In Search of an International Public Order for Cyber Activities

*Stefan A. Kaiser**

Abstract

Despite the increasing influence of cyber activities on our everyday lives, researchers encounter difficulties in understanding this subject matter and in legally qualifying these activities and their effects. Current discussions tend to concentrate on distinct aspects, which lead to a fragmented, rather than a holistic understanding of the legal aspects of cyber activities. This paper approaches the legal dimension of cyber activities from a more general direction and searches for elements and legal principles that may be found in international law, including space law, and can apply to cyber activities.

INTRODUCTION

1. In Search of a Definition

Before searching for an international public order for cyber activities we need to define what we mean when we speak of 'cyber' or 'cyber activities'. The notion of 'cyber' is inconsistently used in different contexts. Perhaps the most meaningful etymological root leads to the mathematician and philosopher Norbert Wiener who created the term 'cybernetics' in 1948.[1] In an interdisciplinary manner, his term 'cybernetics' combines automated control mechanisms with communication and the impact on living beings. This early concept is farsighted, because Norbert Wiener built a bridge between computing based servomechanisms and neuroscience, psychopathology and society.

Even today there is no internationally agreed definition of 'cyber'. However, some players have attempted to define sub-sets thereof. The US Air Force defines 'cyber-space' as

* LLM (McGill). Wassenberg, Germany, stefanakaiser@aol.com

1 Norbert Wiener, Cybernetics: Or Control and Communication in the Animal and the Machine. Paris, Cambridge, Mass., 1948.

> "*a 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.*"[2]

The International Telecommunication Union defines 'cybersecurity' as

> *"the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise … Availability, Integrity …, Confidentiality."*[3]

Interestingly, also the Convention on Cybercrime[4] does not define the term 'cyber'. It defines a list of criminal offenses, like illegal access and interception, data and system interference, misuse of devices, computer-related forgery and fraud, etc., but without relying on the terms of 'cyber' or 'cyber activities'.

2. Fragmented Approach

It is thus not surprising that today's discussions, just like the 'cyber' definitions, tend to concentrate on distinct aspects, and do not approach the legal aspects of cyber activities in a generic manner. Some of these aspects are:

- the law of the internet,
- cyber security,
- cyber activities in armed conflict,
- automation of kinetic processes,
- automation of information processing,
- privacy and data protection.

2 US Air Force Doctrine, Annex 3-12, Cyber Operations, Introduction, 30 Nov 2011, https://doctrine.af.mil/download.jsp?filename=3-12-D01-CYBER-Introduction.pdf (accessed on 03 August 2018)

3 International Telecommunication Union, Telecommunication Standardization Sector, ITU-T X.1205, Definition of cybersecurity, Overview of cybersecurity, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

4 Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series - No. 185; 61 accessions in September 2018, in force since 1 July 2004.

Whereas all of these aspects have their meaning in the own right, only a holistic methodology can capture the breadth of aspects required to lay the foundations of an international public order for cyber activities.

(a) The law of cyber activities is broader than the law of the internet. The term of internet law is not clear cut and often used as a bracket for online sales and business transactions and related issues of competition law, intellectual property and personal rights.[5] Even though the internet is today the most important global data networking infrastructure, cyber activities in other (segregated) networks need to be considered as well, and also cyber activities that introduce malware, for example on storage media, to non-connected networks.
(b) There can be no doubt that cybersecurity is an item of high importance, because malicious cyber activities can affect all aspects of our lives, directly or indirectly. For that reason, organizations like the ITU, the European Union[6] and States strive to raise the level of security of network and information systems against unauthorized cyber interference in a pro-active manner, and not only by reactive means of criminal prosecution, for example on the basis of the Convention on Cybercrime Convention. The prevention of *unauthorized* or *malicious* cyber activities, as important as it is, shall however not divert our attention from the foremost purpose of information technologies: to safeguard *legitimate* cyber activities for all fair-minded users who rely on the systems and networks in good faith.

(c) Currently a lot of the legal literature on cyber activities focuses on the (the law of) armed conflict or, more commonly, on cyber-warfare.[7] This is a consequence of the early equipment of military forces with computer and information technology and the ongoing trend to 'network-centric' warfare, which means both, an increasing cyber vulnerability of military forces, but also cyber activities as a means and method of war. As important as cyber activities are in the law of armed conflict, this discussion should not overshadow the implications of cyber activities during peacetime and their meaning in international law outside of armed conflict.[8]

5 See for example Helmut Hoffmann, Die Entwicklung des Internetrechts bis Mitte 2018, ZLW 2018, 2453.
6 See for example the European Union Directive on security of network and information systems (NIS Directive), Directive (EU) 2016/1148.
7 Most prominently, Michael Schmitt (ed.), Tallinn Manual on the International Law applicable to Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge, 2013.
8 See Katharina Ziolkowski (ed), Peacetime Regime for State Activities in Cyberspace, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2013, https://www.diplomacy.edu/resources/books/peacetime-regime-state-activities-cyberspace

(d) In the context of the law of cyber activities, the automation of kinetic processes and autonomous systems become increasingly important. In combination with today's technology, many of these applications are directly linked to cyber activities, for example through the so-called 'internet of things'. Typically, automation and autonomous processes do not act in isolation, but need inputs from the surrounding world and from other stakeholders by network exchanges. What may appear just as a new application of existing information exchanges and data applications over the internet, is nothing conceptually new. It is indeed one of the aspects of Norbert Wiener's cybernetics. In 1948, his concept of automated control mechanisms through communication tools did first of all relate to real-world kinetic processes, just as we see them today on the 'internet of things'.

(e) Related to the automation of kinetic processes is the automation of information processing. It is often based on the collection of large amounts of data, also referred to as 'big data',[9] including metadata,[10] which is analysed by algorithms[11] with the intention to predict real world events, including human behaviour.[12] The automation of information processing partly overlaps with artificial intelligence,[13] which is a broader notion and can also apply to automated kinetic processes.

(f) Privacy and data protection is a field that has continuously gained importance with the advancement of computer technology, networking and their everyday application to all aspects of the personal lives of a society. The

9 Definitions of 'big data' often contain the so-called three 'vs' to describe the quantitative dimensions of volume, velocity and variety. Some include veracity, as a fourth 'v', to signify quality, certainty and trustfulness of data; Jonathan Stuart Ward, Adam Barker, Undefined By Data: A Survey of Big Data Definitions, https://arxiv.org/pdf/1309.5821.pdf (accessed 03 August 2018)

10 Metadata describes the context of data and is important for the interpretation of large amounts of data. Metadata is "structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information", National Information Standards Organization, Understanding Metadata, 2017.

11 Algorithms are finite sequences of unambiguous mathematical instruction sets to perform a specific task. Their stringent mathematical structure leads from the same input to the same output.

12 Wagner and Vieth consider algorithms as instruments of power and they deem algorithmic decisions not less prone to errors and prejudice as human decision-making; Kilian Vieth, Ben Wagner, Teilhabe, ausgerechnet: Wie algorithmische Prozesse Teilhabechancen beeinflussen können, Bertelsmann Stiftung, 2017, 8, 11, available at:https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/Graue Publikationen/Teilhabe_ausgerechnet.pdf (accessed on 03 August 2018).

13 Artificial intelligence can be understood as a discipline of information and computational science dealing with the automation of intelligent behaviour that mirrors human behaviour.

protection of personal data[14] is an important legal element in the context of cyber activities, but it does not encompass the full breadth of protection of all data subjects affected by cyber activities, including individuals, commercial users, industry and governments.

The absence of a generic definition of 'cyber' and the fragmented approach to certain technical and legal aspects of cyber activities show the need for a more general, all-encompassing methodology to address the legal regime applicable to cyber activities.

II. CYBER SPACE VERSUS CYBER ACTIVITIES

The concept of 'cyber space' allows to tackle cyber activities in a broad manner, without the need to define what is actually meant. The underlying idea is simple. All activities undertaken in that 'cyber space' fall within its scope. As simple as this method appears, it raises two principle problems:

- 'Cyber space' is a technical fiction that has nothing in common with a physical three-dimensional space and it is not clear where it extends and where are its limits.
- In a legal context, the concept of 'cyber space' is prone to be misconstrued as if it could establish the jurisdiction and control regimes that we apply in existing physical spaces, like in national or international airspace or in outer space.

1. The Fiction of 'Cyber Space'

In regard to the technical fiction of a quasi-physical 'cyber space', we need to take a closer look at the way how it is used. We can say for sure about the functioning of 'cyber space' that a person, located at a physical place, makes an input, that can have an impact on another person, and its rights, located somewhere else. Input and output are connected by 'cyber space' and can take place in different States and jurisdictions. The output can take different forms. If an automated kinetic process is involved, it may have a direct physical effect on a person or its property at a defined physical location. It may also consist of an impact on information related to the person affecting, directly or indirectly, his personal, social, economic, cultural, or political rights. It is apparent that this effect alone is not sufficiently precise to characterize an activity in 'cyber space', as opposed to other non-cyber activities.

14 As a recent prominent example in the European Union, see the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, which entered into force on 25 May 2018.

2. The Computer Network Layer Models

Of help can be the so-called layer models of the internet and other computer networks with a similar architecture. Whereas these models explain network functionalities with more or less layers, depending on the level of detail,[15] for understanding the legal ramification of cyber space versus cyber activities, a simplified model reduced to three-layers can help. It consists of the physical layer, the data link / network / transport layer and the application layer.[16]

The physical layer consists of hardware, like computers, network hardware, telecommunication equipment, including copper cables, fibre-optics and also wireless data links, including satellites. The physical layer is installed in the territory of States, but can also rest on the seabed or be located in outer space.

The data link /network / transport layer combined here for easier understanding serves the (software-based) core communication functions that logically connects all end-user devices by different, layer specific, communication protocols[17] and sends information, layer trough layer, among selected end user equipment.

The application layer is the one mostly visible for users, because this is "*where applications work and produce data over the network to their communication peers* ...".[18] The application layer becomes increasingly important, because by application layer protocols it can control end-user devices of the 'internet of things'.

3. Defining 'Cyber Activities'

Having delved into these details, one may define 'cyber activities' 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. Following this line of thought, not every effect on digital information content or application should be deemed to be a 'cyber activity', but only a networked action, or more precisely the use of the data link / network /transport layer and the related communication protocol, which affects the digital content or applications. For clarification, an action affecting the physical layer, for example by cutting off the electrical power or by

15 There are numerous computer network layer models, including the more detailed OSI (Open Systems Interconnect) model with 7 layers, defined by ISO (International Organization for Standardization) standard 7498.

16 For more details of the various layer models, see Emin Caliskan, Raimo Peterson, Technical Defence Methods, Tools, Techniques and Effects, in: Katharina Ziolkowski (ed), *supra* note 7, p. 62-65.

17 These communication signal protocols include, among others, for the transport layer: the Transport Control Protocol (TCP) and the User Datagram Protocol (UDP), for the network layer: the Internet Protocol (IP, currently up to version 6 IPv6), for the data link layer: Ethernet and Point to Point Protocol (PPP).

18 Emin Caliskan, Raimo Peterson, *supra* note 15, p. 62.

physically damaging hardware, should not qualify as a 'cyber activity', since it is not undertaken by an action that uses digital information as a tool which is transmitted through a network and it does not use a communication protocol.

4. Jurisdiction and Control

As an additional effect, the concept of 'cyber activity', as opposed to 'cyber space', avoids confusion in regard to jurisdiction and control regimes of States in existing physical spaces. Trying to establish jurisdiction and control over physical system elements, misses the crucial characteristics of 'cyber activities': the role of the transport/logical layer or protocol.

Packaged information from one to another end-user device can be sent over numerous different paths, using physical infrastructure in many different countries. It can likewise be stored, long term or short term, on physical devices and servers in many different countries. Consequently, trying to 'spatially' locate a 'cyber activity' within the territorial jurisdiction of a State becomes meaningless. 'Cyber space' is a technical fiction. Unlike State frontiers, it has no limits or borders. A similar spatial fiction is used for the term 'cloud' to pretend that de-centralized data storage is achieved in a common physical place. But this should not create the impression, that in 'cyber space' there is a legal vacuum.

'Cyber activities' are prompted by human activity, directly or indirectly, and this is the key aspect that State jurisdiction and control needs to attach to. The notion of 'cyber space' tends to obscure the concept that humans need to be accountable for their actions. Humans have fundamental rights which are not to be curtailed by the fact that a technical environment creates difficulties in identifying chains of causation and in attributing human actions. For legal considerations, the concept of 'cyber activities', as opposed to activities in 'cyber space', should therefore be the preferred choice to support the role of law in establishing a public order for human activity.

III. GENERAL PRINCIPLES

When speaking of the legal characteristics of cyber activities, we should foremost pay attention to the role cyber capabilities increasingly play in our society, and only as a subsequent step engage in the protection against malicious cyber activities. Information exchanges over networks, also in combination with a growing degree of the automation, have become vital for our social, cultural and political lives, for economic, industrial and scientific activities, and for all kinds of infrastructure, health, safety and security. An international public order for cyber activities therefore needs to be centred around an assurance for members of the society to partake in legitimate cyber activities and to use the cyber infrastructure in a fair and non-discriminatory manner, as a means to exercise their fundamental rights and freedoms. The ability for the public to engage in cyber activities reaches further than the

'classical' freedom of opinion and expression - the "*freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers*"[19] and thus to partake in the social, cultural and political life. Also the more technically oriented "*right of the public to use the international telecommunication service by public correspondence*" of Article 33 of the Constitution of the International Telecommunication Union,[20] is limited to the traditional scope of assuring expression and information.

1. Towards Freedom of Cyber Activities

With steadily increasing networked information exchanges, it is clear that cyber activities can be a key enabler for the exercise of the freedoms of religion, education and science, the exercise of professional activities and the participation in commerce. Through networked application software, automation and autonomous systems and the internet of things, cyber activities become crucial for the exercise of fundamental rights and freedoms in the physical world, including those of life and health (for example telemedicine), and property (for example security and surveillance functions).

(a) It becomes therefore apparent that the public needs to have a right to undertake cyber activities and use cyber infrastructure to exercise their full range of fundamental rights and freedoms that can be carried out by such cyber activities. It is debatable, if the freedom to exercise cyber activities is a new, generic freedom, but rather a derivative of a broad range of already existing freedoms. But most importantly, in a public order for cyber activities, cyber capabilities of legal subjects and their use of cyber infrastructure need to be understood as an exercise of fundamental rights and freedoms.

(b) Along these lines, the Internet Governance Principles of the Council of Europe of 2011 recognize that

> "*Internet governance arrangements must ensure the protection of all fundamental rights and freedoms and affirm their universality, indivisibility, interdependence and interrelation in accordance with international human rights law. They must also ensure full respect for democracy and the rule of law and should promote sustainable development. …*"[21]

19 Article 19, Universal Declaration of Human Rights, UNGA Res. 217A (III), U.N. Doc A/810 at 71 (1948); See also Article 19, International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966.

20 Article 33 (179 PP-98), Constitution of the International Telecommunication Union, ATS (1994) 28; BTS 24 (1996).

21 Council of Europe, Declaration by the Committee of Ministers on Internet governance principles, adopted by the Committee of Ministers on 21 September 2011

In regard to internet users, the same declaration stipulates that they

> *"… should be fully empowered to exercise their fundamental rights and freedoms, make informed decisions and participate in Internet governance arrangements, in particular in governance mechanisms and in the development of Internet-related public policy, in full confidence and freedom."*[22]

2. Peaceful Purposes

Aviation officials and representatives from States and regional and international organizations took another interesting approach in the Declaration on Cybersecurity in Civil Aviation in 2017.[23] They declared[24] under section 2. of that document that "*Cyber capabilities applied to aviation should be used exclusively for peaceful purposes and only for the benefit of improving safety, efficiency and security*".

Noteworthy are two aspects:

- the reference to the concept of 'peaceful purposes',
- and the definition of a regime for cyber capabilities from the perspective of legitimate users for peaceful purposes, as opposed to defining non-legitimate uses for measures of cyber security.

The concept of 'peaceful purposes' is repeatedly mentioned in the Outer Space Treaty,[25] most prominently in the Preamble and Article IV. This concept is at the verge of civil and military space activities that have co-existed from the very beginning of the space age. Unfortunately, even after 50 years since the signature of the Outer Space Treaty, state practice has not shaped more detailed characteristics of this concept. Different interpretations of 'peaceful purposes' define it either as 'non-military' or 'non-weaponized' or 'non-aggressive'.[26]

The Declaration on Cybersecurity in Civil Aviation is more ground breaking, because it positively postulates a regime for the use of cyber capabilities for peaceful purposes and for the benefit of improving safety, efficiency and

---

at the 1121st meeting of the Ministers' Deputies, Principle 1. on Human rights, democracy and the rule of law

22 *Ibid*, Principle 4. on empowerment of internet users.

23 Declaration on Cybersecurity in Civil Aviation, Dubai, United Arab Emirates, 6 April 2017.

24 An aspect not discussed here is the legal effect of this declaration by officials and representatives from certain States and regional and international organizations.

25 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.

26 Stephan Hobe/ Niklas Hedman, Preamble, sec. 9 in Hobe, Schmidt-Tedd, Schrogl (eds.), Cologne Commentary on Space Law, Volume 1 (Outer Space Treaty), Cologne, 2009.

security. This methodical step attempts to break the mould of defining, on the negative side, malicious or non-peaceful cyber activities for the purpose of cyber security. In that sense, the approach followed in said declaration underpins the positive concept that the foremost reason of a legal framework for cyber activities is to enable all stakeholders to use cyber infrastructures for their legitimate – peaceful - purposes and in exercise of their (cyber) freedoms.

3. Other Space Law Principles

In 2013 Mejía-Kaiser submitted an even more comprehensive proposal to apply space law principles to cyber activities. Because cyberspace "*serves the whole international community and, due to the increasing dependency of the world economy and critical safety functions, must be kept operational*",[27] she concluded that the following principles of the Outer Space Treaty should also apply to its use:

- Article I (1) on the benefit and in the interest of all countries irrespective of their degree of economic or scientific development,
- Article I (2) on non-discrimination on a basis of equality and in accordance with international law, and
- Article III on maintaining international peace and security and promoting international cooperation and understanding.[28]

This package of principles could be a good starting point for an international public order for cyber activities.

IV. CYBER SECURITY

Cyber security is a complementary element to the exercise of fundamental rights and freedoms of users who carry out cyber activities. The reason for cyber security is the protection of these users' rights and freedoms against malicious cyber activities of others. Cyber security includes technical and regulatory measures to prevent unauthorized cyber interference with computers, networks and information. The regulatory measures comprise procedural and substantive measures, whose effects can either be pro-active or re-active.[29]

27 Martha Mejía-Kaiser, Space Law and Unauthorised Cyber Activities, in Katharina Ziolkowski (ed), *supra* note 7, 349, 371.
28 *Ibid.*
29 For the more detailed definition of cyber security by ITU, see *supra* I.1.

1. Protection of all Fundamental Rights

Cybersecurity aims at vulnerabilities that follow from an increasing dependency on a combination of (mobile) computers and information technology systems, automation and connectivity. The scope of protection of cyber security is therefore as broad as the rights and freedoms of those who legitimately undertake cyber activities. With the words of the Council of Europe, it includes the protection of all fundamental rights and freedoms in accordance with international human rights law, the full respect for democracy and the rule of law.[30]

2. The NIS Directive

The European Union's regulatory approach to cyber security focusses on procedures. The Directive on Network and Information Security (NIS Directive)[31] applies across many sectors[32] and seeks to improve cybersecurity capabilities at the national level embedded in an increased cooperation at EU-level,[33] by risk management and incident reporting obligations for operators of essential services and digital service providers.[34] Concentrating on procedures, the NIS Directive does, however, not establish substantive requirements for hardware or software, but refers instead to "European or internationally accepted standards relevant to the security of NIS"[35]. Another shortcoming of the directive is its narrow scope which relates to service interruption only,[36] but does not consider automated applications with a safety impact.

3. Reference to Unspecified Standards

When the NIS Directive refers to unspecified standards, like 'accepted security standards' without providing additional substance, this bears the risk of implementing the commercial practices and products of the information industry, instead of formulating independent substantive rules on hardware, software and the systems as such. That security standards are 'accepted' does not necessarily mean they are accepted by States, but that they may represent industry practice. This means that commercial product solutions may lead the way for tackling cyber security shortcomings that are the result of the same industry and its products.

30 See *supra* III.1.
31 Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.
32 *Ibid,* Annex II lists the sectors of energy, transport, banking, financial market, health, drinking water, digital infrastructure.
33 *Ibid,* chapters II, III.
34 *Ibid,* chapters IV, V.
35 *Ibid,* Article 19.
36 *Ibid,* Article 6.

4. Safety Standards versus Security Standards

An additional complication arises from automated applications and their impact on physical safety. Existing physical safety standards are not to be confused with the standards required for assuring cyber security. The difference between the two is rooted in the heightened level of protection measures against intentional security violations, especially those that exploit security gaps. For compliance with existing physical safety standards it suffices to demonstrate with reasonable probability that non-intentional interference will not impact physical safety. However, cyber security standards need to be stricter and assure with reasonable probability that an attacker cannot intentionally exploit a security gap of safety critical systems.[37]

V. ATTRIBUTION

The attribution of cyber activities raises factual and legal issues. Attribution is the link that connects cyber activities with natural or legal persons. As subjects of law, persons have rights and freedoms when performing cyber activities, but they also have obligations and responsibilities, for example to abstain from interfering with the rights of others.

1. Factual Attribution

Contrary to the widespread perception that the originators cannot be identified and malicious acts cannot be factually attributed to perpetrators, cyber activities leave traces in metadata, similar to fingerprints, that show commonalities of cyber activities originating from the same individual.[38] The factual attribution is thus a matter of methods for securing evidence and of forensic analysis. This may be a cumbersome exercise, but in substance not so much different to evidence procedures practiced in other legal proceedings.

2. Legal Attribution and Jurisdiction

The legal attribution becomes foremost relevant for establishing (legal) accountability of persons for cyber activities who have violated the rights and freedoms of others. Besides intricate evidence procedures, cyber activities typically span across State borders and pose jurisdictional issues for the prosecution of perpetrators.

States have jurisdiction over their nationals, but also over non-nationals who commit unlawful acts within their area of jurisdiction – this jurisdiction is in most cases exercised for acts committed in their territory. As elaborated above, the concept of 'cyber space' is not suitable for establishing jurisdiction.

37 Stefan A. Kaiser, Martha Mejía-Kaiser, Cyber Security in Air and Space Law, ZLW 2015, 396, 400.

38 Hakan Tanriverdi, Der Mythos vom anonymen Hacker wankt, Süddeutsche Zeitung, 16 February 2018, http://www.sueddeutsche.de/digital/cyberangriffe-der-mythos-vom-anonymen-hacken-wankt-1.3868826 (last accessed 03 August 2018).

The nexus for jurisdiction is instead to be derived from the person who undertook or was affected by the cyber activity in question. Based on that, States can typically establish jurisdiction either based on the nationality of the offender or by the concepts of *locus actus* or *locus injuriae*.

3. Legal Attribution to States

As a general principle of public international law, States are not responsible for acts of their nationals or for non-nationals committing crimes or wrongful acts in their territory, be it by cyber or other activities. However, States increasingly engage in cyber activities themselves, by State organs or persons or entities exercising elements of governmental authority, which can be legally attributed to them.[39] For these cyber activities of States the same (national) rules for the protection of the fundamental rights and freedoms like for any other acts of State.

Additional complications pose so-called hybrid activities and threats when

> *"state and non-state actors ..* [challenge].. *countries and institutions they see as a threat, opponent or competitor to their interests and goals. The range of methods and activities is wide, including: influencing information; logistical weaknesses like energy supply pipelines; economic and trade-related blackmail; undermining international institutions by rendering rules ineffective; terrorism or increasing insecurity."* [40]

Depending on the circumstances, this kind of conduct can be attributed to a State, if it is directed or controlled by a State or carried out in the absence or default of its official authorities.[41] To that end, *"States should agree on the primary responsibility to refrain from tolerating, coordinating and/or engaging in whatever form in cyber activities"* that affect the rights of third parties, for example when seizing *"a space object without the authorization of the launching State"*[42]
Such an attribution of cyber activities to a State can also be supported under the standard of 'overall control' established in the appeal of the *Tadic* case by the International Criminal Tribunal of the former Yugoslavia (ICTY), based on a State supporting armed groups by planning, coordinating and organizing their activities.[43]

---

39 Articles 4 and 5, International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Yearbook of the International Law Commission, 2001, vol. II (Part Two).

40 The European Centre of Excellence for Countering Hybrid Threats , Hybrid Threats, https://www.hybridcoe.fi/hybrid-threats/ (last accessed 08 August 2018).

41 Articles 8 and 9, International Law Commission, *supra* note 38.

42 Stefan A. Kaiser, Martha Mejía-Kaiser, *supra* note 36 at 408.

43 Stephan Hobe, Rada Popova, Law in Cyberspace?, ZLW 2018, 254, 273, 274; the Prosecutor v. Dusko Tadic, ICTY Appeals Chamber, judgement IT 94-1-A, 15 July 1999, ILM 38 (1999), 1518.

VI. THE ROLE OF STATES

It is the role of States to safeguard the fundamental rights and freedoms of persons under their jurisdiction. This safeguarding function applies not only as a protection for natural and legal persons against acts of States. For maintaining public order and security within their jurisdiction, States furthermore have to uphold fundamental rights and freedoms also in the relationships of persons among each other. The same is valid for cyber activities, even when States do neither provide the cyber infrastructure nor engage in cyber activities in relation to the persons affected. Cyber infrastructure needs to be seen here as any other infrastructure or public utility for which States have to establish a governance regime to warrant fair and equal access and participation, assure non-discrimination and protect the fundamental rights and freedoms of all subjects. Considering the practical difficulties for an international infrastructure where cyber activities often span across jurisdictional borders, States have to take due care, as not to harm persons outside of their jurisdiction.

Within the multi-stakeholder environment of governments, the private sector, civil society, the technical community and users, the Council of Europe acknowledged in its internet governance principles the following responsibilities of States:

> *"States have rights and responsibilities with regard to international Internet-related public policy issues. In the exercise of their sovereignty rights, states should, subject to international law, refrain from any action that would directly or indirectly harm persons or entities outside of their territorial jurisdiction. Furthermore, any national decision or action amounting to a restriction of fundamental rights should comply with international obligations and in particular be based on law, be necessary in a democratic society and fully respect the principles of proportionality and the right of independent appeal, surrounded by appropriate legal and due process safeguards."*[44]

Cyber security is a sub-set of security for which States bear the ultimate responsibility. It might have been the perception that the internet is just another means for exercising the fundamental rights of expression and information and, in order to avoid interference with these freedoms, States were inclined to follow a *laissez-faire* policy. However, since it has become clear that cyber activities encompass the exercise of all fundamental rights and increasingly are linked to physical actions, States have to accept their responsibility for cyber security, just like for other aspects of physical security.

44 *Supra* note 20, Principle 3.

VII. CONCLUSIONS

The search for a coherent international public order for cyber activities faces obstacles, since there is no agreed definition of 'cyber' and so far legal aspects have been addressed in a fragmented manner.

(a) It is therefore proposed to use 'cyber activities' as the starting point for defining a holistic cyber regime, as opposed to 'cyber space'. By putting 'cyber activities' into the centre, a link is created to human activities, to which State jurisdiction and control can be attached. There is no anonymous cyber space, absent of State jurisdiction.

(b) A public order for cyber activities should foremost be rooted in the right to undertake cyber activities and to use cyber infrastructure in a fair and non-discriminatory manner to exercise the full range of fundamental rights and freedoms that can be carried out by such cyber activities. One could speak of the freedom of cyber activities.

(c) A number of principles of public international law that are applied to space law are also suitable for cyber activities, to include the principles of peaceful purposes, the principle of benefit and interest of all countries, non-discrimination, accordance with international law, maintaining international peace and security, and promoting international cooperation and understanding.

(d) Cyber security is only the flipside of the exercise of this freedom of cyber activities. Cyber security is the protection against malicious cyber activities which interfere with fundamental rights and freedoms exercised by cyber activities.

(e) Attribution is the link between cyber activities and persons and the root for the jurisdiction of States. For the factual attribution of cyber activities to persons, cyber forensics need to be further developed and applied, so that States can fulfil their role in cyber security. The legal conditions under which cyber activities may be attributed to States, other than those undertaken by State organs and representatives, need to be further developed.

(f) Even though we see a multi-stakeholder governance of the internet, States need to take a more active role in assuring the exercise of fundamental rights and freedoms of those who engage in cyber activities and they need to actively protect them against malicious cyber acts. In the existing multi-stakeholder environment, States need to overcome their *laissez-faire* posture and actively create a counter-balance to other actors. The increasing role of cyber activities require States to adjust their structures, rules and procedures in the legislative, executive and judicial branches.