www.jusletter-it.eu

Rolf H. Weber

Cybersecurity Governance – international law as policy driver?

Governance issues in the cybersecurity context have so far not become a key discussion topic, probably due to the fact that the existing legal instruments of global organizations do not play an important role in reality. This contribution pleads for a change of the perspective: As new regulatory models, alternative normative standards such as the concept of public goods, the concept of shared spaces and the concept of State responsibility should be made fruitful. These concepts appear to be suitable for giving guidelines at hand that support the improvement of the cybersecurity environment.
The Internet as the most important global infrastructure is an ecosystem in which international law, with all its perplexities, should exercise a relevant function, particularly in view of the threats to which cybersecurity is exposed. Yet the current approach of politicians, scholars and practitioners shows a pertaining reluctance to embrace the challenges posed by cyberattacks to the most important international electronic network. An effective and coherent application of international legal concepts could support the efforts of realizing a higher level of Internet integrity.

Category of articles: Articles
Region: EU
Field of law: Cybercrime

Citation: Rolf H. Weber, Cybersecurity Governance – international law as policy driver?, in: Jusletter IT 27 May 2021

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Contents

1. Introduction

[2] 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 to describe such kind of integrity of the Internet. At the beginning, cybersecurity was the most used word, followed by other terms such as the stability and the resilience of cyberspace; hereinafter, cybersecurity will remain the keyword of the international law considerations.

[3] Cybersecurity refers to processes and measures protecting networks and data form cybercrimes. So far, no standard or universally accepted definition of the term cybersecurity exists. 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]

[4] 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 data and information for authorized

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.

users.[3] The International Organization for Standardisation (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.

[5] Usually, the cyberthreat landscape is described by using a linear approach that distinguishes either between (i) threat agents, (ii) threat tools, and (iii) threat types[4] or between (i) computer network exploitations, (ii) computer network attacks, and (iii) information operations.[5] While such categorizations are useful for certain legal qualifications, they do not paint a comprehensive picture of the very complex nature and characteristics of cyberthreats.[6] The array of external and internal agents endangering cybersecurity is mostly very wide, going from nation States to hackers and insiders. Threat tools encompass malware and its variances as well as botnets. Threat types include information modification or misuse, information destruction, unauthorized access, data breach, data theft and distributed denial-of-service.

[6] 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.[7] 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.

[7] This contribution does not analyze the details of the existing legal instruments (or their preparatory documents) combatting cybercrime, but shortly mentions their existence and some key issues thereof (chapter 2). Based on the (substantively rather pessimistic) assessment of their relevance, a bridge will be built from legal instruments to concepts (chapter 3) and the core question will be discussed to what extent the established and widely accepted international normative concepts (in particular the concept of global public goods, of shared spaces and of State responsibility) can contribute to an acceptable global cybersecurity governance (chapter 4); specific challenges are posed by the implementation of the mentioned concepts (chapter 5). An outlook closes the contribution (chapter 6).

3 Rolf H. Weber, Cybersecurity in International Law, in: Asian Academy of International Law (ed.), 2019 Colloquium on International Law, Hong Kong 2020, 279, 281.

4 See the detailed explanations in Rolf H. Weber/Evelyne Studer, Cybersecurity in the Internet of Things: Legal aspects, Computer Law & Security Review 32 (2016), 715, 717/18 with further references.

5 See Martin Dahinden, Swiss Neutrality in the Age of Cyber Warfare, ICT4Peace Foundation, Policy Brief, Geneva 2021, 7/8, with further references.

6 See also Dominik Herrmann/Henning Pridöhl, Basic Concepts and Models of Cybersecurity, in: Christen/Gordijn/Loi (eds.), The Ethics of Cybersecurity, Cham 2017, 11 et seq.

7 Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges, Zurich 2009, 2.

2. Cybersecurity as Issue of Existing Cybercrime Instruments

2.1. Global Level

[8] Cybersecurity now routinely tops political agendas.[8] For decades, international and regional organizations have tried to develop legal instruments that could harmonize the regulatory standards in the field of cybersecurity prevention.[9] Some efforts have been (partly) successful, mainly if implemented as so-called security exceptions in multilateral agreements of sector-specific international organizations (ITU, WTO).[10]

[9] 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.[11] In particular, the third UNGGE (2012/13) advocated for the application of the UN Charter to cyberspace, which was to remain open, secure, peaceful and accessible. The group also confirmed that States were sovereign to regulate cyberspace and had the territorial jurisdiction over the cyberspace infrastructure. Furthermore, it argued that State efforts to address the security of ICT must go hand-in-hand with respect for human rights and fundamental freedoms and that States were obliged not to use proxies to commit internationally wrongful acts.[12]

[10] The fourth UNGGE (2015) produced a comprehensive report on norms, rules and principles regarding the responsible behavior of States in cyberspace as well as with regard to international cooperation, confidence building measures, and capacity building. Its findings confirmed four principles concerning the application of international law to cyberspace.[13] In particular, principle 1 states that in their use of ICT, States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful means, and non-intervention in the international affairs of other States. Specifically, the fourth UNGGE made the following forward-looking statement:[14]

> 1. In their 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. Existing 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.

8 The World Economic Forum (WEF) publishes a yearly Global Risk Report; cyberattacks and critical information infrastructure breakdowns regularly rank highly.

9 For an overview see Weber (supra n. 3), 284 et seq.

10 Specific security provisions are contained in the ITU- and WTO-Agreements (for further details Weber [supra n. 3], 288–290).

11 For further details see Joanna Kulesza/Rolf H. Weber, Protecting the Internet with International Law, Computer Law & Security Review 40 (2021) 105531, 5; Anders Henriksen, The end of the road for the UN GGE process: The future regulation of cyberspace, Journal of Cybersecurity 5/1 (2019), 1, 4 et seq.

12 UN Doc. A/68/98.

13 UN Doc. A/70/174.

14 UN Doc. A/70/174.

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.

[11] The fifth UNGGE (2016/17) did not really overcome the challenge of transposing the generally accepted principles into detailed obligations being operable for the States. The failure was also caused by political tensions of various kinds.[15]

[12] In 2019, two newly established groups were mandated to come up with further recommendations in the course of 2021.[16] However, a basic problem consists in the fact that the two mandates do not appear to be coherent.[17] Notwithstanding the recent publication of the Final Substantive Report by the UN Cyber OEWG (Open-ended working group),[18] the key assessment of the fourth UNGGE pointing to the importance of the principles of international law as normative pillars of cybersecurity remains valid and justifies a deeper analysis of applicable legal concepts.

2.2. Regional Level

[13] Regional approaches have been more successful: particularly in Europe, multilateral legal instruments do exist and are also applied in practice. The main organizations are the Council of Europe and the European Union.

[14] (i) The Council of Europe (CoE) adopted the (Budapest) Convention on Cybercrime in 2001 encompassing now more than 60 ratifying States (also outside of Europe, including Argentina, Australia, Canada, Chile, Israel, Japan and the United States).[19] As set forth in the Preamble, the main objective of the Budapest Convention is to pursue a common criminal policy against cybercrime by adopting appropriate legislation and fostering international cooperation. The aim of the Convention is to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as misuse of such systems.[20] The most effective security measures should be implemented to prevent unauthorized access to protected infrastructures.

[15] The Budapest Convention was the first (ambitious) attempt to harmonize the legal framework for combatting cybercrime. Despite its role in providing an internationally recognized

15 For further details see Weber (supra n. 3), 287/88; Eneken Tikk, Introduction, in: United Nations Office for Disarmement Affairs (ed.), Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Informations and Communications Technology, A Commentary, New York 2017, 1 et seq.; Paul Meyer, Norms of Responsible State Behaviour in Cyberspace, in: Christen/Gordijn/Loi (eds.), The Ethics of Cybersecurity, Cham 2017, 347, 352/53, 357.

16 Resolution, A/C/1/73/L.37 and A/C/1/73/L.27 Rev. 1.

17 See also Rolf H. Weber, Internet Governance at the Point of No Return, Zurich 2021, 85.

18 For further details see below chapter 6.2.

19 Council of Europe, Convention on Cybercrime, ETS no. 185, Budapest, November 2001.

20 For further details see Explanatory Report, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentID=09000016800cce5b.

framework for global harmonization, the Convention has been panned by its critics as largely outdated and in great need of reform.[21] Various reasons have been cited for its supposed obsolescence, including the fact that the Convention is based on the types of offenses that prevailed at the time of its drafting (i.e. the late 1990s) and therefore (logically) does not take into account new cyberattack rules (such as botnets and ransomware)[22]. As a result, there have been calls for a general revision of the Budapest Convention and even calls for the adoption of a new (and truly) universal treaty on cybercrime.[23] Now, a revision of the Convention is on the way, but its final adoption cannot be forecasted.

[16] (ii) Apart from the General Data Protection Regulation (GDPR) 2016/679 of 27 April 2016, in force since 25 May 2018, that is containing several regulations on data security, the European Union (EU) released the Network and Information Society (NIS) Directive[24] 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 (implementing a certification regime).[25] As a noteworthy remark it may be emphasized 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.[26] The success of the NIS Directive and the Cybersecurity Act cannot yet be assessed since the national implementation only dates back a short time. Nevertheless, it should be positively stated that the role of the European Union Agency for Cybersecurity (ENISA) has gained importance and that the established national Computer Security Incident Response Teams (CSIRT) have attempted to improve cross-border cooperation.[27]

[17] The EU Commission is continuing to address cybersecurity issues with a high priority as the new Cybersecurity Strategy for the Digital Decade of 16 December 2020 clearly evidences to the widespread addressees.[28] The Cybersecurity Strategy points to the importance of resilience in respect of infrastructures and critical services and proposes to build a European Cyber Shield (including the implementation of a cyber-skilled EU workforce). As special aspects the call for an advancement of responsible State behavior in cyberspace and the call for cooperation in a multistakeholder community are particularly noteworthy.

2.3. Interim Assessment

[18] 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

21 Jonathan Clough, A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation, Monash University Law Review 40 (2014), 698, 701.

22 Weber (supra n. 3), 293.

23 Weber/Studer (supra n. 4), 723.

24 OJ 2016 L 119/1 of 4 May 2016.

25 OJ 2019 L 151/15 of 7 June 2019.

26 To the discussions in the context of Annex III see Joanna Kulesza/Rolf H. Weber, Protecting the Public Core of the Internet, 2017, https://cyberstability.org/research/briefing-and-memos-of-the-research-advisory-group, 87.

27 Weber (supra n. 3), 297.

28 See https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade; for a detailed discussion of this new strategy see Annegret Bendiek/Matthias C. Kettemann, EU-Strategie zur Cybersicherheit: Desiderat Cyberdiplomatie, SWP-Aktuell, Berlin, February 2021, 1.

not have remarkable effects.[29] The EU legal instruments are limited to their regional scope of application. Therefore, the search for other normative frameworks becomes imperative; as will be shown, the widely acknowledged international legal concepts appear to be a viable alternative solution.

3. Bridge over Troubled Waters: From Instruments to Concepts

3.1. Cyber Operations and Subsequent State Practice

[19] Among the State-led responses that target cybersecurity challenges, the North Atlantic Treaty Organizations (NATO), an intergovernmental organization of Western countries focused on conflicts and international peace, has been at the forefront in adapting numerous prominent documents. At its Security Summit in 2016, NATO recognized cyberspace as the fifth warfare domain and confirmed that a cyberattack against any of its allies would be considered an act of war.[30] A particularly important document is the Tallinn Manual of 2013, now available in the revised, amended and improved version Tallinn Manual/2.0 of 2017, being the first comprehensive study of international law applicable to cyberspace.[31]

[20] The Tallinn Manual defines critical infrastructure to include all systems and assets, physical and virtual, within a nation State's jurisdiction; it also describes the term cyberinfrastructure as governing communications, storage, and computing resources upon which computer systems operate.[32] The Tallinn Manual 2.0 offers a comprehensive regulatory scheme (154 rules), laying out the general legal principles governing cyber operations and their interaction with specialized international law regimes.[33]

[21] A recent study about the implementation of the rules laid down in the Tallinn Manual shows a differentiated picture: some principles have been taken over by a couple of countries into the national law, some others were rejected. The findings are described as evidencing a limited support in state practice for certain key Rules making it difficult to ascertain whether states accept the Tallinn Rules and wish them to become authoritative articulations of international law governing cyberoperations.[34] The case study reveals three interrelated strategies employed by States under the given conditions:[35]

> (1) *Optionality* – regarding the framework described in the Tallinn Manuals as optional, in the sense that the states have a choice about whether or not to invoke international law rights and obligations applicable to cyberspace;

29 For further details see Clough (supra n. 21), 701 et seq.; Weber (supra n. 3), 283/84.

30 NATO, Warsaw Security Summit Communiqué, 2016, 70/71.

31 Weber (supra n. 3), 299.

32 Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed. Cambridge 2017, 288 et seq.

33 Dan Efrony/Yuval Shani, A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice, The American Journal of International Law 112 (2018), 583, 584.

34 Efrony/Shany (supra n. 33), 585.

35 Efrony/Shany (supra n. 33), 586.

> (2) *Parallel Tracks* – state practice in the field of cyberoperations appears to develop along to parallel tracks, acknowledged and unacknowledged, resulting in the emergence of two sets of rules of the game – international law rules and softer informal rules, which also limit state power. [....]
>
> (3) *Gradations* in law enforcement – states seem to develop with regard to cyberoperations a nuanced understanding of law enforcement, distinguishing between violations likely to lead to some form of response and those unlikely to do so.

[22] In general, the impression prevails that law will gradually develop into the direction of encompassing data and other non-physical targets of consequential importance.[36] But the problem exists that a certain lack of transparency in this field exists due to underreporting of cyberoperations and limited attribution claims that makes it difficult to identify relevant State practice.[37] In addition, the experience has shown that the identification of customary international law containing indications of *opinio juris* appears to be difficult in this context.[38]

[23] As recently pointed out by well-known cybersecurity scholars, States are also adopting a cautious approach toward publicly attributing State responsibility; rather the approaches of silence and ambiguity are followed even if this may convey a message of impunity to other would-be cyberattackers.[39] Consequently, from the field of the Internet law in general the lesson can be drawn that policy reluctance or even disagreements in respect of the application of legal norms to new technologies is prevailing in many respects.

3.2. Building a Bridge

[24] The expression bridge over troubled water stems from the world-known song of Simon and Garfunkel. Notwithstanding the fact that the expression was coined fifty years ago, it keeps its importance also in the context of cybersecurity and international law. The discussions about an improved cybersecurity framework show the relevance of global concepts for Internet integrity and cyberspace stability.[40]

[25] In the cybersecurity context, international law develops and functions under conditions of significant normative uncertainty (and partly also in the absence of effective enforcement mechanisms).[41] Nevertheless, international law does not exist in a vacuum; attributions of tasks and responsibilities are possible. Even if the uneasy fit between traditional international law principles governing the exercise of State power inside and outside its territory and the regulation of a de-territorialized cyberspace is obvious, the conclusion that no international law regulation of cyberoperations would be possible or desirable goes into the wrong direction.[42] No reason appears

36 See also Michael N. Schmitt, The Law of Cyber Warfare: Quo Vadis?, Stanford Law & Policy Review 25 (2014), 269 et seq.

37 Efrony/Shany (supra n. 33), 595.

38 Michael Byers, Custom, Power and the Power of Rules – International Relations and Customary International Law, Cambridge 1999, 156 et seq.

39 Efrony/Shany (supra n. 33), 633.

40 Weber (supra n. 17), 83 et seq.

41 Efrony/Shany (supra n. 33), 647.

42 Efrony/Shany (supra n. 33), 654.

to exist that would prevent States from reacting against unprovoked cyberattacks or cyberoperations deliberately harming civilians based on the generally accepted global legal concepts which are to be outlined hereinafter.

[26] The bridge that must be built could start with the implementation of behavioral rules. For example, in the sustainability context the general principle that acting with due diligence or with due care can contribute to the avoidance of transboundary harm appears to be widely acknowledged.[43] Taken over to the cyber world this would mean that States should avoid to potentially disrupt communication channels and should closely cooperate in the efforts to pursue cyber-related global interoperability.

[27] 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;[44] as most important international normative standards, (i) the concept of global public goods, (ii) the concept of shared values and (iii) the concept of State responsibility will be further analyzed hereinafter.

4. Adherence to International Legal Concepts

[28] In principle, it is not contested that new norms and policies should be developed 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.[45] 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 encompassing (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.[46]

[29] This approach can be validly underlined with three international legal concepts having achieved a high level of acceptance in the concerned community; the respective concepts will be discussed in detail hereinafter.

4.1. Concept of Global Public Goods

[30] One of the starting points for a discussion on protecting cybersecurity could be the concept of global public goods.[47] Although not perfectly aligned to the needs of cybersecurity and the

43 See Joanna Kulesza, Due Diligence in International Law, Leiden/Boston 2016, 205 et seq.

44 See also Kulesza/Weber (supra n. 11), 8 et seq. and Weber (supra n. 17), 89 et seq.

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

46 Global Commission on the Stability of Cyberspace, Advancing Cyberstability, Final Report, Berlin, November 2019, 14.

47 For a general overview see Inge Kaul/Isabelle Grunberg/Marc A. Stern, Defining Global Public Goods, in: Kaul/Grunberg/Stern (eds.), Global Public Goods: International Cooperation in the 21st Century, New York/Oxford 1999, 10 et seq.; Rolf H. Weber/Valérie Menoud, The Information Society and the Digital Divide: Legal Strategies

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.[48]

[31] 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.[49] It refers to all globally available goods that are non-rivalrous (consumption does not influence the quantity available to others) and non-excludable (their use cannot be prevented); the examples of global public goods include knowledge as well as the common heritage of mankind.[50]

[32] 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 Nobel Memorial Prize (2018) laureate William N. Nordhaus pointed 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.[51] But international law is not without solutions to such problems; for example, the notion of the public core of the Internet being important in cybergovernance can be made fruitful;[52] indeed, core values also influence cybersecurity.[53]

[33] Equally, 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*.[54] Similarly, the concept of critical infrastructures and their protection can serve as another or complementary point of reference.[55] In addition, the well-known public interest concept is also able to peremptorily impose binding obligations on States that have a comparable foundation.[56] Based on these thoughts it can be argued that global public goods

to Finance Global Access, Zurich 2008, 24 et seq.; Gregory Shaffer, International Law and Global Public Goods in a Legal Pluralist World, European Journal of International Law 23 (2012), 675 et seq.; Nico Krisch, The Decay of Consent: International Law in an Age of Global Public Goods, The American Journal of International Law 108 (2014), 1 et seq.

48 Weber/Menoud (supra n. 47), 24.

49 Krisch (supra n. 47), 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.

50 Kulesza/Weber (supra n. 26), 81/82.

51 William N. Nordhaus, Paul Samuelson and Global Public Goods, 2005, http://www.econ.yale.edu/{~}nordhaus/homepage/homepage/PASandGPG.pdf.

52 See for instance 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 et seq.; see also Kulesza/Weber (supra n. 11), 6/7, and Krisch (supra n. 47), 4.

53 See Ibo van de Poel, Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security, in: Christen/Gordijn/Loi (eds.), The Ethics of Cybersecurity, Cham 2017, 45 et seq.

54 Weber/Menoud (supra n. 47), 24.

55 See Weber (supra n. 17), 92/93; Kulesza/Weber (supra n. 11), 4.

56 Weber (supra n. 3), 304.

theories involve a broad approach that considers political economy implications besides legal aspects[57] and, therefore, merits attention in future discussions.

4.2. Concept of Shared Spaces

[34] International cooperation on critical infrastructure protection is not the only analogy to be drawn from existing legal frameworks.[58] Equally, for example, the concept of shared 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.[59]

[35] Many global legal areas, constituting a law on international spaces[60], 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.[61] Based on this understanding areas of international law that can be used for reference with regard to guaranteeing cybersecurity include:[62]

[36] (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 Sea of 1982.[63] 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.[64]

[37] (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.[65] The main purpose of this treaty consists (i) in the submission of all activities in outer space to international law, as well as (ii) in the principles of non-discrimination and of non-appropriation by any claim of sovereignty.[66] Air law is also subject to many multinational treaties under the auspices of the International Civil Aviation Organization (ICAO).[67]

57 Weber/Menoud (supra n. 47), 25–27.

58 Rolf H. Weber, Realizing a New Global Cyberspace Framework, Zurich 2014, 19.

59 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.

60 This term was introduced by John F. Kish, The Law of International Spaces, Leiden 1973.

61 See Vinton G. Cerf/Patrick S. Ryan/Max Senges/Richard S. Whitt, IoT safety and security as shared responsibility, Business Informatics 35 (2016), 7, 15/16.

62 Kulesza/Weber (supra n. 26), 88; Weber (supra n. 17), 93/94.

63 450 UNTS 11; 1833 UNTS 397.

64 See also Weber (supra n. 58), 20.

65 610 UNTS 205.

66 See also Weber (supra n. 58), 21; Joanna Kulesza, International Internet Law, London/New York 2012, 145/46.

67 The original multilateral treaty is the Chicago Convention on International Civil Aviation (1944), followed by many Montreal Protocols.

[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.[68]

[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)[69] as well as the two UN Covenants (i) on Civil and Political Rights and (ii) on Economic, Social and Cultural Rights (1966).

[40] (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.[70]

[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).[71]

[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.[72]

[43] (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.[73]

[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 context 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.[74]

[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

68 500 UNTS 95.

69 UN Resolution 217 A (III) of 10 December 1948.

70 See also Schmitt (supra n. 32), 284 et seq.

71 The need for such behavior of States can be easily derived from the different reports of the Intergovernmental Panel on Climate Change (IPCC).

72 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.

73 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).

74 Wolff Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, International Legal Studies 89 (2013), 123, 134 et seq.

account:[75] (i) sovereignty, (ii) jurisdiction, (iii) state responsibility, and (iv) due diligence.[76] 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.[77] 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 necessary and can be expressed through (i) international cooperation, (ii) exchange of good practices, and (iii) benchmarking.[78]

4.3. Concept of State Responsibility

[46] The concept 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.[79] 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.

[47] The development of legal rules related to State responsibility is not an easy task; the efforts of the International Law Commission (ILC) lasted decades and the final guidelines of 2001 have been adopted by the UN bodies.[80] The ILC based its work on two fundamental presumptions:[81] (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.

[48] 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.[82] The due diligence principle can be seen as shared element of treaty-based regimes and rules of conduct[83] having a very broad scope of application that also extends to private actors as for example shown in the OECD Due Diligence Guidance.[84]

[49] The principle of due diligence in preventing transboundary harm has become mainly important in environmental matters.[85] Nevertheless, by analogy, a due diligence standard for cyberse-

75 Tallinn Manual, 2.0 on the International Law Applicable to Cyber Operations, 2017.

76 See also Schmitt (supra n. 32), 11 et seq.

77 Weber (supra n. 3), 299.

78 Global Commission on the Stability of Cyberspace (supra n. 46), 95.

79 Kulesza (supra n. 43), 115 et seq.

80 Draft Articles on Responsibility of States for Internationally Wrongful Acts, ILC Report, 2001, UN Doc. A/56/10 att. 10.

81 Kulesza (supra n. 43), 149 et seq. and Jovan Kurbalija, State Responsibility in Digital Space, Swiss Review of International and European Law 26 (2016), 307, 318 et seq., both with further references.

82 Kulesza/Weber (supra n. 11), 9; Weber (supra n. 17), 95/96.

83 Kulesza (supra n. 43), 253 et seq.

84 OECD Due Diligence Guidance for Responsible Business Conduct, Paris 2018.

85 Kulesza (supra n. 43), 205 et seq.; Jay Butler, The Corporate Keepers of International Law, The American Journal of International Law 114 (2020), 189, 209/10.

curity with shared responsibility[86] 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.[87] 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)[88] 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.[89] 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.[90]

4.4. Further Potential Concepts

[50] The three discussed concepts, namely the global public goods, the shared spaces and the State responsibility, appear to constitute the most important international normative standards. Nevertheless, further Internet-specific concepts have been developed that could also be made fruitful; in particular, the Global Commission on the Stability of Cyberspace (GCSC) addressed the following principles:

[51] (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.[91]

[52] (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 inadvertently escalating tensions or increasing instability are avoided.[92]

[53] (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.[93]

[54] The Global Commission on the Stability of Cyberspace as the expert group having developed the most recent standards in the context of Internet integrity has also drafted specific norms; for the sake of completeness, it is worth to quote the respective norms:[94]

86 See also Cerf/Ryan/Senges/Whitt (supra n. 61), 8/9.

87 For further details see Kulesza (supra n. 43), 276 et seq. and 288 et seq. with further references.

88 See also Cerf/Ryan/Senges/Whitt (supra n. 61), 14 ; Broeders (supra n. 52), 366 et seq.

89 Schmitt (supra n. 32), 30 et seq. and 553 et seq.

90 Weber (supra n. 17), 94/95.

91 Global Commission on the Stability of Cyberspace (supra n. 46), 18.

92 Global Commission on the Stability of Cyberspace (supra n. 46), 19.

93 Global Commission on the Stability of Cyberspace (supra n. 46), 19.

94 Global Commission on the Stability of Cyberspace (supra n. 46), 21/22.

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 information systems and technologies. The default presumption should be in favor 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.

[55] These fundamental standards are to be kept in mind when implementing legal rules in practice as explained hereinafter. Furthermore, ethical considerations merit to play a more important role.[95]

5. Implementation of International Legal Concepts

[56] The identification of international legal concepts 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 global normative concepts.

95 To the ethical dimensions which cannot be further discussed in this contribution see Michele Loi/Markus Christen, Ethical Frameworks for Cybersecurity, in: Christen/Gordijn/Loi (eds.), The Ethics of Cybersecurity, Cham 2017, 73 et seq.

[57] 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.[96] Implementing norms in a more granular way helps building consensus on the meaning of norms and can lead to a better understanding of their relevance. In addition, such kind of measures have a potential to prevent and mitigate conflicts.[97] Partly, the respective efforts have been introduced but much more needs to be done.[98]

[58] Nevertheless, capacity building and confidence building alone do not lead to a fully satisfactory 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.[99] The respective efforts should include increased cooperation in the areas of protection and defence.[100] The duty of cooperation is a well-known principle in international law[101] and merits to be equally applied in the cybersecurity context.

[59] The recently published Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG) of 10 March 2021, unanimously adopted on 12 March 2021 (OEWG-Report), also refers to confidence building measures (paras. 41–53) as well as to capacity building (paras. 54–67).[102] (i) Confidence building measures should comprise transparency, cooperative approaches and stability measures that contribute to preventing conflicts, avoiding misperceptions and misunderstandings, and reducing tensions (para. 41). In addition, such measures can strengthen the overall security, resilience and peaceful use of ICTs; furthermore, they are suitable for implementing norms of responsible State behaviour, in that they foster trust and ensure greater clarity, predictability and stability (para. 41). Nevertheless, it should not be overlooked that the OEWG is not really putting forward new measures (except the establishment of National Contact Points) but pleads for pursuing existing efforts instead of taking specific forward-looking actions.[103]

[60] (ii) The OEWG-Report equally flags the fact that capacity building is an important aspect of international cooperation in order to achieve an open, secure, stable, accessible and peaceful ICT environment (para. 55). The States should be guided by the following principles (para. 56): (i) Capacity building must be understood as a sustainable process, comprising specific activities by and for different actors; (ii) the activities must have a clear purpose and be result-focused; (iii) the measures need to be evidence-based, politically neutral, transparent, and accountable, etc. Again, these measures are to be implemented on a voluntary basis (para. 64) meaning that their realization depends upon the willingness of the States to go ahead with the respective actions.

96 Global Commission on the Stability of Cyberspace (supra n. 46), 23.

97 Dahinden (supra n. 5), 15.

98 See for example ICT4Peace, Work in Support of Norms of Responsible State Behavior and Confidence Building Measure in Cyberspace, https://ict4peace.org/activities/norms-of-responsible-state-behavior/?load=all.

99 Global Commission on the Stability of Cyberspace (supra n. 46), 23/24.

100 See Dahinden (supra n. 5), 10.

101 See Weber (supra n. 17), 90/91.

102 UN Doc. A/AC.290/2021/CRP.2.

103 ICT4Peace, The UN OEWG 2021 Final Report: Some Progress, Much Remains Unresolved, 3, https://ict4peace.org/activities/the-un-oewg-2021-final-report-some-progress-much-remains-unresolved/.

[61] Consequently, the respective international legal concepts must be operationalized by incorporating them into international and national policies as well as into legislation. This activity should also go along with a more intensive cyber diplomacy between the States; the most recent EU Cybersecurity Strategy drives into this direction and outlines potential initiatives that could be pursued in the near.[104]

6. Way Forward

[62] In order to achieve a reasonable cybersecurity governance encompassing the necessary steering functions the new regulatory framework must be based on international legal concepts and be implemented 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.[105] Such kind of multistakeholder approach appears to have the best chances in realizing an appropriate regulatory framework.

6.1. Need of a Cooperative Approach

[63] 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. Risk prevention and risk mitigation are issues requiring cooperation between States; therefore, the implementation of a broadly understood duty of cross-border cooperation as a general legal standard is required.[106]

[64] Risk prevention and risk mitigation are not only a governmental task but also a matter to be dealt with by private actors. In particular, precautionary measures can be taken by the market participants; insofar, generally accepted data/information security standards are existing; for example, the network security provisions of ISO/IEC 27001 of 2013 as well as the updated specific security provisions of ISO/IEC 27701 of 2019 are widely complied with by the concerned industry.[107]

[65] Previous experience in the field of cybersecurity has shown that the traditional international law approach operating on the State level through multilateral treaties, thereby failing to directly address duties of private actors, is hardly able to cope with the challenges of combatting interference with the integrity of the Internet (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 2017/18 when suggesting the adoption of an international treaty to guarantee the peaceful use of cyberspace.[108] The proposal to develop a Digital Geneva

104 For further comments see Bendiek/Kettemann (supra n. 28), 1 et seq.

105 Weber (supra n. 3), 307.

106 For further details Rolf H. Weber, Duty of Co-operation as New Cybergovernance Concept, Jusletter IT, 25 February 2021, passim.

107 International Standardisation Organisation, ISO/IEC 27001:2013, https://iso.org/standard/54534.html.

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

Convention envisaged to implement an international legal instrument similar to the Treaty on the Non-Proliferation of Nuclear Weapons and the Treaty on Chemical Weapons; these examples of international regimes have the objective of limiting vital threats to human existence. However, the Microsoft proposal met the scepticism of many States and it also seems to be unclear to what extent other Internet stakeholders could be included in such an arrangement.[109]

[66] Since Microsoft's Convention proposal did not really advance, a new initiative has been established, namely the Geneva Dialogue on Responsible Behaviour in Cyberspace.[110] This initiative, mainly led by Switzerland, should contribute to shaping a joint vision regarding the security of digital products/services and to enhancing those global policy processes which attempt to achieve a trusted, secure, and stable cyberspace. During phase 1 of the Geneva Dialogue a so-called Baseline Study was published in June 2019 by DiploFoundation,[111] based on two framework documents of November 2018, prepared by the private sector and by civil society. The Geneva Dialogue envisages to develop common policy requirements for boosting the security of digital products as well as to improve the feedback loop between corporate efforts and cybersecurity processes that develop norms, regulations, policies, and standards during the ongoing phase 2 in 2021.

6.2. New International Efforts

[67] As mentioned, the open-ended working group on developments in the field of information and telecommunications related to international security (OEWG) adopted the Final Substantive Report of the involved participants on 12 March 2021 (OEWG-Report).[112] At the beginning, political observers did not expect that the large number of involved countries would unanimously agree on certain principles within relatively short time. Amongst others, the OEWG has developed rules, norms and principles for responsible State behaviour (paras. 24–29 of the Report), followed by specific recommendations (paras. 30–33 of the Report). The respective norms are voluntary and non-binding; however, progress should be made by way of shared experiences and good practices.

[68] Furthermore and most importantly, the OEWG points to the relevance of taking into account the principles and concepts of international law (paras. 34–40 of the Report) which should be concretely applied to the use of ICTs in the context of international security (para. 38 of the Report). The reference to international law takes up the respective recommendation of the fifth UNGGE (2016/17).[113] But the OEWG-Report is insofar only a reiteration of the status quo and does not advance the inclusion of international law into the policies' design.[114] In particular, some States (China, Cuba, Belarus) voiced their opposition to the applicability of international humanitarian law, arguing that such a perception could be seen as justification of cyberspace militarization. However, this argument does not appear to be very convincing since the applica-

109 Therefore, Brad Smith, CEO of Microsoft, proposed the name A Digital Geneva Convention to protect cyberspace.

110 See https://genevadialogue.ch.

111 See https://genevadialogue.ch/wp-content/uploads/Geneva-Dialogue-Baseline-Study.pdf.

112 UN Doc. A/AC.2090/2021/CRP.2.

113 See above chapter 2.1.

114 See also the critical assessment of ICT4Piece (supra n. 103), 3.

bility of international humanitarian law would be suitable to limit or prevent the development of new cyber capabilities.[115]

[69] In addition, the OEWG Report does not clearly address and emphasise the multistakeholder concept playing a central role in the Internet Governance context.[116] Equally, the efforts of the UN realizing an environment of digital cooperation (UN High-Level Panel Report of 2019 and UN Secretary-General's Roadmap of 2020) are not prominently reflected. Such omissions contradict the inherent value of the cyberspace governance ecosystem that touches upon aspects which have a common interest character being a well-known concept in international law.[117]

[70] Summarizing, in a nutshell, 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 coordinated regulatory framework are required; the recent OEWG Report can serve as a starting point, however, it does not suffice as a solid foundation for a safe environment.

[71] Moreover, the widely accepted international legal notions such as the concept of public goods, the concept of shared spaces and the concept of State responsibility might be a good way to go forward. The normative contents of these concepts can give guidance for cybersecurity governance and potential behavioural rules designing the ecosystem of a stable and resilient cyberspace. Thereby, it is also up to businesses and academics to contribute to these efforts with more emphasis.

Prof. Dr. Rolf H. Weber, is professor of international business law at the Law Faculty, Zurich University, Switzerland (rolf.weber@rwi.uzh.ch). There he acts as co-director of the Research Program on Financial Market Regulation, the Center for Information Technology, Society, and Law as well as the Blockchain Center. He is also member of the Editorial Board of Swiss and international legal periodicals and a practicing attorney-at-law at Bratschi Ltd., Zurich (rolf.weber@bratschi.ch). An earlier shorter version of this article was presented at the Annual Symposium of GigaNet during the Internet Governance Forum on 2 November 2020.

All Internet sources were last visited on 20 April 2021.

115 See also the critical assessment of DiploFoundation, What's new with cybersecurity negotiations? UN Cyber OEWG Final report analysis, 5, https://www.diplomacy.edu./blog/.

116 See DiploFoundation (supra n. 115), 7; for a very recent overview of the multistakeholder concept see Weber (supra note 17), 44 et seq. with further references.

117 Weber (supra note 17), 101.