When Cyber Activities Are Space Activities

Definitions Are Key

*Stefan A. Kaiser**

Abstract

Cyber space is not Outer Space and cyber activities are different to space activities. But where are the dividing lines? Space law applies to cyber activities when they are space activities. This leads to the question how we define space activities in the meaning of the Outer Space Treaty. With increasingly refined space applications, including satellite communication, remote sensing and navigation and networked environments that span from the Earth into Outer Space, space activities need to be defined more precisely. The other term that needs to be defined are cyber activities. They depend on network connectivity and this is the possible connecting point with space activities. However, in a computer networked environment, not every signal that traverses through Outer Space becomes a space activity. Based on the definition of both, space and cyber activities, this article attempts to delineate their intersection for a practicable understanding about when a cyber activity is a space activity. Following this approach, additional terms and concepts in connection with unauthorized cyber activities need to be more precisely distinguished, including jamming, spoofing, interference and attack. More precise definitions are key to the understanding of the concepts and the linkage between cyber and space activities.

Keywords: cyber activities, space activities, non-authorized cyber activities, hacking, jamming, spoofing, interference, cyber attack, launch and operation of space objects, remote sensing, satellite communications, satellite navigation

* LLM (McGill). This paper represents the author's personal opinion and shall not be attributed to any organization with which he is affiliated.

1. Introduction

The significance of the delineation between space and cyber activities results from Article VI of the Outer Space Treaty of 1967 (OST).[1] In a manner exceptional in public international law, under Article VI OST

> States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty.

Under general concepts of public international law, States are not responsible for the activities of their nationals, unless they act in an official capacity. When interpreting "*national activities in outer space*" broadly, the increasing number of cyber activities by non-governmental actors that are somehow linked to Outer Space could be deemed to fall under Article VI, so that States would be responsible for them.

2. Space Activities

2.1. The Wording of the Outer Space Treaty

The wording of Article VI OST uses the term "*national activities in outer space*". By the literal meaning of this article, these 'activities' have two attributes. They need to be 'national' and 'in outer space', but the OST does not contain a more explicit definition. During the negotiations of Article VI OST, national representatives concentrated not so much on the nature of 'space activities', but on the actors undertaking them. As a result, States bear legal responsibility for the 'space activities' of both, governmental and non-governmental entities, while the term 'space activities' is open to interpretation. Other provisions of the OST mention 'exploration and use of outer space',[2] 'studies in and exploration of outer space'[3] and 'launching of space objects',[4] all of which can be understood as space activities; but space activities are certainly not limited thereto.

2.2. The Interpretation of States

Interpretations of States can be found in their national legislation. This is a side effect of Article VI OST, which requires State Parties to the OST to authorize and continuously supervise the national space activities for which they are responsible. As a matter of due diligence, an increasing number of

1 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, 1967, 610 U.N.T.S. 205.
2 Title, Preamble, Articles I, III OST.
3 Article IX OST.
4 Articles VII, VIII OST.

States have enacted national legislation to establish transparent and clear rules about their national regimes of authorization and supervision, and on the scope of activities in outer space for which they accept responsibility. In their national legislation, States define 'space activities' differently, but two general tendencies are apparent. The first group of States puts a stronger emphasis on the purpose of space activities, while the others attempt to address the nature of the activities they consider as space activities.

2.2.1. Focus on Purpose

Stating the purpose of space activities, follows to a certain extend the wording of the OST. The definitions typically refer to space exploration, space research, use and development of space technologies and also the use of outer space.[5] The various definitions are quite different. Given their purpose-oriented approach, unfortunately they provide no solid anchoring point for determining the role of cyber activities in relation to space activities.

2.2.2. Focus on Substance

States of the other group[6] define 'space activities' by the substance or nature of the undertakings they deem relevant. They typically do this by an enumerative listing. The reason is likely to limit the scope of their national responsibility to only these activities. All States of this group mention two elements, in one way or another:

- Launching of space objects - some States also mention attempted and/or procured launches and/or return to Earth;
- Operating space objects - some add command, control and/or guidance.

5 Russian Federation: Art. 2 1. Law on Space Activity 1993, amended 1996, 2004, 2006; Ukraine: Art. 1. Law on Space Activity, 15 November 1996, amended 2000, 2006; Korea: Art. 2 1. Space Development Promotion Act, Law No. 7538, 31 May 2005; United States: §20103 (1), Title 51 USC, National and Commercial Space Program, 18 December 2010; Indonesia: Art. 1 2. Law of Republic of Indonesia, No. 21 of 2013 on Space Activities.

6 Sweden: Sec. 1 Act on Space Activities, 1982, 963; South Africa: Sec.1. Space Affairs Act, No. 84, 1992; UK: Application of Act 1. Outer Space Act 1986, 1986 Chapter 38; Hong Kong: Sec. 3 Chapter 523, Outer Space Ordinance, Special Administrative Region Government; Belgium: Art. 2 §1 Law of 17 September 2005 on Activities of Launching, Flight Operations and Guidance of Space Objects, revised 2013; Netherlands: Chap. 1 Sec. 1. b, Space Activities Act, Bill 13 June 2006; France: Art. 1 3º Space Operations Act, 2008; Austria: §2 1. Austrian Outer Space Act, 6 December 2011; Denmark: Part 2, 4, 1) Outer Space Act, 11 May 2016; Finland: Sec. 4 1) Act on Space Activities (63/2018), 23 January 2018.

A limited number of States in this group also list

- Activities in Outer Space – which can be considered as an opening clause, because of its general nature;
- Operation or use of (launch) facilities and installations.

However, also these definitions that focus on the substance or nature are not specific enough to explain whether cyber activities are part of them. It is nevertheless evident, that space objects are operated, commanded, controlled and guided from control centres on the Earth by remote control radio links. For that reason, several researchers have expressed that certain activities on Earth are space activities when they are 'predominantly and intentionally directed at outer space'.[7]

Space activities are dependent on remote control. Today, space objects rely increasingly on pre-programmed software, but autonomous operations in space are still rare. Likewise, most portions of human space flights are not directly controlled by the astronauts on board. From its early days, space flight has been dependent on (radio) remote control. At that time, present day data networks did not exist. One can indeed consider space operations as one of the first cyber activities, at a time when this term did not yet exist.[8]

3. Cyber Activities

3.1. Elements

There is no internationally agreed definition of 'cyber' or 'cyber activities'. Despite being written for military purposes, a useful starting point can be the United States' Joint Chiefs of Staff's definition of 'cyberspace operations':

> Cyberspace operations (CO) is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.
>
> Cyberspace, while part of the information environment, is dependent on the physical domains of air, land, maritime, and space. CO use links and nodes located in the physical domains and perform logical functions to create effects first in cyberspace and then, as needed, in the physical domains. …[9]

This definition contains three elements that need to be highlighted:

- Cyber activities are in the information environment and are performed through logical functions.
- Cyber activities depend on physical domains.

7 Michael Gerhard in Stephan Hobe et. al. (eds.), Cologne Commentary on Space Law, Vol. 1, Article VI, note 21, with further references in footnote 21.

8 See also *infra* note 10.

9 United States Joint Chiefs of Staff, Joint Publication 3-12, Cyberspace Operations, 08 June 2018, Executive Summary, page viii, and more broadly in Chapter I 2., https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (accessed 12 September 2020).

- Cyber activities perform effects either in cyberspace or in the physical domains.

3.1.1. Logical Functions

That cyber activities are in the information environment and are performed through logical functions describes how cyber activities work. This means, cyber activities are not only based on information,[10] but they also perform logical functions. For such logical functions, typically some form of computer program is required (more precisely: self-executing software code) that can activate a software function. The use of self-executing software code is key for understanding cyber activities.

The logical function element distinguishes cyber activities from other activities which are either physical in nature or do not perform a logical function, but may have a similar effect as cyber activities. For example, a physical activity that effects the network infrastructure, like shutting off the electrical power, or physically damaging hardware or cables cannot qualify as a cyber activity, because it is not undertaken by an action that uses digital information to perform a logical function.

3.1.2. Dependence on Physical Domain

The second element are the 'links and nodes located in the physical domains' on which logical functions in the information environment depend. The US Air Force doctrine of 2011 was more specific, when it mentioned this domain to consist

> *of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.*[11]

Networks comprise a large variety of wired (copper, fibre optics) and wireless (radio) links which can be located at or span across land, sea, air and Outer Space. Connections between ground stations and space objects and their related hardware form wireless links that can become part of this infrastructure or 'physical domain'.

3.1.3. Effects of Cyber Activities

The third element of the Joint Chiefs of Staff's definition shows where cyber activities take effect, either in cyberspace or in the physical domains. Effects in cyberspace means changes of data, of numeric values that cyber activities operate with – just think of a numeric value change in your on-line bank account. Effects in the physical domain relate not only to the links and nodes

10 Today, digital technology is standard for executing logical functions. In the pre-digital age, also analogue signals were used in early high-tech applications to prompt logical functions through remote control.

11 US Air Force Doctrine, Annex 3-12, Cyber Operations, Introduction, 30 Nov 2011.

of the network infrastructure, but to any physical effect that can be caused through peripherally connected devices, like in the 'internet of things'. This ranges from domestic applications of 'smart homes' to industrial processes.
For a more precise explanation, the Joint Chiefs of Staff's definition refers to a three-layer computer network model.[12] Numerous computer network models with even more layers are discussed in the literature.[13] In an earlier publication I tried to define cyber activities based on its effects based nature and a three-layer model as "*actions prompted by digital information to produce outputs on the application layer by using the data link / network / transport layer and the related communication signal protocols.*"[14]

3.2. Non-Authorized Cyber Activities

From a security and legal viewpoint, non-authorized or malicious cyber activities play an important role. For that reason, the various methods and the terminology require some clarification.

3.2.1. Hacking

Hacking is a common term used for non-authorized cyber activities, by which a digital code is used for gaining access to networks and computers for the purpose of non-authorized/malicious access, use, manipulation or theft of data and/or for prompting effects through the network in the physical domain.

3.2.2. Jamming

Jamming relates to interference of a radio transmission by a stronger radio signal at the same frequency that predominates it, so that the original transmission and its message is distorted or not any longer receivable. The prevention of harmful interference between radio stations is the main purpose of the International Telecommunication Union's (ITU) Radio Regulations.[15] Jamming does not qualify as a cyber activity under the elements discussed above, because it is not prompted by a logical information functionality through a network. Jamming should rather be understood as an

12 They speak of three interrelated layers: physical network, logical network, and cyber-persona. Other publications use different names, e.g. physical layer, data link / network / transport layer and application layer – there is no conceptual difference.

13 For example, the OSI (Open Systems Interconnect) model with 7 layers, defined by ISO (International Organization for Standardization) standard 7498. For more details of the various layer models, see Emin Caliskan, Raimo Peterson, Technical Defence Methods, Tools, Techniques and Effects, in: Katharina Ziolkowski (ed), Peacetime Regime for State Activities in Cyber Space, NATO CCD COE Publication, Tallinn 2013, pp.62-65.

14 Stefan A. Kaiser, In Search of an International Public Order for Cyber Activities, IAC-18, E7,5,2, x43994, Colloquium on Space Law 2018, 671, 676.

15 Art. 45 of the Constitution of the International Telecommunication Union, U.N.T.S. 1825, 1826, Art. 15 (ITU) Radio Regulations.

electromagnetic interference with, or disruption of, the network infrastructure, in this case radio links, that cyber activities depend on.

3.2.3. Spoofing

Spoofing can be understood as mimicking information in electronic format so that a system, does not portray the factual situation any longer. The effect can be, for example, that false aircraft are indicated in an air traffic surveillance system or that false radio navigation signals lead to wrong location determinations.[16] Today, spoofing is typically accomplished in systems using digital data formats. Following the above methodology for identifying cyber activities, spoofing suffices the requirement of a logical information functionality. Whether spoofing is performed in and through a network depends on the specific spoofing method used and on how broadly we define networks.

3.2.4. Interference

The term 'interference' is used in different ways. The ITU uses 'harmful interference' in a narrow sense that relates to radio signals only.[17] 'Harmful interference' is used more broadly in Article IX OST, where it signifies activities or effects imposed by humans that detrimentally affect space activities. In the context of cyber activities, the term 'interference' is sometimes used to indicate a non-authorized/malicious cyber activity and to avoid confusion imposed by the term 'cyber-attack'.

3.2.5. Cyber Attack

Within the computer community, the term 'cyber-attack' is often applied synonymously with unauthorized or malicious cyber activities. Legal professionals tend to avoid to use 'cyber-attack' broadly, because of the different meaning of 'attack' in the law of armed conflict and to avoid that any cyber intrusion is considered as a new means of war.

4. The Space Activity – Cyber Activity Nexus

Practical scenarios can be analysed for better understanding when cyber activities qualify as space activities. Only when a cyber activity forms an integral part of a space activity, it can be qualified as a space activity by itself.

16 For a definition of spoofing Global Navigation Satellite Systems, see International Civil Aviation Organization (ICAO), Doc 9849, Global Navigation Satellite System (GNSS) Manual, 3rd ed. 2017, section 5.3.5: "*Spoofing is the broadcast of GNSS-like signals that cause avionics to calculate erroneous positions and provide false guidance.*"

17 *Supra* footnote 15.

4.1. Practical Scenarios

4.1.1. Launch, Return and Operation of Space Objects

There is no doubt, that the launch, return and operation of space objects are space activities. Since the beginning of the space age, ground based control centres undertake command and control actions for performing launch, return and operations remotely through radio links. This means, these (cyber) actions are an integral part of launching, returning and operating a space object, even when they are performed on the Earth.

Sixty years ago, these radio commands were in analogue format. Today, the command, control and guidance signals are in digital formats, performed in the information environment through logical functions; they use the network infrastructure: computers, ground-stations, radio links; this means they are cyber activities. Having an effect on space objects, by physically navigating and positioning the space object and by controlling the on-board systems for its operation in Outer Space, they also qualify as space activities.

4.1.2. Remote Sensing

Satellites carry payloads depending on the purpose of the satellite. For example, the payload of a remote sensing satellite carries the equipment for taking images and measurements of the Earth (and likewise of Outer Space, celestial bodies and other space objects). Unquestionably, these are space activities. Ground stations operate, maintain and adjust the sensor payload by remote signals. These commands from Earth, today in digital format, are therefore both, cyber activities and space activities. The data sent back to ground stations in digital format (but not with self-executing software code) are the products of this space activity. Further processing, refining, embedding of additional information and interpretation of these space (data) products do not qualify as space activity.

4.1.3. Satellite Communications

Satellite communications is somewhat more complex. The operation of communications payloads on board satellites, typically transponders that receive and transmit signals, qualifies as a space activity.

The signals handled by the communications payload of the satellite, require a more differentiated view. Satellite or transponder operators commercialize their transponder capacity for the use by other parties, who supply the information content of the signals. As a result, the wireless communication links to and from satellites are part of the network infrastructure. A user may send different types of information through this link. This is a cyber activity when the sent information contains a sequence of (self-executing) software code that prompts an effect somewhere else. However, it is not a space activity, as long as it has no effect on the operation of the satellite or the operation of its payload.

Satellite communications show that cyber activities become space activities only, when they have an effect in space or on space objects. A radio signal of a cyber activity that merely traverses through outer space is not sufficient.

4.1.4 Satellite Navigation

Satellite navigation uses communication technology, but goes further than this. Navigation satellites broadcast highly precise radio signals with information on the satellite's location and timing. This means, a navigation satellite operator, at the moment governmental bodies only, provides signal content. At that point, the role of a navigation satellite operator reaches beyond that of a communication satellite operator who provides only a communication pipeline. Consequently, the broadcast of a location and timing signal from a navigation satellite in space is a space activity.

However, these broadcast signals from space do not themselves determine the location of a user. The user's navigation receiver on the Earth does the active part. This unit receives the broadcasts from a number of satellites simultaneously and it uses the signal content (satellite location and timing) and differences in signal run times, to calculate the user's location. This activity on Earth is based on (information) products from space activities,[18] but it is not a space activity by itself.

The activities of the control segment of a navigation satellite system on the Earth that controls and calibrates the space-based navigation payloads are space activities. The command and control signals for accomplishing this function also qualify as a cyber activity.

4.1.5. Activities in Outer Space

Activities in outer space are a broad category. It reaches beyond the operation of space objects and includes activities of humans in space.

At first glance, one may think that every activity of humans in space is a space activity. This is true, as long as we look only at an astronaut's physical activity. But cyber activities of astronauts performed in outer space are a game changer. Whether a cyber activity initiated by an astronaut on-board the space station is also a space activity, depends on the location where the resulting effect occurs. If the resulting effect is on the space station, on another space object, or somewhere else in outer space, the astronaut's cyber activity qualifies as a space activity.

If, however, the effect of a cyber activity initiated in space occurs on Earth, it cannot be a space activity. An example could be the unauthorized access of

18 Also related with these aspects is the question of liability in satellite navigation, for more details see Stefan A. Kaiser, Satellite Navigation Systems: The Impact of Interoperability, XXXVII AASL 2012, 369, 387.
Re-print: von der Dunk (ed.), International Space Law, International Law series, Edward Elgar Publishing, 2018.

an on-line bank account on Earth from a computer on board the International Space Station.[19]

4.2. Authorized and Non-Authorized Cyber Activities in Outer Space

Considering that certain cyber activities can also be space activities, States bear responsibility for them under Article VI OST. This should not pose a problem. To the contrary, the command and control actions of a ground control centre that have an effect on a space object can be considered as a typical space activity.

Another complication arises, when such cyber activities with effects on space objects or in outer space are not authorized (or are malicious), for example by hacking the network of a space operator. Following the definitions above, also this non-authorized cyber activity is a space activity, regardless of the missing authorization. Consequently, Article VI OST would make that State responsible to whom the cyber activity can be attributed.[20]

5. Conclusion

As a conclusion, the following definitions and principles can be deducted:

- There is no internationally agreed definition of space activities.
- The literature and national legislation suggest that space activities encompass the launching, operation and return of space objects (including the related command, control and guidance actions from Earth), and activities that happen in Outer Space.
- Transmissions of information that merely traverse outer space without having an effect on a space object do not qualify as space activities.
- The processing and refinement on Earth of information products that originate from space activities are not space activities.
- There is no internationally agreed definition of cyber activities.
- Cyber activities are performed with information that execute logical functions, i.e. they comprise program files/self-executing code.
- Cyber activities depend on and are performed through a physical infrastructure (networks and computers). The networks span across air, land, sea and Outer Space and comprise wireless network links.

19 Accusations in 2019 against an astronaut to that effect were unfounded. New York Times, NASA Astronaut Anne McClain accused by spouse of crime in space, 23 August 2019, https://www.nytimes.com/2019/08/23/us/astronaut-space-investigation.html.

20 For an adjustment and re-allocation of responsibility and liability in such cases, see Stefan A. Kaiser, Martha Mejía-Kaiser, Cyber Security in Air and Space Law, ZLW 2015, 396, 405.

- Cyber activities have effects either in cyberspace (e.g. effects on digital data) or in the physical domains (e.g. 'internet of things').
- Disruptions of the physical infrastructure, through effects from outside do not qualify as cyber activity, e.g. physical disruption of a cable.
- Jamming of a radio link has a similar effect from the outside on the infrastructure of cyber activities – and not through a network - like the physical disruption of the physical infrastructure. Jamming is therefore not a cyber activity.
- Spoofing injects false data into functionalities like radio surveillance or navigation through digital data formats, but spoofing is not necessarily performed in and through a network.
- Regardless from where it is prompted, a cyber activity qualifies as a space activity when it has an effect on a space object or in outer space.
- An unauthorized (malicious) cyber activity that has an effect on a space object or in Outer Space qualifies as a space activity.

These definitions and principles can help to explain when cyber activities are space activities. This can serve as a basis for an improved understanding of the responsibility of States under Article VI OST in case of authorized and non-authorized cyber actions that qualify as space activities.