configuration, actors can be summarised in the following four categories [6]: Nation State Actor, Private Economic Actor, Hacktivists/Natural Persons and International Entities. Each of which may be in one of the following positions: instigator of an attack, responsible for the attack, victim of the attack or collateral victim of the attack.

3.1 Nation State Actor

The presence of a state actor represents, *a priori*, the most expected situation in the context of a cyber-attack. The state, as a strategic military force, is at the same time the actor that seems most likely to suffer an attack from another state, individual or organization, or to be the instigator. In the context of cybersecurity, the role and responsibility of the state must be seen in a much broader way. Firstly, because this type of attack can easily be commissioned to a private entity to "cover" the traces, but also because damage to a state's strategic infrastructure could be caused by a single individual who could cause damage to one or more states and/or their companies [7]. In the first scenario the proof of a state responsibility is still difficult to raise as the international law has not yet been ruled as it is well summarized in Scott J. Shackelford's article: "State responsibility for cyber-attacks: competing standards for a growing problem" [8]. According to the international law, to be responsible for an attack it should be proven that a state was in "control" of it. However, this notion is always subject to controversy. The International Court of Justice (ICJ) has, indeed, interpreted it as a "complete dependence" [9] of a non-state actor towards the state ordering the attack or what is legally called the "overall control". This means that there should be no doubt of a State sponsoring the attack (that it involves in planning and coordination of the attack). However, directing operations or instructions are not required to engage the State responsibility. On the contrary, in 2007 the International Criminal Tribunal for the former Yugoslavia (ICTY) established that an "effective control" [10] was enough in the State responsibility for an attack. Beyond the law controversy, these two interpretations show that states are responsables, in international public Law for sponsoring any actors in an attack but the degree of their interference can lead to different legal responses that will be developed in the following chapter. In addition, the question of the "responsibility to protect" [11] a State should be raised in case of damages to private economic actors and/or civil society as well as the statute recognition of the State as a victim of the attack. An attack on a private satellite could cause damage either on its own facilities or its economic development. Collateral victims of a conflict between two states-actors could also occur for example if a debris hit a commercial satellite or if a third state actor would see its capacities limited (e.g. loss of geo-spatial imageries). Therefore, the implication of Nation States seems inevitable and should be addressed either in the law applicable in case of a state conducting or being victim of the attack but also on its responsibility regarding its companies, the behaviour of its own citizens and its necessity to build infrastructure and policy capable of protecting those actors.

3.2 Private Economic Actor

Cyber-attacks are currently difficult to quantify as companies fear the economic impact of disclosing these information. Therefore it is highly likely that the same phenomenon of information disclosure can take place in the space domain with consequences such as reputational damage and/or negative market effects negative market effects. According to Thomson Reuteurs, [12] the current state of the Cybersecurity liability of private companies is imposed generally if the following conditions exist:

a) "An entity failed to implement safeguards required by statute or reasonable security measures,
b) An entity failed to remedy or mitigate the damage once the breach occurred,
c) Failure to timely notify the affected individuals under a state's data breach notification statute, may give rise to liability for civil penalties imposed by a state attorney general or other state enforcement agency."

Data's breach responsibility goes normally on the data owner's and not the operator. Reparations should be on pecuniary level in this regard. Nevertheless, depending on the contract the owners can always go to trial, at a civil level, against the operation.

3.3 Hacktivist/Natural Persons

The dependence of many services on space technology (agriculture, internet, etc.) raises the question of the status of a civil victim in the event of an attack. Would it be possible for an individual to bring before a court a claim for compensation against a company that has suffered an attack and/or against the perpetrator of the attack itself. Collective actions could be envisaged and whether or not per country or more globally. From a civil point of view, the existence of damage may give rise to a claim for reparation, but the dispersal of victims over several countries or even continents could make the procedures particularly complex. Individuals could also be perpetrators of an attack. There are two possible cases: that

of the "lone wolf" having perpetrated an attack with a political aim or wanting to demonstrate an ability to make such a manoeuvre or having acted on behalf of a state/company/group or the case of a malicious act on the part of, for example, an employee of a company. The status of the "individual" must be defined whether acted as part of a group or as a civil servant. In this respect, the recent decision of the European Union (EU) to take sanctions against individuals having participated in entities or States perpetrating cyber-attacks and/or "attempted attacks". This shows that the level of response, including by an international organisation, can be at the individuals [13] level. Nevertheless, it can be seen that no reparation measures have been taken, as may be the case in a civil liability case, and that the sanctions applied are similar to those of the entity without distinction between entities and individuals. Also the EU seems to have preferred to target individuals and not directly the State that sponsored the attack.

3.4 International Entities

As has been highlighted previously with the recent EU decision, [13] an entity can be sanctioned for both "cyber-attack" and "attempted cyber-attack". NGOs or civil organisations do not own satellites and it seems unlikely that political or terrorist groups would be able to access the infrastructure necessary for a satellite launch. Nevertheless, the development of nano and cubesat could lead NGOs, e.g. environmental or human rights NGOs, to seek access to space. This would make them targets for States or companies concerned by their surveillance. Special protection should therefore be envisaged at the international and legal levels if these actors were to develop this type of technology.

In recent years there has been an increase in the number of actors involved in the cyberattacks. Identifying the perpetrator and/or the victim of the attack is essential and international cooperation is required.

3.5 Distinction between civil and military operators

Space Operations have been carried out by civil and military organisations with different objectives, however these operations could be carried out simustanialy with dual-use technologies. Earth observation has obviously a military application but it is also used for civilian purposes so protecting those assets and protecting those capabilities, is critically important. To do so, is fundamental to identify the applicable law.

Risks of cyber events are increasing day by day and there is a need for protection for high-level satellite data and services that are interconnected. For military stakeholders, satellite data may become a relevant target so the levels of resilience to cyber intrusions are strongly mixed not only as far as the single components of satellite infrastructure are concerned but in particular, with regard to connected periphery links, including supply chain providers, user terminals and user devices.

4. Legal implications of cyber threats against space assets

Many discrepancies and policy gaps exist regarding the application of cybersecurity measures to space infrastructure, especially to space based assets. Guidelines, standards, and suggested norms tend to be limited to a field or a State's territory, or at the negotiation phase.

Implementing cybersecurity measures in space legal framework depends on the capacity for this field to adapt to such changes. Both fields, cyber and outer space lack a unique, strong, and coherent integration in a legal framework. Space activities should not only be compliant with space law as *lex specialis* but also with general international law. However, the legal regime that applies to space and cyber operations and activities tends to be scattered.

In the event a malicious cyber operation is carried out by a State against another State, there is a need to interpret whether such an operation does not raise to the level of use of force in its scale and effects. Pursuant to Art. 2§4 UN Charter, all UN Members "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence [14] of any State, or in any other manner inconsistent with the Purposes of the United Nations". The Purposes of Article 2§4 of the UN Charter may be interpreted as prohibiting threat or use of force against another State's territorial integrity or political independence. The UN Charter binds States and in contentious cases, only states are eligible to appear before the International Court of Justice (ICJ). Additionally, even though no cases on cyber incidents have been brought before the ICJ so far, earlier cases with content that have relevance in discussions on cyber law. But without a positive attribution to States, the UN Charter is not applicable and the ICJ has no jurisdiction to deal with individuals or private entities.

Due to the difficulty to trace the source of an attack, attribution is a particular challenge with regards to cyber warfare. Locating the origin of a cyber-attack is highly complicated due to the possibility that an attacker could be stationed in a different jurisdiction.

In cyberspace, it is possible to consider the doctrinal definition of Tallinn Manual 2.0. A cyber-operation may qualify as a use of force amounting to an aggression when it has necessary "scale and effects", a notion used by the International Court of justice to qualify certain actions as

an armed attack [15]. This notion of "scale and effects" comprise several elements [16], presence of which may be used to qualify a cyber-operation as a use of force [17]. However, depending on the physical consequences of a malicious cyber-operation, the Lotus principle may dismiss legal restrictions in cyberspace. Furthermore, the outer space treaty of 1967 only prohibits the placement of weapons of mass destruction in outer space. In other words, the notion of cyber-attack is not defined and therefore, international obligations may not apply to States carrying out malicious cyber operations against other States. Therefore, they are not explicitly forbidden. However, space assets using cyber technologies are vulnerable to threats and have to be protected. States' interpretation of the notion of "peaceful use of outer space" differs: For some states, it means "non-military", for others, it means "not aggressive". This lack of consensus is challenging as it makes unclear how states subject to malicious cyber-operations can defend themselves and proportionally replicate while remaining compliant with international law.

The ICJ considered actions of non-kinetic nature can be regarded as use of force [18]. Additionally, in an advisory opinion of 1996, the ICJ considered that all established principles and rules of international humanitarian law apply to all forms of warfare so we can include space and cyber [19]. The question of the status of the different stakeholders is also at stake. During peacetime, a malicious actor may launch an attack on computers constituting the space infrastructure from malicious software. In this case, there isn't any certainty whether the actor is working independently or on behalf of a State, an international entity or a military force. Hence determining the military or civilian nature of the actor is challenging as well as identifying which law applies to the case at hand.

The features and use of malicious cyber activities in non-armed conflict situations as well as the scope and consequences of cyber criminality have stimulated discussions and important guidance can be found in soft law. Currently, independent projects are underway to develop manuals that will articulate the international laws applicable to cyberspace, such as the Tallinn Manual 2.0, but also to military space operations. Ongoing discussions outside the formal multilateral channels are providing ideas and perspectives. Two of the major ones, the MILAMOS Project and the Woomera manual involve another convert non-governmental efforts to develop manuals on how international law applies to military activities in outer space, both in peacetime and wartime. The ability to define international norms and standards relevant to international behaviour represent its own form of soft power, therefore it is important for States to be involved in these types of discussions. With the emergence of new activities carried out on celestial bodies, new economic interests are appearing. States have an increasing interest in protecting private companies and organizations. Unfortunately, it doesn't seem we have a strong and coherent international legal framework. It is challenging for lawmakers to understand how essential a strong cybersecurity strategy is, for both space operations and digital systems. Cyberattacks may cause critical disruptions undermining private companies', State's and military forces' capacity to ensure a strong service. The international dimension and the multitude of companies and organisations involved in the supply chain to build space assets is an important aspect to consider. The question of security is crucial for critical space infrastructure within all these stakeholders. As a consequence of this interdependence, if one actor or one state in the supply chain is weak, then other actors and states cannot deal effectively with cyber threats. Because of the challenge of creating a protective legal framework enforced by a strong entity, mitigation measures to prevent an escalation in cyber vulnerabilities may be the most efficient way to protect space stakeholders, for them to have a good estimation of the risks of having their infrastructure threatened by an attack. The challenge for commercial actors is to maintain the necessary level of cybersecurity, especially if the satellite is a critical infrastructure or has national security implications. Space actors need to assess the potential threats and balance with the costs of mitigating those threats, depending on the importance of the data transmitted, the value of the information systems, but also on its criticality.

With these issues in mind, setting up security mechanisms and strategies among the relevant stakeholders would be beneficial to identify the most efficient current and future requirements ensuring cybersecurity in space operations.

5. Conclusions

While space operations and cyberspace operations are distinct, operations in space enable many cyberspace operations, and space systems' control segments require use of cyberspace. Both outer space and cyberspace relate to domains that are not legally defined but are generally perceived in their scope. So far, States have not come to an agreement on an international regulatory framework for cyber activities. The International Telecommunication Union (ITU) has recognised its competence in questions pertaining to the Internet and has elaborated a reference guide for States for developing their national cybersecurity strategy.

The features and use of malicious cyber activities in non-armed conflict situations as well as the scope and consequences of cyber criminality have stimulated

discussions and important guidance can be found in soft law. Ongoing discussions outside the formal multilateral channels are providing ideas and best practices in the implementation of new policies. As Professor Hofmann and Professor Masson-Zwaan stated in their publication: Introduction to space law: "many of the open questions about outer space will be unanswerable without either State agreement to formal rules or from the lessons learned if armed hostilities break out in the space domain" [20]. This provides a clear overview in the medium time scenario that such hostility will happen at a specific point of junction between outer space and cyberspace.

References

[1]T. Uhlig, F. Sellmaier, M. Schmidhuber, Spacecraft Operations, Springer-Verlag, Wien, 2015.

[2]Defense Intelligence Agency, Challenges to Security in Space, 2019 https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf, (accessed 01.08.20).

[3]European Commission, Interim evaluation of Copernicus, Final Report, July 2017 https://www.copernicus.eu/sites/default/files/2020-05/ET0417742ENN.en_.pdf, (accessed 01.08.20).

[4]ITU, Evolving satellite communications, ITU's role in a brave new world https://www.itu.int/en/itunews/Documents/2019/2019-02/2019_ITUNews02-en.pdf, (accessed 01.08.20).

[5]A. Carlo, N. Veazoglou, ASAT Weapones: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era, MESAS 19, Palermo, Italy, 2019, 29-31 October.

[6]P. Wallace, R. J. Schroth, W. H. DeLone, Cybersecurity regulation and private litigation involving corporations and their directors and officers: A legal perspective, Kogod Cybersecurity Center, Kogod School of Business, American University, 2015.

[7]Khan, Fahad Ullah, States Rather than Criminals Pose a Greater Threat to Global Cyber Security: a Critical Analysis, Strategic Studies, vol. 31, no. 3, pp. 91–108. 2011.

[8]Scott J. Shackelford & Richard B. Andres, State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, Georgetown journal of international law. Vol. 42. p. 971-1017, 2011.

[9]International Court of Justice, Nicaragua v. United States of America, 1984.

[10]International Criminal Tribunal for the former Yugoslavia, Tadić (IT-94-1), 1995

[11] Gross, Oren, Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents, Cornell International Law Journal, Vol. 48 No. 3, Article 1, 2015.

[12]T. Reuteurs (legal), Who is liable when a data breach occurs?, 2020.

[13]Council decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[14]M. N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, Tallinn, February 2017, p. 329, §2.

[15]International Court of Justice, The Republic of Nicaragua v. The United States of America (1986), §195.

[16]Katharina Ziolkowsky, General Principles of International Law as Applicable in Cyberspace, in Peacetime regime for state activities in cyberspace, 172-173 (Katharina Ziolkowsky ed., 2013).

[17] M. N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, Tallinn, February 2017, p. 333.

[18]International Court of Justice, The Republic of Nicaragua v. The United States of America (1986).

[19]International Court of Justice, Legality of the Threat or Use of Nuclear Weapons (1996).

[20]Tanja Masson-Zwaan, Mahulena Hofmann, Introduction to Space Law, Fourth Edition, Kluwer Law International, 2019.