# Cybersecurity Governance through Principles of International Law

*Abstract*

*Cybersecurity Governance has so far remained weak since the existing legal instruments of global organizations do not exercise an effective impact. Moreover, international legal principles such as the concept of public goods, the concept of shared spaces and the concept of State responsibility should be made fruitful. The contribution shows that such principles are suitable for giving guidelines at hand that support the efforts in the cybersecurity context. Thereby, soft law based on self-regulatory and co-regulatory approaches merits to be more intensively taken into account. In addition, capacity building and confidence building must be fostered apart from the higher emphasis on the sharing of best practices and of security/resilience standards implemented on the basis of the relevant normative guidelines.*

***Table of Contents***

The Internet as the most important global "infrastructure" is an environment in which international law, with all its perplexities, should be effectively and coherently applied. Yet the current approach of politicians, scholars and practitioners shows a pertaining reluctance to embrace the challenges posed by global cyber governance of the most important international electronic network.

## 1. Introduction

The integrity of the Internet depends on its proper functioning without technical interference and (unjustified) governmental intervention. During the last few years, different terms have been coined in order to describe such kind of integrity of the Internet. At the beginning, cybersecurity was the most commonly used word, followed by other terms such as cyberstability and cyber resilience; hereinafter, cybersecurity with remain the keyword of the international law considerations.

Cybersecurity refers to processes and measures protecting networks and data form cybercrimes. So far, no standard or universally accepted definition of the term cybersecurity is existing. As the Internet Society remarked, "as a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges and 'solutions' ranging from the technical to the legislative".[1] The International Telecommunications Union (ITU) defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions trainings, best practices, assurance and technologies that can be used to protect the cyber environment and the organizations' and users' assets".[2]

General security objectives include (i) confidentiality, (ii) integrity, and (iii) availability, also known as the "CIA" triad in the information security industry. Thereby, confidentiality means that information is not improperly disclosed to unauthorized individuals, processes or devices; integrity refers to information being protected against unauthorized modification or destruction; availability pertains to a timely and reliable access to

[1] Karen O'Donoghue, Some Perspectives on Cybersecurity, 2012, Internet Society, https://www.internetsociety.org/resources/doc/2012/some-perspectives-on-cybersecurity-2012/.

[2] ITU Definition: http://www.itu.int/n/ITU-T/studygroups/com17/Pages/Cybersecurity.aspx.

data and information for authorized users.[3] The International Organization for Standardization (ISO) defines "information security" as the preservation of confidentiality and availability in its "ISO/IEC (International Electrotechnical Commission) 27'000 Family of Information Security Management System Standards". Cybersecurity encompasses not only the protection of information and data but also the protection of assets that are non-information based and vulnerable to threats.

Usually, the cyberthreat landscape is described by using a linear approach that distinguishes between (i) threat agents, (ii) threat tools, and (iii) threat types.[4] While such categorization is useful for certain legal qualification, it does not aim to paint a comprehensive picture of the very complex nature and characteristics of cyberthreats. The array of external and internal agents threatening cybersecurity is mostly very wide, going from Nation States to hackers and insiders. Threat tools encompass malware and its variance as well as botnets. Threat types include information modification or misuse, information destruction, unauthorized access, data breach, data theft and distributed denial-of-service.

The term "governance" can be traced back to the Greek word "kybernetes", the "steersman", leading over the Latin word "gubernator" to the English notion "governor" addressing aspects of steering and governing behavior.[5] Consequently, cybersecurity governance looks at the measures taken by the concerned players with the objective to protect information and data as well as the underlying assets and infrastructure.

This contribution does not analyze the details of existing legal instruments (or their preparatory documents) combatting cybercrime, but only mentions their existence and some key messages (chapter 2). Moreover, the contribution has the objective to assess in more depth to what extent the established and widely accepted international legal principles (in particular the concept of global public goods, of shared spaces and of State responsibility) can contribute to an acceptable cybersecurity governance (chapter 3); such a "regime" of international principles could then be supported by the already existing self-regulatory initiatives (chapter 4). Specific challenges are posed by

[3] Weber, 2020, 281.
[4] See the detailed description given by Weber/Studer, 2016, 717/18, with further references.
[5] Weber, 2009, 2.

the implementation of international principles (chapter 5). An outlook closes the contribution (chapter 6).

## 2. Limited Efficacy of Existing Cybercrime Instruments

For decades, international and regional organizations have tried to develop legal instruments that could harmonize the regulatory standards in the field of cybersecurity prevention.[6] Some efforts have been (partly) successful, mainly if implemented by sector-specific international organizations (ITU, WTO).[7]

On the global level, legal instruments intending to combat cybercrime are discussed for quite some time. Already five United Nations Group of Governmental Experts (UNGGE) have exchanged ideas and published reports, without, however, agreeing on binding principles.[8] The most forward-looking statement has been made by the fourth UNGGE:[9]

"1. In der use of ICTs, States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States.

2. Obligations under international law are applicable to State use of ICTs and States must comply with their obligations to respect and protect human rights and fundamental freedoms.

3. States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-State actors to commit such acts.

4. The UN should play a leading role in promoting a dialog on the security of ICTs in their use by States, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behavior."

Two newly established groups are mandated to come up with further proposals by 2021.[10] At the moment, the outcome of these expert group efforts is unclear, however,

---

6 For an overview see Weber, 2020, 284 et seq.
7 Specific security provisions are contained in the ITU- and WTO-Agreements (for further details Weber, 2020, 288-290).
8 For further details see Kulesza/Weber, 2020, …; Henriksen, 2019, 4 et seq.
9 UN Doc. A/70/174.
10 Resolution, A/C.1/73/L.37 and A/C/1/73/L.27 Rev. 1.

as the assessment of the fourth UNGGE shows, the principles of international law play a major role, justifying a deeper analysis of relevant international legal principles.

Regional approaches have been more successful: The Council of Europe (CoE) adopted the (Budapest) Convention on Cybercrime in 2001 (being partly outdated in the meantime) encompassing now more than 60 ratifying States (also outside of Europe)[11] and the European Union (EU) released the Network and Information Society (NIS) Directive[12] in 2016 (with the main objectives/measures of improving [i] national cybersecurity capabilities, [ii] the EU-level-cooperation and [iii] the security and incident notification requirements) as well as the Cybersecurity Act in 2019.[13] As a noteworthy remark it may be added that "digital infrastructure" is named alongside to energy, transport, banking, health sector and drinking water supply as a "critical infrastructure" in Annex III of the NIS-Directive.[14]

Reality shows that in particular the efforts on the global level for the implementation of cybercrime regulations have failed to be successful. Even the CoE Cybercrime Convention did not have remarkable effects.[15] The EU legal instruments are limited to a regional scope of application.

## 3. Adherence to International Legal Principles

In principle, it is not contested that new norms and policies should be developed in order to enhance the global resilience, stability and security of the Internet. This statement is commonly accepted even if Martti Koskenniemi has skeptically noted a limited practical applicability of international law, not constituting on actual enforcement mechanism for a global consensus on values.[16] In November 2019, at the occasion of the Internet Governance Forum (IGF) in Berlin, the Global Commission on the Stability of Cyberspace (GCSC) has proposed a comprehensive Cyberstability Framework en-

[11] Council of Europe, Convention on Cybercrime, ETS no. 185, Budapest, November 2001.
[12] OJ 2016 L 119/1 of 4 May 2016.
[13] OJ 2019 L 151/15 of 7 June 2019.
[14] To the discussions in the context of Annex III. see Kulesza/Weber, 2017, 87.
[15] Clough, 2014, 701 et seq.; Weber, 2020, 283/84.
[16] Koskenniemi, 2009, 562 et seq.

compassing (1) multistakeholder engagement, (2) cyberstability principles, (3) the development and implementation of voluntary norms, (4) adherence to international law, (5) confidence building measures, (6) capacity building objectives and (7) the open promulgation and wide spread use of technical standards ensuring cyberstability.[17]

As will be outlined hereinafter, cybersecurity might be reasonably warranted if the international community is ready to accept some basic and common legal standards being applicable around the globe. Several theoretical models have been developed so far;[18] as most important international legal principles, the concepts (i) of global public goods, (ii) of shared values and (iii) of State responsibility will be further analyzed in the following sub-chapters.

### 3.1 Concept of Global Public Goods

One of the starting points for a discussion on protecting cybersecurity could be the concept of "global public good".[19] Although not perfectly aligned to the needs of cybersecurity and the network's architecture, it is worth a closer look. Ideally, global public goods are those which benefit humanity as a whole; accordingly, these goods should be advantageous to (i) more than one group of countries or geographic regions, to (ii) a broad spectrum of the global population, crossing population segments, and (iii) to present generations without jeopardizing the ability of future generations to meet their own needs.[20]

The idea of guaranteeing cybersecurity as a public core of the Internet or as a "global public good" can be perceived as a derivative of a policy concept: The ambiguous notion of "global public goods", as generated in the era of globalization, is derived from the economic literature on "public goods".[21] It refers to all globally available goods that are non-rivalrous (consumption does not influence the quantity available to others) and

---

17 Global Commission on the Stability of Cyberspace, 2019, 14.
18 See also Kulesza/Weber, 2020.
19 For a general overview see Kaul/Grunberg/Stern, 1999, 10 et seq.; Weber/Menoud, 2008, 24 et seq.; Shaffer, 2012, 675 et seq.; Krisch, 2014, 1 et seq.
20 Weber/Menoud, 2008, 24.
21 Krisch, 2014, 3 et seq.; see also International Task Force on Global Public Goods, Meeting Global Challenges: International Cooperation in the National Interest, Final Report, Stockholm 2006, 15.

non-excludable (their use cannot be prevented); the examples of global public goods include knowledge as well as the common heritage of mankind.[22]

International law in its classical form with its consent-based structure is not easily suitable to meet the requirements of the global public goods concept. Moreover, a structural bias exists; in particular, the Westphalian system leads to severe problems for this concept. As Nordhaus points out: "The requirement for unanimity is in reality a recipe for inaction. […] To the extent that global public goods may become more important in the decades ahead, one of our major challenges is to devise mechanisms that overcome the bias toward the status quo and the voluntary nature of current international law in life-threatening issues".[23] As will be shown hereinafter, the international law is not without solutions to such problems.[24]

Indeed, from an international law perspective, global public goods theories are not totally new. The idea of a certain "communality" already lies at the core of Roman law concepts of "*ius cogens*" or "*erga omnes*".[25] Similarly, the concept of "critical infrastructures" and their protection can serve as another or complementary point of reference.[26] In addition, the well-known "public interest" concept is also able to peremptorily impose binding obligations on States that have a similar foundation.[27] Based on these thoughts it can be argued that global public goods theories involve a broad approach that considers political economy implications besides legal aspects[28] and, therefore, merits attention in future discussions.

### 3.2 Concept of Shared Spaces

International cooperation on critical infrastructure protection is not the only analogy to be drawn from existing legal frameworks.[29] Equally, for example, the concept of shared

[22] Kulesza/Weber, 2017, 81/82.
[23] William N. Nordhaus, Paul Samuelson and Global Public Goods 8 (2005), http://www.econ.yale.edu/~nordhaus/homepage/homepage/PASandGPG.pdf.
[24] Krisch, 2014, 4.
[25] Weber/Menoud, 2008, 24.
[26] See below chapter 4.2.
[27] Weber, 2020, 304.
[28] Weber/Menoud, 2008, 25-27.
[29] Weber, 2014, 19.

spaces, to be used by all States in a uniform, non-harmful way is not new to the international community and in international relations. Already Grotius in the seventeenth century explained the law of all nations as the law "derived from nature, the common mother of us all, and whose sway extends over those who rule nations".[30]

Many global legal areas, constituting a "law on international spaces"[31], have turned out to be relevant over time. From a substantive perspective, it can be said that a feature common to the international spaces encompasses the obligation of peaceful use of resources and the principle of equal rights of all States. Indeed, several authors already expressed the opinion that Internet safety and security are a shared responsibility.[32] Based on this understanding areas of international law that can be used for reference with regard to guaranteeing cybersecurity include:[33]

(i) *Law of the sea*: The most important rules for the maritime area (i.e. the oceans) are contained in the Convention on the High Seas of 1958 and the Convention on the Law of the See of 1982.[34] The main objective of these Conventions being a good example of a wide multifaceted cooperation, consists in the establishment of the freedom of the seas' principle meaning that seas might not be subject to individual sovereignty claims.[35]

(ii) *Air and space law*: The legal regime of outer space was basically established by the Treaty of Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies of 1976.[36] The main purpose of this treaty consists (i) in the submission of all activities in outer space to

[30] Hugo Grotius, The freedom of the seas or the right which belongs to the Dutch to take part in the East Indian Trade: a dissertation, ed. by James Brown Scott, New York, 1916, 5.
[31] This term was introduced by John F. Kish, The Law of International Spaces, Leiden 1973.
[32] See Cerf/Ryan/Senges/Whitt, 2016, 15/16.
[33] Kulesza/Weber, 2017, 88.
[34] 450 UNTS 11; 1833 UNTS 397.
[35] See also Weber, 2014, 20.
[36] 610 UNTS 205.

international law, as well as (ii) in the principles of non-discrimination and of non-appropriation by any claim of sovereignty.[37] Air law is also subject to many multinational treaties under the auspices of the International Civil Aviation Organization (ICAO).[38]

(iii) *Diplomatic and consular law*: The Vienna Convention on Diplomatic Relations of 1961 contains basic, partly even comprehensive rules about the principles to be observed and complied with in the diplomatic and consular world.[39]

(iv) *International human rights law*: The need to harmonize global rules in the context of human and fundamental rights has become obvious in the aftermath of the Second World War; the main legal sources are the UN Universal Declaration of Human Rights (1948)[40] as well as the two UN Covenants on Civil and Political Rights as well as on Economic, Social and Cultural Rights (1966).

(v) *International telecommunication law*: The International Telecommunications Union (ITU) is the second-oldest international body having been founded in 1865; the need to harmonize the communications rules has been obvious since then and has even become more important with the advent of the Internet.[41]

(vi) *International environmental law*: The fact that environmental resources must be used respectfully, sustainably and in a shared way is well known for decades; several international treaties are existing and have culminated in the declarations related to the climate change challenges (for example the Kyoto Agreement and the Paris Agreement).[42]

(vii*) International trade law*: The World Trade Organization, following the General Agreement on Tariffs and Trade and being in place since January 1995, is the best example for the acknowledgment that harmonized global trade rules are of importance.[43]

---

[37] See also Weber, 2014, 21; Kulesza 2012, 145/46.
[38] The original multilateral treaty is the Chicago Convention on International Civil Aviation (1944), followed by many Montreal Protocols.
[39] 500 UNTS 95.
[40] UN Resolution 217 A (III) of 10 December 1948.
[41] See also Schmitt, 2017, 179 et seq.
[42] The need for such behavior of States can be easily derived from the different reports of the Intergovernmental Panel on Climate Change (IPCC).
[43] The re-nationalization of trade policies during the Covid-19-crisis and the subsequent sharp drop of the global trade volume shows the importance of the WTO-rules.

(viii*) Money laundering and terrorism financing laws and policies*: Having some similarities to the measures combating the negative effects of cyberattacks, the fight against money laundering and terrorism financing is a global task. The respective activities are exercised by the Financial Action Task Force (FATF), a UN body domiciled with the OECD in Paris.[44]

While each of these legal regimes offers interesting insights that can be useful to Internet stability, a concise and general assessment derived from all those areas of international law and relations is still outstanding. Nevertheless, the basic principles being applicable in all mentioned areas of laws, in particular the notion of due diligence, can be made fruitful in respect of cybersecurity; governments should closely cooperate in a continuing effort to arrive at an operable consensus that takes into consideration global interoperability, network stability, reliable access and cybersecurity due diligence.[45]

For the sake of completeness it may be added that according to the Tallinn Manual 2.0 overarching international law principles relevant to all those specified regimes are to be taken into account:[46] (i) sovereignty, (ii) jurisdiction, (iii) state responsibility, and (iv) due diligence.[47] While sovereignty and the matrix of jurisdictional principles remain an unresolved challenge for critical infrastructure protection, subject to enhanced debate and still far from consensus, the two other principles, namely state responsibility and due diligence, can be easily applied to the biggest international open networks and their key components.[48] As the Global Commission on the Stability of Cyberspace has identified, uniform standards of protection for the whole infrastructure and its services recognized as fundamental to the global networks' stable and reliable operation are

[44] According to its own mission, the FATF as inter-governmental body sets international standards that aim to prevent money laundering and terrorism financing activities and the harm they cause to society; as a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas (https://www.fatf-gafi.org/about/whoweare/#d.en.11232).

[45] Heintschel von Heinegg, 2013, 134 et seq.

[46] Tallinn Manual, 2.0 on the International Law Applicable to Cyber Operations, 2017.

[47] See also Schmitt, 2017.

[48] Weber, 2020, 299.

necessary and can be expressed through (i) international cooperation, (ii) exchange of good practices, and (iii) benchmarking.[49]

### 3.3 Concept of State Responsibility

The legal principle of State responsibility can be perceived as a general normative framework, applicable in addition to all other specified international law norms imposing obligations upon States.[50] Once an international obligation of a State is breached – be it an obligation of conduct or one of result – the consequences provided for in the law of State responsibility entail.

The development of legal rules related to the State responsibility is not an easy task; the efforts of the International Law Commission (ILC) lasted decades and the final guidelines of 2001 are still in draft form and not fully adopted by the UN bodies.[51] The ILC based its work on two fundamental presumptions:[52] (i) A breach of an international obligation of a primary norm leads to a responsibility if a "sanction" is stated therein; otherwise, the responsibility is vested in the general international principle of responsibility as secondary norm. (ii) An international wrongful act causes a State responsibility.

The responsibility principle is linked to the due diligence requirement implying a State's duty to act with proper care in preventing a violation of international law. Indications of what is meant with "due care" in particular circumstances are to be derived from the legal practice within individual areas of international relations between States.[53] In-

[49] Global Commission on the Stability of Cyberspace, 2019, 95.
[50] Kulesza, 2016, 115 et seq.
[51] Draft Articles on Responsibility of States for Internationally Wrongful Acts, ILC Report, 2001, UN Doc. A/56/10 att. 10.
[52] Kulesza, 2016, 149 et seq. with further references.
[53] Kulesza/Weber, 2020, …

deed, the due diligence principle can be seen as shared element of treaty-based regimes[54] and has a very broad scope of application also extending to private actors (OECD Due Diligence Guidance).[55]

The principle of due diligence in preventing transboundary harm has become mainly important in environmental matters.[56] Nevertheless, by analogy, a due diligence standard for cybersecurity with shared responsibility[57] could equally build an entry point for the State's responsibility in respect of an omission resulting in transboundary harm, e.g. a disruption of communications channels within a State territory.[58] The existing community standards with regard to good business practice within each of the specific Internet sectors (e.g. root zone operation, IXP operation, DNS and TLD management)[59] could be referred to in connection with State responsibility. Due diligence appears in almost all legal regimes, and it is even relevant for the law on neutrality in armed conflicts, which is, in principle, applicable to cyberspace.[60] In other words, governments should closely cooperate in a continuing effort to arrive at an operable consensus that takes into consideration global interoperability, network stability, reliable access and cybersecurity due diligence.[61]

### 3.4 Further Potential Concepts

The three discussed concepts, namely the global public goods, the shared spaces and the State responsibility, appear to constitute the most important international legal principles. Nevertheless, further Internet-specific concepts have been developed that could also be made fruitful; in particular, the GCSC addressed the following principles:

[54] Kulesza, 2016, 253 et seq.
[55] OECD Due Diligence Guidance for Responsible Business Conduct, Paris 2018.
[56] Kulesza, 2016, 205 et seq.; Butler, 2020, 209/10.
[57] See also Cerf/Ryan/Senges/Whitt, 2016, 8/9.
[58] For further details see Kulesza, 2016, 276 et seq. and 288 et seq. with further references.
[59] See below chapters 4.1 and 4.2 as well as Cerf/Ryan/Senges/Whitt, 2016, 14.
[60] Schmitt, 2017.
[61] Kulesza/Weber, 2020, …

(i) The requirement of "restraint" imposes on State and non-state actors the behavioural rule to act in accordance with general principles of international peace and security in order to avoid that harmful acts are undermining the resilience and stability of cyberspace.[62]

(ii) The requirement to "act principle" contains a duty to take affirmative action for preserving the stability of cyberspace; State and non-state actors should take care that inadvertibly escalating tensions or increasing instability are avoided.[63]

(iii) Furthermore, human rights are important legal yardsticks that can safeguard cyberspace stability; the disruptive effect on human activity resulting from the threats for the availability or integrity of information and communications technologies is obvious and impacts human rights of individuals in a severe way.[64]

The Global Commission on the Stability of Cyberspace as the expert group having developed the most recent principles in the context of Internet integrity and cyber stability has also drafted specific norms; for the sake of completeness, it is worth to quote the respective norms:[65]

"1. State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

2. State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

3. State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.

4. State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.

5. States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in

[62] Global Commission on the Stability of Cyberspace, 2019, 18.
[63] Global Commission on the Stability of Cyberspace, 2019, 19.
[64] Global Commission on the Stability of Cyberspace, 2019, 19.
[65] Global Commission on the Stability of Cyberspace, 2019, 21/22.

information systems and technologies. The default presumption should be in favour of disclosure.

6. Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures, to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.

7. States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.

8. Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur."

These fundamental norms are to be kept in mind when discussing soft law principles hereinafter.

## 4. Relevance of Soft Law Principles for Cybersecurity

Experience has shown that the traditional "hard law" is not able to cope with all normative challenges appearing around the globe in all segments of society. Moreover, different forms of "soft law" increasingly play an important role in the normative environment.[66] Indeed, legal doctrine is now stating that the dichotomy between hard law and soft law must be overcome.[67] This assessment goes hand in hand with the acknowledgment that private actors can also become "keepers of international law".[68] Alternative approaches of (also private) rule-making equally encompass fundamental legal principals to be observed by the concerned actors; hereinafter, the two main forms, namely self-regulation and co-regulation, will be discussed.

### 4.1 Self-regulatory Approaches

Self-regulation refers to the rules that are autonomously developed and implemented by the "governed" persons, independently from any structured form of rule-making.

[66] Weber, 2002, 85 et seq.
[67] Weber, 2012, 8 et seq.
[68] Butler, 2020, 189.

The legitimacy of self-regulation is based on the merits of the incentive- and need-driven rule-setting processes. Self-regulation is responsive to changes in the environment and can establish rules without regard to the territoriality principle.[69]

A universally accepted theory as to the "legal quality" of self-regulation has not (yet) been formulated. Since self-regulation is not enforceable through public action, such rules do not have the quality of law in the traditional understanding.[70] However, compliance with self-regulatory guidelines is usually more than only an ethical undertaking because these provisions correspond to standards that reflect the common sense behaviour expected to be observed by the concerned actors.[71]

The strengths of self-regulation encompass the following elements:[72] (i) The rules created by the concerned actors of a specific community are efficient since they respond to real needs and mirror the technology. (ii) Meaningful self-regulation provides the opportunity to adapt the regulatory framework to the changing technology. (iii) Self-regulation can usually be implemented at reduced costs. (iv) Due to the private initiatives the chances are high that the rules contain incentives for compliance. (v) Effective self-regulation induces the concerned actors to be open to a permanent consultation process related to the development and implementation of the rules.

Self-regulation has played in the past and is still playing an important role of the context of the critical Internet infrastructure: At least from a technical angle, the current Internet governance landscape was originally designed on the basis of bottom-up governance models, rooted strongly in the technical community, for example the Internet Society (ISOC) or the Internet Engineering Task Force (IETF) with its "Requests for Comments" (RfC);[73] these bodies are implementing community-developed common standards to be voluntarily followed by their members, namely Internet service providers and software developers.[74]

---

69 Weber, 2014, 23 with further references; see also Butler, 2020, 199 et seq.
70 Weber, 2002, 81-83; Guzman/Meyer, 2010, 179-183.
71 Weber, 2014, 25.
72 Weber, 2002, 83/84 with further references.
73 Rescorla, 2003, 57; see also Butler, 2020, 209/10.
74 Kulesza/Weber, 2017, 82.

While "security by design" remains a common paradigm within both, ISOC and IETF, there is no connection to be made between this extra-legal, community-based rule-making approach and the hard norm-setting models of States.[75] Notwithstanding the fact that the Internet Corporation for Assigned Names and Numbers (ICANN), the ISOC, and the Internet Governance Forum (IGF) have been attending to the issue, this communications' gap holds crucial relevance for the development of any effective international cybersecurity policies and must be addressed by whatever model of global cyber governance.[76] There can be no effective cybersecurity policy developed solely at governmental level, without strong presence of the technical community and vigilant input from civil society. Experience has shown that a compromise between the protection of fundamental infrastructure (Internet) functions and community-based technical standards must be achieved.[77]

Looking from the angle of self-regulatory initiatives, the already discussed policy paper of the Global Commission on the Stability of Cyberspace (GCSC) also advocates for the inclusion of private "rule-makers" (multistakeholderism).[78] The developed principles to be observed by State and non-state actors have the objective of securing an environment in which the actors do not to engage in any activities that impair the stability of the Internet and/or endanger the protection of the Internet's public core (enshrining its integrity).[79] In addition, actors are invited to enact appropriate measures to ensure basic cyber hygiene.[80] Taking into account the various approaches developed in the global arena of international organizations, private actors and academic scholars, the norms and principles of the GCSC-Report merit to be further concretized.

### 4.2 Co-regulatory Approaches

Self-regulatory initiatives can also be supported by international organizations or national governments. This approach is often called "co-regulation" being a term that has

[75] Kulesza/Weber, 2017, 82 and 89.
[76] For the parameters of a cyberspace framework see Weber, 2014, 102 et seq.
[77] For a thorough study of the impact of technical standards on cybersecurity see Broeders, 2017, 366 et seq.
[78] Global Commission on the Stability of Cyberspace, 2019, 17.
[79] Global Commission on the Stability of Cyberspace, 2019, 18/19.
[80] See also Recital 8 of EU Cybersecurity Act 2019 (supra note 13).

been coined by Hoffmann-Riem in 2000.[81] The involvement of other stakeholders than the directly concerned actors is usually strengthening the rule-making processes. Apart from the term "co-regulation" such kind of cooperative rule-making is also called regulated self-regulation, directed self-regulation or audited self-regulation.[82]

Co-regulation as model is often designed by a general framework established in the form of governmental regulations which than is substantiated by the private sector; in other words, the State legislator sets the legal yardsticks and leaves the qualification of the given principles by way of specific rules to private bodies. Thereby, regulation can remain flexible and innovation-friendly. In addition, the government remains involved in the private rule-making activities at least in a monitoring function supervising the progress and the effectiveness of the initiatives in meeting the perceived objectives.[83]

Since it is often difficult to fully tackle the cybersecurity challenges by way of self-regulatory initiatives due to the lack of enforcement means, co-regulation can have a positive impact on the behaviour of the concerned market participants. Joint efforts of various stakeholders also allow the governments to assess the representativeness of self-regulatory standards and judge the appropriateness of best practices; interventions appear justified if a higher level of protection measures is desirable.[84] Reality shows that such kind of co-regulatory approaches are already existing in the field of critical infrastructure:

(i) An important intergovernmental attempt to directly address the issue of Internet's infrastructure at the policy level is the CoE Report of 2009 with the title "Internet Governance and Critical Internet Resources".[85] It identified "Critical Internet Resources" (CIR) that require particular care from the international community to ensure the free and reliable flow of information online. According to the CoE, the CIR include root serv-

[81] Hoffmann-Riem, 2000.
[82] Weber, 2014, 23/24.
[83] Senn, 2011, 43, 139-148, 230; Marsden/Meyer/Brown, 2020, 9.
[84] Marsden/Meyer/Brown, 2020, 9.
[85] Council of Europe, Internet Governance and Critical Internet Resources Report, Strasbourg 2009.

ers, Domain Name System (DNS), Internet Protocol and the Internet "backbone structures", as well as Internet Exchange Points (IXPs).[86] The CoE emphasized the need to secure universal broadband access and network neutrality and linked the need to protect CIR with the existing critical resources perception, indicating the Internet itself as a "critical resource" and arguing that for it to remain "sustainable, robust, secure and stable" it must be protected "in the same way than other critical common resources are protected".[87]

(ii) Critical infrastructure protection as provided by existing national regimes and international cooperation programs, such as the European Programme for Critical Infrastructure Protection (EPCIP), usually encompass networks fundamental to the daily operation of any modern society: water and energy supply, mass transportation, health and emergency services and alike.[88] The last and newest category included in Annex II to the NIS Directive covers "digital infrastructures" and includes (i) IXPs, (ii) DNS service providers and (iii) Top-Level-Domain (TLD) name registries.[89] These categories mirror the current EU approach to cybersecurity, viewing crucial Internet infrastructures as part of the European critical infrastructures ecosystem. Effectively, they all require the same level of protection from their operators, including e.g. security due diligence measures and risk assessments.[90]

## 5. Implementation of International Legal Principles and Soft Law

The identification of international legal principles and relevant norms of soft law does not suffice. Moreover, it is important to fully implement the respective (binding or non-binding) guidelines. As experience has shown during the last years, enforcement of legal provisions is always difficult in the international context, even more so in case of soft law.

[86] Council of Europe (supra note 82), 13-15.
[87] Council of Europe (supra note 82), 23; see also Kulesza/Weber, 2017, 82/83.
[88] Kulesza/Weber, 2017, 86.
[89] NIS-Directive (supra note 12), Annex II.
[90] See also Kulesza/Weber, 2017, 83/84.

A first step could consist in the improvement of the involved actors' commitments, for example by engaging in capacity building efforts and confidence building measures.[91] Implementing norms in a more granular helps building consensus on the meaning of norms and can lead to a better understanding of their relevance. Partly, the respective efforts have been introduced but much more needs to be done.

Nevertheless, capacity building and confidence building alone do not lead to an appropriate implementation of normative guidelines. The sharing of best practices and of resilience/security standards must be encouraged on the basis of the relevant normative guidelines. Concrete steps are necessary to give them force.[92] The respective international legal principles are to be operationalized by incorporating them into international and national policies as well as into legislation.

## 6. Outlook

Cybersecurity governance is an objective that should eliminate or at least minimize risks caused by an inappropriate use of international electronic infrastructures. Risk is the function of the likelihood of an adverse event, interacting with the magnitude of harm upon the occurrence of an adverse event.[93] Precautionary measure can be taken by the private actors, for example by way of standardization, as the network security provisions of ISO/IEC 27001 of 2013 as well as the updated extension ISO/IEC 27701 of 2019 show.[94] In order to achieve a reasonable cybersecurity governance it is necessary to implement a new regulatory framework based on international legal principles through (i) private institutions with regulatory functions, (ii) hybrid intergovernmental-private arrangements, (iii) distributed regimes of regulators in cooperative schemes and (iv) collective actions by transnational networks.[95]

Previous experience in the field of cybersecurity has shown that the traditional international law approach operating on the State level through multilateral treaties, thereby

---

91 Global Commission on the Stability of Cyberspace, 2019, 23.
92 Global Commission on the Stability of Cyberspace, 2019, 23/24.
93 Weber, 2020, 307.
94 International Standardisation Organisation, ISO/IEC 27001:2013, https://iso.org/standard/54534.html.
95 Weber, 2020, 307.

failing to directly address duties of private actors, is hardly able to cope with the challenges of combatting interference with Internet integrity (in different forms). Therefore, the inclusion of various stakeholders into a new regulatory framework appears to be unavoidable. This attempt has been undertaken by Microsoft in 2018 when suggesting of adopting an international treaty to guarantee the peaceful use of cyber space.[96] The proposal to develop a "Digital Geneva Convention" referred to the "Treaty on the Non-Proliferation of Nuclear Weapons" and the "Treaty on Chemical Weapons" as examples of international regimes limiting vital threats to human existence. However, this proposal met the scepticism of many States and it also appears to be unclear to what extent other Internet stakeholders could be included in such an arrangement.[97]

The so far (incoherent) patchwork of cybersecurity regulations does not really correspond to the political needs. The only exception concerns the EU with the recently adopted (directly or indirectly applicable) legal regime; however, the practical implementation in the EU still needs to become successful. On a global level, further efforts to achieve a better co-ordinated regulatory framework are required; the widely accepted international legal principles such as the concept of public goods, of shared spaces and of State responsibility might be a good way to go forward. Thereby, it is also up to the businesses and the academics to contribute to these efforts with more emphasis.

## 7. Bibliography

Broeders, 2017. Dennis Broeders, Aligning the international protection of "the public core of the internet" with state sovereignty and international security, Journal of Cyber Policy 2 (2017), 366-376.

Butler, 2020. Jay Butler, The Corporate Keepers of International Law, The American Journal of International Law 114 (2020), 189-220.

[96] Microsoft, Cybersecurity Privacy Framework, Geneva 2018, https://www.microsoft.com/en-us/Cybersecurity/content.hub/Cybersecurity-Policy-Framework.

[97] Therefore, Brad Smith, CEO of Microsoft, proposed the name "A Digital Geneva Convention" to protect cyberspace.

Cerf/Ryan/Senges/Whitt, 2016. Vinton G. Cerf, Patrick S. Ryan, Max Senges and Richard S. Whitt, IoT safety and security as shared responsibility, Business Informatics 35 (2016), 7-19.

Clough, 2014. Jonathan Clough, A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation, Monash University Law Review 40 (2014), 698-736.

Global Commission on the Stability of Cyberspace, 2019. Global Commission on the Stability of Cyberspace, Advancing Cyberstability, Final Report, Berlin, November 2019.

Guzman/Meyer, 2010. Andrew Guzmann and Timothy L. Meyer, International Soft Law, Journal of Legal Analysis 2 (2010), 171-225.

Heintschel von Heinegg, 2013. Wolff Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, International Legal Studies 89 (2013), 123-156.

Henriksen, 2019. Anders Henriksen, The end of the road for the UN GGE process: The future regulation of cyberspace, Journal of Cybersecurity 5/1 (2019), 1-9.

Hoffmann-Riem, 2000. Wolfgang Hoffmann-Riem, Regulierung der dualen Rundfunkordnung, Baden-Baden 2000.

Kaul/Grunberg/Stern, 1999. Inge Kaul, Isabelle Grunberg and Marc A. Stern, Defining Global Public Goods, in: Kaul/Grunberg/Stern (eds.), Global Public Goods: International Cooperation on the 21st Century, New York/Oxford 1999, 51-64.

Koskenniemi, 2009. Martti Koskenniemi, From Apology to Utopia: the Structure of International Legal Argument, 3rd ed. Cambridge 2009, 562-573.

Krisch, 2014. Nico Krisch, The Decay of Consent: International Law in an Age of Global Public Goods, The American Journal of International Law 108 (2014), 1-40.

Kulesza, 2012. Joanna Kulesza, International Internet Law, London/New York 2012.

Kulesza, 2016. Joanna Kulesza, Due Diligence in International Law, Leiden/Boston 2016.

Kulesza/Weber, 2017. Joanna Kulesza and Rolf H. Weber, Protecting the Public Core of the Internet, 2017, https://cyberstability.org/research/briefing-and-memos-of-the-research-advisory-group.

Kulesza/Weber, 2020. Joanna Kulesza and Rolf H. Weber, Saving the Internet with International Law (forthcoming).

Marsden/Meyer/Brown, 2020. Chris Marsden, Trisha Meyer and Ian Brown, Platform values and democratic elections: How can the law regulate digital disinformation, Computer Law & Security Review 36-105373 (2020), 1-18.

Rescorla, 2013. Eric Rescorla, Guidelines for Writing RFC Text on Security Considerations, 2003, https://tools.ietf.org/html/rfc3552.

Schmitt, 2017. Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyberoperations, 2nd ed. Cambridge 2017.

Senn, 2011. Myriam Senn, Non-State Regulatory Regimes. Understanding Institutional Transformation, Berlin 2011.

Shaffer, 2012. Gregory Shaffer, International Law and Global Public Goods in a Legal Pluralist World, European Journal of International Law 23 (2012), 669-693.

Weber, 2002. Rolf H. Weber, Regulatory Models for the Online World, Zurich 2002.

Weber, 2009. Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges, Zurich 2009.

Weber, 2012. Rolf H. Weber, Overcoming the Hard Law/Soft Law Dichotomy in Times of (Financial) Crisis, Journal of Governance and Regulation 1 (2012), 8-14.

Weber, 2014. Rolf H. Weber, Realizing a New Global Cyberspace Framework, Zurich 2014.

Weber, 2020. Rolf H. Weber, Cybersecurity in International Law, in: Asian Academy of International Law (ed.), 2019 Colloquium on International Law, Hong Kong 2020, 279-308.

Weber/Menoud, 2008. Rolf H. Weber and Valérie Menoud, The Information Society and the Digital Divide: Legal Strategies to Finance Global Access, Zurich 2008.

Weber/Studer, 2016. Rolf H. Weber and Evelyne Studer, Cybersecurity in the Internet of Things: Legal Aspects, Computer Law and Security Review 32 (2016), 715-728.