Integrity in the 'Infinite Space' – New Frontiers for International Law

Rolf H. Weber*
University of Zurich, Zurich, Switzerland
rolf.weber@rwi.uzh.ch

Abstract 601
Keywords 602
I. Introduction 602
II. Internet Integrity and Cybersecurity Challenges 603
1. From Cybersecurity to Cyber Resilience 603
2. Limited Impact of Existing Cybercrime Instruments 605
III. Searching the Holy Grail: Embedding Internet Integrity into International Legal Concepts 607
1. Moving to Global Cosmopolitan Governance 607
2. Coping with Digital Sovereignty 609
IV. Fructification of Available Legal Concepts 610
1. Concept of Global Public Goods 610
2. Concept of Shared Spaces 612
a) Objective of the Concept 612
b) Examples: Comparable International Legal Instruments 613
c) Starting Point for Cooperation 615
3. Concept of State Responsibility and Due Diligence 616
4. Further Potential Concepts 618
V. Relevance of Soft Law for Internet Integrity 619
1. Self-Regulatory Approaches 619
2. Co-Regulatory Approaches 621
VI. Forward-Looking Perspectives 624
1. Implementation of International Legal Concepts Based on Soft Law 624
2. Search of New Paths Leading to Internet Integrity 624

Abstract

Internet integrity encompassing the security, stability, robustness, and resilience of the most widely used global infrastructure has become a key topic of governance debates. The early emphatic cyberspace pronouncements volatilised; in addition, network security influence interests and national Internet policies increasingly jeopardize the global normative order. Since multilateral treaties are hardly suitable to realize an open space, international

* The Author is Professor at the University of Zurich, Faculty of Law.

DOI 10.17104/0044-2348-2021-3-601 ZaöRV 81 (2021), 601-626

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

legal concepts, particularly the concept of global public goods, of shared spaces, and of State responsibility, merit to be applied on a wider scale. Thereby, a bridge should be built between Internet governance principles and public international law.

Keywords

Concept of Shared Spaces – Concept of State Responsibility – Co-Regulation – Global Public Goods – Internet Integrity – Soft Law

I. Introduction

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. The now 25 years old 'Declaration of Independence of Cyberspace' (John Perry Barlow) does not suffice. Yet the current approach of politicians, scholars and practitioners shows a pertaining reluctance to embrace the challenges posed by global cyber governance in respect of present and future cross-border electronic networks, notwithstanding the fact that Internet regulations deserve a steady place in the international law dogmatic.

In particular, available international legal concepts are not yet sufficiently debated in the policy-makers' circles. Internet governance principles should be contextualised within public international law. The classification into different categories must be overcome and replaced by bridge-building efforts. The '*Infinite Space*' (as coined by Star Trek almost ten years ago) may not remain without normative guidelines designing an appropriate social order.

This article attempts at contributing to the building of bridges between the discussed Internet governance principles and public international law. The specific research object of the article is the not yet widely analysed issue of *Internet integrity*. At various existing venues, the practically important Internet integrity is debated but the narratives are often dispersed. In addition, the Internet as the most important global network is still not seen as a stable part of international legal scholarship.[1] Nevertheless, the article does not reflect the decades old argument of 'the law of the horse'[2] but rather develops ideas

1 For a first attempt into this direction see Joanna Kulesza and Rolf H. Weber, 'Protecting the Internet with International Law', Computer Law & Security Review 40 (2021), 105531, 1 ff.

2 See Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach', Harv. L. Rev. 113 (1999), 501-549, reacting to Frank H. Easterbrook, 'Cyberspace and the Law of the Horse', University of Chicago Legal Forum 1 (1996), 207-216.

 DOI 10.17104/0044-2348-2021-3-601

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

for a comprehensive and future-oriented assessment of the today prevailing challenges.

At the beginning, the research object, namely Internet integrity being exposed to security challenges, is discussed (chapter II.). Thereafter, the article develops the relevant elements which can embed Internet integrity into the existing pillars of public international law (chapter III.), to be followed by the main part of the article analysing a possible fructification of acknowledged legal concepts in this context (chapter IV.). Subsequently, the relevance of soft law for Internet integrity is laid out (chapter V.). The article closes with the presentation of forward-looking perspectives outlining new paths that are suitable to realise Internet integrity (chapter VI.).

II. Internet Integrity and Cybersecurity Challenges

The integrity of the Internet depends on its proper functioning without technical interference and (unjustified) governmental intervention. The technical setting must ensure that data is real, accurate, and safeguarded from unauthorised modification. The preservation of these qualities is a matter of proper governance of the Internet environment.

The term governance can be traced back to the Greek word *kybernetes*, the steersman, leading though the Latin word *gubernator* to the English notion *governor* addressing aspects of steering and governing behaviour.[3] Consequently, cyber governance looks at the measures taken by the concerned actors with the objective to protect information and data as well as the underlying assets and infrastructures.

1. From Cybersecurity to Cyber Resilience

During the last few years, different terms have been coined with the objective of safeguarding the integrity of the Internet. At the beginning, (i) *cybersecurity* was the most commonly used word, followed by other notions such as (ii) *cyber stability* and (iii) *cyber resilience*; these terms can be described in short as follows:

(i) *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,

3 Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges (Zurich: Schulthess 2009), 2.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

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'.[4] The International Telecommunication Union 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 organisations' and users' assets'.[5] Apart from the unclear definition, cybersecurity encompasses two different relevant phenomena, namely the traditional cybercrime appearances and the increasingly important 'cyberwar' phenomena.

(ii) *Cyber stability* means that everyone can be reasonably confident in the ability to use the Internet and – generally – cyber space in a safe and secure manner; this relatively new term having recently gained importance addresses the availability and integrity of services and information to be provided in a secure way.[6]

(iii) *Cyber resilience* is the ability to provide and maintain an acceptable level of service rendering as well as to deliver the offered or envisaged outcome, despite adverse cyber events.[7] This term was mainly developed in the context of private organisations' risk management frameworks.

Notwithstanding the above described *cyber notions*, general security objectives including (i) confidentiality, (ii) integrity, and (iii) availability, also known as the CIA triad of the information security industry, always play an important role. Confidentiality means that information is not improperly disclosed to unauthorised individuals, processes, or devices; integrity refers to information being protected against unauthorised modification or destruction; availability pertains to a timely and reliable access to data and information for authorised users.[8] The International Organisation for Standardisation (ISO) defines information security as the preservation of confidentiality and availability in its ISO/IEC (International Electrotechnical Commission) 27'000:2018 standards on Information Security Management Systems.[9]

---

4 Karen O'Donoghue, 'Some Perspectives on Cybersecurity', Internet Society 2012, <https://www.internetsociety.org>.

5 ITU Definition: <http://www.itu.int>; for a more general overview see Rolf H. Weber and Evelyne Studer, 'Cybersecurity in the Internet of Things: Legal Aspects', Computer Law & Security Review 32 (2016), 715-728 (716-717).

6 Global Commission on the Stability of Cyberspace (GCSC), Advancing Cyberstability, Final Report (IGF Berlin: November 2019), 13.

7 Fredrik Björck, Martin Henkel, Janis Stirna and Jelena Zdravkovic., 'Cyber Resilience – Fundamentals for a Definition', <https://doi.org/10.1007/978-3-319-16486-1_31>.

8 Rolf H. Weber, 'Cybersecurity in International Law' in: Asian Academy of International Law (ed.), *2019 Colloquium on International Law* (Hong Kong: AAIL 2020), 279-308 (281).

9 See <https://www.iso.org/>.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

This article does not analyse the details of existing legal instruments (or their preparatory documents) combatting cybercrime, but only mentions their existence and some key messages at the beginning. Moreover, the article has the objective to assess in more depth to what extent the established and widely accepted international legal concepts (in particular the concept of global public goods, of shared spaces, and of State responsibility) can contribute to an acceptable cyber governance (chapter IV.). These legal concepts do not coincide with the international legal principles as contained in the Statute of the International Court of Justice (mainly article 38) and often addressed in the traditional discipline of public international law. The hereinafter discussed legal concepts could further be supported by the already existing self- and co-regulatory initiatives (chapter V.).

2. Limited Impact of Existing Cybercrime Instruments

For decades, international and regional organisations have tried to develop legal instruments that could harmonise the regulatory standards mainly in the field of cybersecurity prevention.[10] Some efforts have been (partly) successful, particularly if implemented by sector-specific international organisations (e. g. International Telecommunication Union, World Trade Organization).[11] However, in the most intensively discussed area, namely cybercrime, the outcomes are rather limited; in addition, cybercrime only covers a part of Internet integrity, for example not a network disruption for political reasons.

On the global level, legal instruments intending to combat cybercrime are discussed for quite some time. Already five United Nations Groups of Governmental Experts (UNGGE) have exchanged ideas and published reports, without, however, being able to agree on binding principles.[12] The most forward-looking statement in respect of the importance of the hereinafter addressed international law has been made by the fourth UNGGE:

> '1. In the 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.

10 For an overview see Weber (n. 8), 284 ff.

11 Specific security provisions are contained in the ITU- and WTO-Agreements (for further details Weber [n. 8], 288-290).

12 For further details see Kulesza and Weber (n. 1), 5-6, and 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 (4 ff.).

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

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.'[13]

Recently, two new groups, namely (i) a further UNGGE and (ii) the United Nations (UN) Cyber Open-ended Working Group (OEWG), have been established (based on not really coherent mandates) with the objective to work out further cybersecurity recommendations in the course of 2021. In March 2021, the OEWG published its Final Substantive Report,[14] but the guidelines remain quite vague. Therefore, the mentioned assessment of the fourth UNGGE that the key principles (or concepts) of international law should play a major role remains valid.

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).[15] The European Union (EU) released the Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union on 6 July 2016[16] with the main objectives/measures of improving (i) national cybersecurity capabilities, (ii) the cooperation on the EU-level and (iii) the security and incident notification requirements as well as the Cybersecurity Act in 2019.[17] As a noteworthy remark it may be added that the term digital infrastructure is mentioned in Annex III of the Network and Information Systems (NIS)-Directive alongside to energy, transport, banking, health sector, and drinking water supply as a critical infrastructure.[18]

Reality shows that in particular the efforts on the global level for the implementation of cybercrime regulations have failed to be successful. Even

13 UNGGE on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of 26 June 2015, A/70/174.

14 For the appointment see UNGA Resolution 73/266 of 22 December 2018, A/RES/73/266 and UNGA Resolution 73/27 of 5 December 2018, A/RES/73/27; for the OEWG-Report of 10 March 2021 see UN Doc. A/AC.290/2021/CRP.2; a first critical analysis of the Report can be found in Rolf H. Weber, 'Cybersecurity Governance – international law as policy driver?', Jusletter IT, 27 May 2021, no. 12 and nos 67-69.

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

16 OJ 2016 L 194/1 of 19 July 2016.

17 Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ 2019 L 151/15.

18 To the discussions in the context of Annex III see Joanna Kulesza und Rolf H. Weber, Protecting the Public Core of the Internet (Delhi: GCSC 2017), 2017, 75-98 (87), <https://www.researchgate.net>; see also Weber (n. 14), no. 16.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-ZA

the CoE Cybercrime Convention did not have remarkable effects.[19] The EU legal instruments are restricted to their regional scope of application. In addition, as mentioned, traditional cybercrimes only are a limited part of the issues influencing the integrity of the Internet, not even covering all aspects of cybersecurity as well as neglecting the elements of cyber stability and cyber resilience.

This assessment justifies a broader analysis of the possibilities to make the international legal concepts fruitful in the Internet integrity context. The objective of this article consists in the attempt of finding a proper foundation for the improvement of Internet integrity. By purpose, not the well-known international legal principles of public international law as stated in Article 38 of the Statute of the International Court of Justice but the widely acknowledged cyberspace concepts will be in the focus of the considerations.

III. Searching the Holy Grail: Embedding Internet Integrity into International Legal Concepts

1. Moving to Global Cosmopolitan Governance

In public international law, it is not contested that new norms and policies should be developed in order to enhance the global security, stability and resilience of the Internet. As Martti Koskenniemi has recently noted, international law contributes to global governance aiming at a 'cosmopolitan future, a united humanity governed by a global law'.[20] The concept of cosmopolitanism drives towards a certain decentralization of State power in the interest of a more global appreciation.[21] An appropriate policy framework encompassing democratic and accountable global governance principles is the most suitable way of implementing cosmopolitan concepts of justice.[22]

19 Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation', Mon. L. R. 40 (2014), 698-736 (701 ff.); Weber (n. 8), 283-284.

20 Martti Koskenniemi, 'International Law as "Global Governance"' in: Justin Desautels-Stein and Christopher Tomlins (eds), *Searching for Contemporary Legal Thought* (Cambridge: Cambridge University Press 2017), 199-218 (199); see also Rolf H. Weber, 'New "Cosmopolitically" Founded Concepts for the Cyberworld' in: Giovanni Biaggini, Oliver Diggelmann and Christine Kaufmann (eds), *Polis und Kosmopolis, Festschrift für Daniel Thürer* (Zurich and Baden-Baden: Dike and Nomos 2015), 779-786 (781-782).

21 See Francis Fukuyama, *Governance and World Order of the Twenty First Century* (Ithaca NY: Cornell University Press 2004), 98-99.

22 For further details see Rolf H. Weber, *Internet Governance at the Point of No Return* (Zurich: EIZ Publishing 2021), 37-38.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

The merits of the international legal concepts to be discussed hereinafter are reflected in the fact that some constitutional norms have already emerged at the global level, even if tensions can exist between different spheres of policy-making and even if the categories that supported universalism from relativism are blurred.[23] In this context, the term societal constitutionalism (Teubner) has been coined to explain developments in civil society and provide for general foundations of rule-making by way of normative standards.[24] Similarly, the term digital constitutionalism is used to describe the practice of articulating a set of political rights, governance norms, and limitations on the exercise of powers on the Internet.[25]

In addition, scholars increasingly acknowledge that based on actual cooperation in networks even treaty compliance might gain better attention in solution-oriented systems of transgovernmentalism.[26] Strategies of transnational advocacy networks in digital constitutionalism have been mobilised from a political and a legal angle. Based on a wide variety of theoretically developed and potentially applicable regulatory models[27] it is generally acknowledged that global civil society in a transnational sphere must encompass manifold stakeholders that realise shared values, dense exchanges of information, and a common discourse.[28]

As a concrete translation of general governance principles in the Internet integrity context, the Global Commission on the Stability of Cyberspace (GCSC) has proposed a comprehensive Cyberstability Framework in November 2019, at the occasion of the Internet Governance Forum (IGF) in Berlin, encompassing (1) multistakeholder engagement, (2) cyber stability principles, (3) development and implementation of voluntary norms, (4) adherence to international law, (5) confidence building measures, (6) capacity building objectives, and (7) open promulgation and wide spread use of technical standards ensuring cyber stability.[29] This framework has again been presented at the (virtual) Internet Governance Forum in November 2020,

23 Gunther Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalisation* (Oxford: Oxford University Press 2012), 51-52.

24 Teubner (n. 23), passim; Weber (n. 20), 781-782.

25 See Dennis Redeker, Lex Gill and Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights', International Communication Gazette 80 (2018), 302-319 (302-303).

26 See Kal Raustiala, 'The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law', Va. J. Int'l L. 43 (2002), 1-92 (1, 23-24, 55-56, 76).

27 The manifold regulatory models cannot be discussed in the context of this article; for a detailed description, differentiating between first generation and second generation regulatory models see very recently Weber (n. 22), 17 ff. with further references.

28 See Weber (n. 22), 44 ff. with further references.

29 GCSC (n. 6), 14.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

however, the future paths have not yet been clearly defined for the time being.

2. Coping with Digital Sovereignty

The sovereignty principle has its roots in the 16th century. As term originally coined by the philosopher and legal scholar Jean Bodin (1576), the historical concept goes along with the building-out of nation States.[30] The first political document enshrining the sovereignty thinking and prominently reflecting this concept is the Westphalian Peace Treaty of 1648.[31] Among others, this document contains the right of each State to monopolise certain exercises of power within its territory.

In the meantime, the global infrastructures as well as some international legal instruments (particularly the UN Charter) set limits to national legislation. Therefore, the traditional sovereignty concept must address alternative values in the context of power allocation. In other words, governance is changing under conditions of interconnectedness now happening. Such a new concept of cooperative sovereignty should lead to a shared responsibility for global resources and to the establishment of standards for interstate cooperation.[32]

During the last few years, political sensitivities related to sovereignty aspects again gained importance. Nation States more frequently claim a right to control the infrastructures and the data flows. As a new term, the notion of digital (or data) sovereignty has been coined.[33] The respective right is invoked by States as a protective or empowerment stance regarding a multitude of stakeholders.[34]

However, an extensive notion of digital sovereignty causes the risk that international governance principles will become re-nationalised and the global Internet evolves into a so-called 'Splinternet', particularly since some countries think of creating an independent national Internet.[35] Such a development that leads to fragmentation is undesirable; any kind of fragmentation

30 Weber (n. 22), 87.

31 Kulesza and Weber (n. 1), 3.

32 For further details see Weber (n. 22), 87-88 with additional references.

33 The term digital sovereignty is partly also used for the vision of digital self-determination being the autonomy of individuals and their right to control the data they own or generate. This notion is not further discussed hereinafter.

34 See Internet & Jurisdiction Policy Network, *We Need to Talk About Data – Framing the Debate Around the Free Flow of Data and Data Sovereignty*, Paris 2021, 35 ff., 39, <https://www.internetjurisdiction.net>.

35 Weber (n. 22), 88-89.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

would not be future-oriented and have a negative impact on global infrastructures.[36]

Consequently, in order to avoid fragmentation, the governance functions should remain embedded in horizontal structures creating a multistakeholder environment.[37] In addition, a political force is needed to stand up for the value of global connectivity and for the right of people everywhere to self-govern their online transactions.[38] The respective substantive foundation of the interrelations can be built by the hereinafter discussed international legal concepts.

IV. Fructification of Available Legal Concepts

Based on the described theoretical concepts of global governance, the general assessment can be made that Internet integrity might be reasonably warranted if the international community is ready to accept some basic and common legal standards being applicable around the globe (in addition to the mentioned international legal principles of the International Court of Justice Statute).[39] Several theoretical models have been developed so far; as the most important international legal notions, the concepts (i) of global public goods, (ii) of shared spaces, and (iii) of State responsibility will be further analysed hereinafter.

1. Concept of Global Public Goods

One of the starting points for a discussion on protecting the integrity of the Internet could be the concept of global public goods.[40] Although not

36 Daniel Voelsen, *Risse im Fundament des Internets: Die Zukunft der Netzinfrastruktur und die globale Internet Governance*, SWP-Studie, Berlin 2021, 27-28; Milton Mueller, *Will the Internet Fragment?, Sovereignty, Globalization, and Cyberspace* (Cambridge: Polity 2017), 131.

37 Roxana Radu, *Negotiating Internet Governance* (Oxford: Oxford University Press 2019), 194.

38 See also Weber (n. 22), 88-89, and Mueller (n. 36), 131-132.

39 Already 15 years ago, Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law' in: Max Planck UNYB, Vol. 10 (The Hague: Brill 2006), 191-272 (271), called on international law to 'take a normative stance' in respect of the Internet's future. Recently, Matthias C. Kettemann, *The Normative Order of the Internet* (Oxford: Oxford University Press 2020), 81 ff., analysed the general principles of international law in depth.

40 For a general overview see Inge Kaul, Isabelle Grunberg and Marc A. Stern 'Defining Global Public Goods' in: Inge Kaul, Isabelle Grunberg and Marc A. Stern (eds), *Global Public Goods: International Cooperation in the 21st Century* (Oxford: Oxford University Press 1999), 2-19 (10 ff.); Rolf H. Weber and Valérie Menoud, *The Information Society and the Digital Divide: Legal Strategies to Finance Global Access* (Zurich: Schulthess 2008), 24 ff.; Gregory Shaffer, 'International Law and Global Public Goods in a Legal Pluralist World', EJIL 23 (2012), 669-693 (675 ff.); Nico Krisch, 'The Decay of Consent: International Law in an Age of Global Public Goods', AJIL 108 (2014), 1-40 (1 ff.).

 DOI 10.17104/0044-2348-2021-3-601

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

perfectly aligned to the needs of Internet integrity 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 to (iii) present generations without jeopardising the ability of future generations to meet their own needs.[41] Insofar, the global public goods contribute to the common heritage of mankind.

The idea of guaranteeing Internet integrity as a public core element of the international infrastructure 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 globalisation, is derived from the economic literature on public goods.[42] 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.[43]

International law in its traditional form with its consensus-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 main 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.'[44]

Nevertheless, experience over the last few years has shown that international law is not without solutions to such problems.[45]

Furthermore, from an international law perspective, global public goods theories are not a totally new approach. The idea of a certain communality (or common interest) already lies at the core of the Roman law concepts of

41 Weber and Menoud (n. 40), 24.

42 Krisch (n. 40), 3 ff.; see also International Task Force on Global Public Goods, *Meeting Global Challenges: International Cooperation in the National Interest*, Final Report, Stockholm 2006, 15.

43 Kulesza and Weber (n. 1), 4.

44 William D. Nordhaus, Paul Samuelson and the Global Public Goods (New Haven: Yale University 2005), 8, <http://www.econ.yale.edu>.

45 See also Krisch (n. 40), 4.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

ius cogens as expression of compelling law or of a peremptory norm based on a universal agreement and of *erga omnes* encompassing rights and obligations being owed toward all.[46] Similarly, the concept of critical infrastructures and their protection is suitable to serve as another complementary point of reference.[47] In addition, the well-known public interest concept is also able to peremptorily impose binding obligations on States that have a similar foundation.[48] Based on these thoughts it can be argued that global public goods theories involve a relatively broad approach that considers political economy implications besides legal aspects[49] and, therefore, merits attention in future discussions.

2. Concept of Shared Spaces

a) Objective of the Concept

International cooperation in the context of infrastructure protection is not the only analogy to be drawn from existing legal frameworks.[50] Equally, for example, the concept of shared spaces, to be used by all States in a uniform, non-harmful way is quite well known to the international community and in international relations. Already Grotius in the 17th 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'.[51]

Many global legal areas, constituting a 'law of international spaces',[52] 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

46 Weber and Menoud (n. 40), 24; Kettemann (n. 39), 33-36; Peter-Tobias Stoll, 'Global Public Goods: the Governance Dimension' in: Volker Rittberger, Martin Nettesheim and Carmen Huckel (eds), *Authority in the Global Political Economy* (New York: Palgrave Macmillan 2008), 116-136 (116 ff.).

47 See below chapter V.2.

48 Weber (n. 8), 304.

49 Weber and Menoud (n. 40), 25-27.

50 Rolf H. Weber, *Realizing a New Global Cyberspace Framework* (Zurich: Schulthess 2014), 19.

51 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*, Leiden 1609, ed. by James Brown Scott (New York: 1916), 5. An impressive new analysis of the international rule of law has recently been given by Martti Koskenniemi, 'Imagining the Rule of Law: Reading the Grotian "Tradition"', EJIL 30 (2019), 17-52.

52 This term was introduced by John F. Kish, *The Law of International Spaces* (Leiden: Sijthoff 1973).

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

States. Indeed, several authors already expressed the opinion that Internet safety and security can be seen as a shared responsibility.[53]

b) Examples: Comparable International Legal Instruments

Based on this understanding, several areas of international law appear to be suitable for reference as emanations of a legal order that guarantees common values similar to Internet integrity:[54]

(i) *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.[55] The main purpose of this treaty consists (i) in the submission of all outer space activities to international law, as well as (ii) in the implementation of the principles of non-discrimination and of non-appropriation by any claim of sovereignty.[56] Air law is also subject to many multinational treaties under the auspices of the International Civil Aviation Organization (ICAO).[57] In fact, the law of outer space appears to be the most prominent example for the implementation of the shared spaces concept.

(ii) *Law of the sea*: The most important rules for the maritime area are contained in the Convention on the High Seas of 1958 and the Convention on the Law of the See of 1982.[58] 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 and in the regulation of the common space (i. e. the oceans) for the economic exploitation.[59] Therefore, the legal instruments governing the maritime environment are good examples for the concept of shared spaces.

(iii) The laws of outer space and of the seas are particularly showing the importance of cooperative efforts in protecting common interests.[60] But other areas of law equally know this underlying thought. Even if the parallelism is less

53 See Vinton G. Cerf, Patrick Ryan, Max Senges and Richard Whitt, 'IoT Safety and Security as Shared Responsibility', Business Informatics (2016), 7-19 (15-16).

54 Kulesza and Weber (n. 18), 88; see also the compilation of articles in Mads Andenas et al. (eds), *General Principles and the Coherence of International Law* (Leiden and Boston: Brill-Nijhoff 2019).

55 610 UNTS 205.

56 See also Weber (n. 50), 21; Joanna Kulesza, *International Internet Law* (London and New York: Routledge 2012), 145-146.

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

58 450 UNTS 11; 1833 UNTS 397.

59 See also Weber (n. 50), 20.

60 For further details to the duty of cooperation see Rolf H. Weber, 'Duty of Co-operation as New Cybergovernance Concept', IT Jusletter, 25 February 2021.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

obvious and the respective legal areas cannot always be easily linked to the shared spaces concept at first sight, the following legal instruments merit to be mentioned:[61]

- *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.[62] In substance, the compliance with shared values is envisaged.
- *International human rights law*: The need to harmonise global rules in the context of human and fundamental rights has become obvious in the aftermath of the Second World War; the key documents are condensed in the International Bill of Human Rights, composed of the UN Universal Declaration of Human Rights (UDHR, 1948)[63] as well as the two UN Covenants on Civil and Political Rights and on Economic, Social and Cultural Rights (ICCPR and ICESR, 1966). Again, these international legal instruments express shared values of humankind.
- *International telecommunication law*: The International Telecommunications Union is the second-oldest international body having been founded in 1865; the need to harmonise the communications' rules has been obvious since then and has even become more important with the advent of the Internet.[64] As in case of outer space law, the telecommunications infrastructure is a space which needs to be shared by the interested players.
- *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).[65] Over time, environmental law will increasingly become an area that requires the implementation of common values in spaces to be shared by everybody.

---

61 This article cannot dig into all details of the mentioned legal instruments; further research deepening the analysis would be worthwhile; see also Weber (n. 14), nos 35-44.

62 500 UNTS 95. Similar principles are contained in the Vienna Convention on Consular Relations of 1963.

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

64 See also Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyberoperations* (Cambridge: Cambridge University Press 2017), 284 ff.; Richard Hill, *The New International Telecommunications Regulations and the Internet* (Zurich: Schulthess 2013), 141 ff.

65 A very clear picture can be drawn from the different reports of the Intergovernmental Panel on Climate Change (IPCC); see for example: An IPCC Report on the impacts of global warming of 1,5°C above preindustrial levels and related global greenhouse gas emission pathways, in the context of strengthening the global response to the threat of climate change, sustainable development, and efforts to eradicate poverty, Summary for Policymakers (October 2018).

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

- *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 the liberalisation of global trade and a rule-based system on trade are of utmost importance.[66] Harmonised rules facilitate the realisation of common (economic) interests.
- *Money laundering and terrorism financing laws and policies*: The fight against money laundering and terrorism financing is a global task. The respective activities are exercised by the Financial Action Task Force (FATF) that has been created as an intergovernmental organisation in 1989 on the initiative of the G7; the standards of the FATF being domiciled at the Organisation for Economic Co-operation and Development (OECD) in Paris are accepted as international recommendations by the World Bank, the International Monetary Fund and the UN Security Council (Resolution 2462 of 28 March 2019).[67] The developed global measures of the FATF have some similarities with the measures combating the negative effects of cyberattacks; both initiatives attempt at safeguarding shared values.

So far, a concise assessment based on the mentioned areas of international law and relations is still outstanding; nevertheless, the basic principles can be made fruitful in the Internet integrity context.

c) Starting Point for Cooperation

From the analysis of the comparable international legal instruments the conclusion can be drawn that the main examples for a cooperative approach to shared spaces (law of outer space and of the seas) as well as the other legal segments pursuing similar objectives show the importance of further research that could deepen the concept of international spaces as well as the cooperation therein.

As mentioned, each of the referenced legal regimes offers interesting insights that can be useful to Internet integrity, however, a more focussed analysis is needed in order to develop a harmonised and stable framework of global policies. In particular, governments should closely cooperate in continuing efforts to arrive at an operable consensus that takes into consideration

66 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.

67 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>.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

global interoperability, network stability, reliable access, and cybersecurity due diligence.[68]

3. Concept of State Responsibility and Due Diligence

The concept of State responsibility can be perceived as a general normative guideline, applicable in addition to all other specified international legal norms imposing obligations (for example the no harm principle) upon States.[69] 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. In contrast to the already mentioned concepts (public goods, shared spaces), the State responsibility principle enshrines a more condensed legal apparatus as an international legal tenet due to its written implementation.[70]

The development of legal rules related to the State responsibility was not an easy task; the efforts of the International Law Commission (ILC) lasted decades; the so-called Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001) have been adopted by UN General Assembly Resolution 56/83 and have become part of the customary law also applied by the International Court of Justice.[71] The ILC based its work on two fundamental presumptions:[72] (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 concept as of the ILC Draft Articles is materially linked to the due diligence requirements being an underlying in substance and 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

68 Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', International Legal Studies 89 (2013), 123-156 (134 ff.). For concrete examples of cooperative approaches see chapters V.1 and V.2.

69 Joanna Kulesza, *Due Diligence in International Law* (Leiden and Boston: Brill/Nijhoff 2016), 115 ff.

70 See also Kulesza and Weber (n. 1), 9 with further references.

71 Draft Articles on Responsibility of States for Internationally Wrongful Acts, ILC Report, 2001, UN Doc. A/56/10 att. 10, (2001) ILCYB, Vol. II, Part Two.

72 Kulesza (n. 69), 149 ff. with further references; see also Jovan Kurbalija, 'State Responsibility in Digital Space', Swiss Review of International and European Law 26 (2016), 307-325 (318 ff.); Weber (n. 22), 95-96.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

of international relations between States.[73] In the meantime, however, the due diligence principle has even been extended to non-State actors; apart from being a shared element of treaty-based regimes[74] its increasingly broad scope of application also encompasses private actors such as multinational enterprises (as for example shown in the OECD Due Diligence Guidance).[75]

The concept of due diligence intending to prevent transboundary harm has mainly become important in environmental matters.[76] Nevertheless, by analogy, a due diligence standard for Internet integrity with shared responsibility[77] 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.[78] The existing community standards with regard to good business practices related to each of the specific Internet sectors (e. g. root zone operation, Internet Exchange Point [IXP] operation, Domain Name System [DNS], and Top-Level-Domain [TLD] management)[79] could be considered as harmonised guidelines to be complied with in order to avoid 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.[80] 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 cyber-related due diligence.[81]

For the sake of completeness it may be added that according to the Tallinn Manual 2.0[82] general international law must be taken into account in respect of four legal notions, namely (i) sovereignty, (ii) due diligence, (iii) jurisdiction, and (iv) State responsibility.[83] 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, and while the Tallinn Manual 2.0 does not necessarily constitute a rule book for

73 Weber (n. 22), 94-95, with further references.

74 See also Kulesza (n. 69), 253 ff.; Kurbalija (n. 72), 323.

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

76 Kulesza (n. 69), 205 ff.; Kurbalija (n. 72), 312 ff.; Kettemann (n. 39), 95-96; Jay Butler, 'The Corporate Keepers of International Law', AJIL 114 (2020), 189-220 (209-210).

77 See also Cerf, Ryan, Senges and Whitt (n. 53), 8-9.

78 For further details see Kulesza (n. 69), 276 ff. and 288 f. with further references.

79 See below chapters V.1 and V.2 as well as Cerf, Ryan, Senges and Whitt (n. 53), 14.

80 Schmitt (n. 64), 30 ff.

81 Kulesza and Weber (n. 1), 9; to the due diligence principle in other legal areas see Kettemann (n. 39), 97-101.

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

83 See also Schmitt (n. 64), 11 ff. with further references; Schmitt formulates not less than 31 specific Rules.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-ZA

States,[84] the two other principles, namely due diligence and State responsibility, can be reasonably applied to the biggest international open networks and their key components.[85] As the Global Commission on the Stability of Cyberspace has identified, uniform standards of protection for the whole infrastructure and its services recognised as fundamental to the global networks' stable and reliable operations are necessary and can be expressed through (i) international cooperation, (ii) exchange of good practices, and (iii) benchmarking.[86]

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 guidelines. Nevertheless, further Internet-specific concepts have been developed that could also be made fruitful; in particular, the GCSC addressed the following legal notions:

(i) The *requirement of restraint* imposes on States 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.[87]

(ii) The *requirement to act principle* contains a duty to take affirmative action for preserving the stability of cyberspace; States and non-state actors should take care that inadvertently escalating tensions or increasing instability are avoided.[88]

(iii) Furthermore, *human rights* are important legal yardsticks that can safeguard cyberspace stability; the disruptive effect on human activity resulting from threats endangering the availability or integrity of information and communications technologies is obvious and impacts human rights of individuals in a severe way.[89]

The mentioned concepts as developed by the GCSC in respect of cyberspace stability equally contribute to and should be part of Internet integrity.

84 For a critical assessment of the Tallinn Manual 2.0 see Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', AJIL 112 (2018), 583 ff.

85 Weber (n. 8), 299.

86 GCSC (n. 6), 95.

87 GCSC (n. 6), 18.

88 GCSC (n. 6), 19.

89 GCSC (n. 6), 19.

 DOI 10.17104/0044-2348-2021-3-601

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

In addition, the eight specific norms drafted by the GCSC[90] are also important in respect of the Internet integrity environment. For example, the first norm reads as follows: '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.'

The above discussed international legal concepts must be kept in mind when assessing the notion of soft law hereinafter.

V. Relevance of Soft Law for Internet Integrity

Having analysed the importance and contents of applicable international legal concepts, the follow-up question arises what legal quality can be attributed to these concepts. Obviously, traditional legal instruments constituting hard law are not largely available in this context. However, alternative legal sources are equally suitable for the implementation of the discussed concepts.

Experience has namely 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.[91] Indeed, legal doctrine is now stating that the dichotomy between hard law and soft law must be overcome.[92] This assessment goes hand in hand with the acknowledgment that – in contrast to the traditional international public law understanding – private actors can also become 'keepers of international law'.[93] Alternative approaches of (private) rule-making equally encompass fundamental legal principles to be observed by the concerned actors; hereinafter, the two main forms, namely self-regulation and co-regulation, will be discussed.

1. Self-Regulatory Approaches

Self-regulation refers to the rules that are autonomously developed and implemented by the governed persons, independently from any structured

90 GCSC (n. 6), 21-22.

91 Rolf H. Weber, *Regulatory Models for the Online World* (Zurich: Schulthess 2002), 85 ff.

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

93 Term used by Butler (n. 76), 189.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

form of rule-making. 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.[94]

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.[95] 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.[96]

The strengths of self-regulation encompass the following elements:[97] (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 in the context of the critical Internet infrastructures: At least from a technical angle, the current Internet governance landscape was originally designed on the basis of bottom-up governance models, strongly rooted in the technical community, for example the Internet Society (ISOC) or the Internet Engineering Task Force (IETF) with its 'Requests for Comments' (RfC);[98] these bodies are implementing community-developed common standards to be voluntarily followed by their members, namely Internet service providers and software developers.[99]

While security by design remains a common paradigm within both, ISOC and IETF, a connection between this extra-legal, community-based rule-making approach and the hard norm-setting models of States cannot easily

94 Weber (n. 50), 23 with further references; see also Butler (n. 76), 199 ff.

95 Weber (n. 91), 81-83; Andrew Guzman and Timothy L. Meyer, 'International Soft Law', Journal of Legal Analysis 2 (2010), 171-225 (179-183).

96 Weber (n. 50), 25.

97 Weber (n. 91), 83-84 with further references.

98 Eric Rescorla, 'Guidelines for Writing RFC Text on Security Considerations' (2003), <https://tools.ietf.org>; see also Butler (n. 76), 209-210.

99 Kulesza and Weber (n. 18), 82.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

be established.[100] 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 Internet integrity policies and must be addressed by whatever model of global cyber governance.[101] There can be no effective 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.[102]

Looking from the angle of self-regulatory initiatives, the already discussed policy paper of the GCSC also advocates for the inclusion of private rule-makers (multistakeholderism).[103] The developed principles to be observed by States and non-state actors have the objective of securing an environment in which the actors do not 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).[104] In addition, actors are invited to implement appropriate measures to ensure basic cyber hygiene.[105] Taking into account the various approaches developed in the global arena of international organisations, private actors, and academic scholars, the norms and principles developed as private rule-making in the GCSC-Report merit to be further concretised.

2. Co-Regulatory Approaches

Self-regulatory initiatives can also be supported by international organisations or national governments. This approach is often called co-regulation being a term that has been coined more than 20 years ago in the context of broadcasting as public good (being one of the above discussed

100 Kulesza and Weber (n. 18), 82 and 89.

101 For the parameters of a cyberspace framework see Weber (n. 50), 102 ff.

102 For a thorough study of the impact of technical standards on cybersecurity see 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.

103 GCSC (n. 6), 17. For a more detailed discussion of the multistakeholder approach see Christine Kaufmann, 'Multistakeholder Participation in Cybespace', Swiss Review of International Law and European Law 26 (2016), 217-234; Rolf H. Weber, 'Legal Foundations of Multistakeholder Decision-Making', ZSR 135 (2016), 247-267.

104 GCSC (n. 6), 18-19; see also Kettemann (n. 39), 25-26.

105 See also Recital 8 of EU Cybersecurity Act 2019 (n. 17).

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

concepts).[106] An 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.[107]

Co-regulation as a model is often designed by a general framework established in the form of governmental regulations which than is concretised by the private sector; in other words, the State legislator sets the legal milestones 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.[108]

In the Internet governance environment the participation models encompassing governmental bodies and private actors has been coined by using the term multistakeholderism; this concept attempts at including all potentially concerned stakeholders in the relevant decision-making processes.[109] Even if multistakeholderism as an increasingly important governance model that cannot be discussed in depth hereinafter is not a value as such and not a one-size-fits-all solution, the concept remains a possible approach for meeting salient public interest objectives. In addition, it should not be overlooked that multistakeholderism is crucial in the traditional Internet environment (for example regarding the processes in ICANN) as well as in the general infrastructure context (for example within the International Telecommunication Union [ITU]).[110]

Since it is often difficult to fully tackle the Internet integrity 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

106 For an early discussion see Gareth Grainger, 'Broadcasting, Co-Regulation and the Public Good' Paris 1999.

107 Weber (n. 50), 23-24; Wolfgang Hoffmann-Riem, *Regulierung der dualen Rundfunkordnung* (Baden-Baden: Nomos 2000), 154-155.

108 Myriam Senn, *Non-State Regulatory Regimes. Understanding Institutional Transformation* (Berlin: Springer 2011), 43, 139-148, 230; Chris Marsden, Trisha Meyer and Ian Brown, 'Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation', Computer Law & Security Review 36 (2020) 105373, 1-18 (9).

109 The (in the meantime) far-reaching discussions about the multistakeholder concept (incl. its strengths and weaknesses) are not within the scope of this contribution (for a general overview see the authors cited in n. 103 with further references).

110 For further details see Kal Raustiala, 'Governing the Internet', AJIL 110 (2017), 491-503 (491, 495-496).

 DOI 10.17104/0044-2348-2021-3-601

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

market participants. Joint efforts of various stakeholders also allow the governments to assess the representativeness of self-regulatory standards and to judge the appropriateness of best practices; interventions appear justified if a higher level of protection measures is desirable.[111] Reality shows that such kind of co-regulatory approaches are already existing in the field of critical infrastructures:

(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'.[112] 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 servers, the Domain Name System (DNS), the Internet Protocol and the Internet backbone structures, as well as Internet Exchange Points (IXPs).[113] The CoE emphasised 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'.[114]

(ii) Critical infrastructure protection as provided by existing national regimes and international cooperation programmes, such as the European Programme for Critical Infrastructure Protection (EPCIP), usually encompasses networks being fundamental to the daily operation of any modern society: water and energy supply, mass transportation, health and emergency services and alike.[115] The last and newest category included in Annex III to the NIS Directive covers 'digital infrastructures' and encompasses (i) IXPs, (ii) DNS service providers and (iii) Top-Level-Domain (TLD) name registries.[116] These categories mirror the current EU approach to cyber resilience, viewing crucial Internet infrastructures as part of the European critical infrastructures ecosystem. Effectively, they all require a high level of protection by their operators, including e. g. security due diligence measures and risk assessments.[117]

---

111 Marsden, Meyer and Brown (n. 108), 9. An example outside of the Internet scope is the UN Security Council Resolution 2462 of 28 March 2019 imposing a duty on the States to comply with the FATF-Guidelines (above chapter IV.2.b) at n. 67).

112 Council of Europe, Internet Governance and Critical Internet Resources Report, Strasbourg 2009.

113 Council of Europe (n. 112), 13-15.

114 Council of Europe (n. 112), 23; see also Kulesza and Weber (n. 1), 6.

115 Kulesza and Weber (n. 1), 8.

116 NIS-Directive (n. 16), Annex II.

117 See also Kulesza and Weber (n. 18), 83-84.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-ZA

VI. Forward-Looking Perspectives

1. Implementation of International Legal Concepts Based on Soft Law

The identification of international legal concepts and relevant soft law norms 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. Furthermore, general principles as well as international legal concepts need to be embedded into the overall normative framework; in this respect, additional elements such as cohesion, convergence, and coherence merit more attention in the future.[118]

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.[119] Implementing norms in a more granular way helps developing a consensus on the inherent value of norms and can lead to a better understanding of their relevance. Global governance also means that the concerned persons are enabled to identify, understand, and address potential transnational problems.[120] Partly, the respective efforts have been introduced but much more needs to be done.

As experience has shown, 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 acknowledged international legal concepts. Indeed, concrete steps are necessary to give them force.[121] The discussed international legal concepts (global public goods, shared spaces, State responsibility) are to be operationalised by incorporating them into global and national policies as well as into transgovernmental regulations.

2. Search of New Paths Leading to Internet Integrity

The governance of the Internet and its integrity is an objective that should eliminate or at least minimise risks caused by an inappropriate use of interna-

118 For more details see Mads Andenas and Ludovica Chiussi, 'Cohesion, Convergence and Coherence of International Law' in: Andenas et al. (n. 54), 9-34.

119 GCSC (n. 6), 23.

120 See Weber (n. 20), 781.

121 GCSC (n. 6), 23-24.

 DOI 10.17104/0044-2348-2021-3-601

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

tional electronic infrastructures. Risk is the function of the likelihood of an adverse event, interacting with the magnitude of harm upon its occurrence.[122] Precautionary measures can also be taken by private actors, for example by way of standardisation, as the network security provisions of ISO/IEC 27001 of 2013 as well as the updated extension ISO/IEC 27701 of 2019 show.[123] In order to achieve a reasonable Internet integrity governance it is necessary to implement a new normative 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.[124]

Previous experience in the field of cybercrime and 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 ongoing interference measures 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 2017/18 when suggesting the adoption of an international treaty to guarantee the peaceful use of cyber space.[125] The proposal to develop a Digital Geneva Convention is referring to the Treaty on the Non-Proliferation of Nuclear Weapons and the Treaty on Chemical Weapons as examples of international regimes that intend to limit vital threats to human existence. However, this proposal met the scepticism of many States and it also seems unclear to what extent other Internet stakeholders could be included in such an arrangement.[126] In addition, the linkage to widely acknowledged international legal concepts appears to be underdeveloped.

The so far (incoherent) patchwork of Internet integrity rules does not really correspond to the political and societal requirements. As the recent developments show, Internet integrity indeed exceeds cybersecurity issues and also encompasses core elements of human rights and of human development.[127] Therefore, the need for a stable normative order is undoubtedly

122 Weber (n. 8), 307.

123 International Standardisation Organisation, ISO/IEC 27001:2013, <https://iso.org/>.

124 Weber (n. 8), 307.

125 Microsoft, Cybersecurity Policy Framework, Geneva 2018, <https://www.microsoft.com/>.

126 Brad Smith, CEO of Microsoft, proposed the name 'A Digital Geneva Convention' in order to underline that cyberspace in a broad scope should be protected (2017), <https://blogs.microsoft.com/>; for further details see Weber (n. 14), nos 65-66.

127 For further details see Kettemann (n. 39), 36 ff.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA

given.[128] The only (partial) exception of normativity concerns the EU with the recently adopted (directly or indirectly applicable) legal cybersecurity regime (NIS-Directive, Cybersecurity Act, Cybersecurity Strategy of December 2020);[129] however, the practical implementation in the EU still needs to become successful. In addition, cyber stability and cyber resilience are only vaguely addressed.

On a global level, further efforts to achieve a better coordinated Internet integrity framework with a broad ambit are required: Amongst others, due diligence standards should be identified based on good business practice, benchmarking, exchange of information, and international cooperation.[130] In addition, the herein discussed commonly developed international legal concepts such as the concept of public goods, of shared spaces, and of State responsibility might be a good way for going forward and for paving a better path to Internet integrity. These concepts could assume a steersman task and thereby realise governance functions. In order to make such approach successful and to avoid disappointments of civil society about the '*Infinite Space*' (Star Trek), academics and businesses are called to contribute innovative ideas to the respective efforts and design possible new frontiers for international law.

128 A respective framework is outlined in Rolf H. Weber, 'Elements of a Legal Framework for Cyberspace', Swiss Review of International and European Law 26 (2016), 195-215 (202 ff.); see also the recent considerations of Kettemann (n. 39), 182 ff. and 233 ff.

129 See also Weber (n. 14), no. 17.

130 Kulesza and Weber (n. 1), 12.

https://doi.org/10.17104/0044-2348-2021-3-601 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY-SA