INTERNATIONAL LAW STUDIES

Published Since 1895

Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies

Dapo Akande, Antonio Coco & Talita de Souza Dias

99 INT'L L. STUD. 4 (2022)

Volume 99

2022

Published by the Stockton Center for International Law

ISSN 2375-2831

Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies

Dapo Akande, Antonio Coco,** & Talita de Souza Dias****

CONTENTS

* Professor of Public International Law & Co-Director, Oxford Institute for Ethics, Law & Armed Conflict, University of Oxford; Fellow, Exeter College, Oxford; Member-elect of the United Nations International Law Commission (2023).

** Lecturer, School of Law, University of Essex; Visiting Fellow, Oxford Institute for Ethics, Law & Armed Conflict, University of Oxford.

*** Shaw Foundation Junior Research Fellow in Law, Jesus College, Oxford; Research Fellow, Oxford Institute for Ethics, Law & Armed Conflict, University of Oxford.

The thoughts and opinions expressed are those of the authors and not necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

I. INTRODUCTION

In the past few years, the applicability of existing international law to cyberspace has received widespread and growing support among States. It has been recognized by individual governments as well as in the 2013[1] and 2015[2] reports by the United Nations (UN) Group of Governmental Experts (GGE) on information and communications technologies (ICTs), both of which were endorsed by the UN General Assembly by consensus.[3] More recently, the Final Substantive Report of the UN open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG), also adopted by consensus among all UN member States, "reaffirmed that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment."[4] A similar statement is found in the latest GGE report, adopted in May 2021.[5]

In particular, there is agreement that "sovereignty and international norms and principles that flow from sovereignty," as well as "[e]xisting obligations under international law" more generally, apply to States' ICT-related activities and their jurisdiction over ICT infrastructure within their territory.[6] Likewise, States have explicitly endorsed the applicability of the UN

1. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter U.N. GGE Report 2013].

2. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶¶ 24, 28(a), U.N. Doc. A/70/174 (July 22, 2015) [hereinafter U.N. GGE Report 2015].

3. G.A. Res. 70/237, ¶¶ 1–2(a) (Dec. 30, 2015).

4. Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 7, U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021) [hereinafter OEWG Final Substantive Report].

5. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, ¶ 69, U.N. Doc. A/76/135 (July 14, 2021) [hereinafter U.N. GGE Report 2021].

6. U.N. GGE Report 2013, *supra* note 1, ¶ 20; U.N. GGE Report 2015, *supra* note 2, ¶ 27; U.N. GGE Report 2021, *supra* note 5, ¶ 71(b).

Charter in its entirety, along with fundamental principles such as dispute settlement by peaceful means and non-intervention.[7] States have also recognized that they must respect and protect human rights and fundamental freedoms and that international humanitarian law applies in armed conflict, including, where applicable, the principles of humanity, necessity, proportionality, and distinction.[8] More generally, they have committed "to meet[ing] their international obligations regarding internationally wrongful acts attributable to them under international law,"[9] as well as to not using proxies to commit such acts.[10]

However, the full extent to which international law applies to ICTs was not spelled out in the 2013, 2015, and 2021 GGE reports, nor in the OEWG Final Substantive Report. This uncertainty has led some States and scholars to question the applicability to "cyberspace" of certain established rules of international law. For instance, the United Kingdom (UK) has opposed the applicability to cyberspace and digital infrastructure of the rule protecting (territorial) sovereignty against certain unauthorized intrusions.[11] Similarly, the applicability of international humanitarian law (IHL) to ICTs has been

7. U.N. GGE Report 2013, *supra* note 1, ¶ 20; U.N. GGE Report 2015, *supra* note 2, ¶¶ 25–28; U.N. GGE Report 2021, *supra* note 5, ¶¶ 70, 71(a), 71(e).

8. U.N. GGE Report 2013, *supra* note 1, ¶ 21; U.N. GGE Report 2015, *supra* note 2, ¶¶ 26, 28(b), 28(d); U.N. GGE Report 2021, *supra* note 5, ¶¶ 70, 71(f).

9. U.N. GGE Report 2013, *supra* note 1, ¶ 23; U.N. GGE Report 2015, *supra* note 2, ¶ 28(f); U.N. GGE Report 2021, *supra* note 5, ¶ 71(g).

10. U.N. GGE Report 2013, *supra* note 1, ¶ 23; U.N. GGE Report 2015, *supra* note 2, ¶ 28(e); U.N. GGE Report 2021, *supra* note 5, ¶ 71(g).

11. U.K. Mission to the United Nations, U.K. Statement on the Application of International Law To States' Conduct In Cyberspace, ¶ 10 (June 3, 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990851/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.pdf; Jeremy Wright, U.K. Attorney General, Speech at the Chatham House Royal Institute for International affairs: Cyber and International Law in the 21st Century (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

questioned by States such as Russia[12] and China,[13] on the grounds that it could further militarize cyberspace. Furthermore, an obligation to exercise due diligence in not allowing ICTs within a State's territory or subject to its jurisdiction to be used for acts contrary to the rights of other States has been explicitly rejected by Argentina,[14] Israel,[15] and the UK,[16] and seriously questioned by New Zealand.[17] To compound such uncertainty, a majority of States have not yet expressed their views about the application of international law in cyberspace.

Arguments that deny the applicability of certain rules or principles of international law to cyberspace usually rest on two assumptions.

First, it is often said that cyberspace is a new and inherently different "space," "field," or "domain" of State activity. On this view, the "cyber domain" requires specifically tailored rules or principles of international law

12. Russian Federation, Commentary on the Initial "Pre-Draft" of the Final Report of the United Nations Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security 2 (May 22, 2020, https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf.

13. Yao Shaojun, Minister-Counsellor for the People's Republic of China, Statement at U.N. Security Council Arria Formula Meeting on Cyber Attacks Against Critical Infrastructure (Aug. 26, 2020), https://www.fmprc.gov.cn/ce/ceun/eng/hyyfy/t1809700.htm; Wu Jianjian, Counsellor for the People's Republic of China, Statement at U.N. Security Council Arria Formula Meeting on Cyber Stability, Conflict Prevention and Capacity Building (May 22, 2020), https://vm.ee/en/activities-objectives/estonia-united-nations/signature-event-estonias-unsc-presidency-cyber (comments at timestamp 1:21:00).

14. Argentina, Intervención de la República Argentina 2° Reunión sustantiva GTCA sobre los progresos de la informática y las telecomunicaciones en el contexto de la seguridad internacional (Feb. 11, 2020), https://media.un.org/en/asset/k18/k18w6jq6eg (comments at timestamp 2:15:00).

15. Roy Schondorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, EJIL:TALK! (Dec. 9, 2020), https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

16. U.K. Statement, *supra* note 11, ¶ 12.

17. New Zealand Ministry for Foreign Affairs and Trade, The Application of International Law to State Activity in Cyberspace, ¶¶ 16–17 (Dec. 1, 2020) (on file with authors). *See also* Michael Schmitt, *New Zealand Pushes the Dialogue on International Cyber Law Forward*, JUST SECURITY (Dec. 8, 2020), https://www.justsecurity.org/73742/new-zealand-pushes-the-dialogue-on-international-cyber-law-forward/.

and possibly a new binding legal instrument.[18] On this view, existing international law could only apply *in* cyberspace if substantiated by sufficient evidence of domain-specific State practice and *opinio juris*.[19] The search for cyber-specific practice and *opinio juris* is usually backed by calls for more national statements on how international law applies to cyber operations. A more nuanced and sophisticated version of this argument is to be found in the statement by Israel's Deputy Attorney General on the application of international law to cyber operations, where he stated that:

> It cannot be automatically presumed that a customary rule applicable in any of the physical domains is also applicable to the cyber domain. The key question in identifying State practice is whether the practice which arose in other domains is closely related to the activity envisaged in the cyber domain. Additionally, it must be ascertained that the *opinio juris* which gave rise to the customary rules applicable in other domains was not domain-specific. Given the unique characteristics of the cyber domain, such an analysis is to be made with particular prudence, as it is very often the case that relevant differences exist.[20]

Secondly, the fact that certain standards of conduct have been framed, in the 2015 UN GGE Report, as "voluntary, non-binding, norms of responsible state behaviour in cyberspace," is taken to mean that the behavior in question is not required by international law. For instance, this has been the case with the concept of due diligence, which seems to be reflected in the UN GGE reports in hortatory terms: "States *should* not knowingly allow their territory to be used for internationally wrongful acts using ICTs" or "*should* seek to ensure that their territory is not used by non-State actors to commit such acts."[21] For some, the implication of labeling a standard of conduct as a "voluntary, non-binding, norm," or framing it as something that States "should" endeavor to achieve, is that the corresponding rules or principles

18. *See* Conference Room Paper of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Chair's Summary, ¶ 16, U.N. Doc. A/AC.290/2021/CRP.3* (Mar. 10, 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf (calling for such a new instrument).

19. *See, e.g.,* U.K. Statement, *supra* note 11, ¶¶ 10, 12.

20. Schondorf, *supra* note 15.

21. U.N. GGE Report 2013, *supra* note 1, ¶ 23; U.N. GGE Report 2015, *supra* note 2, ¶ 13(c).

have not yet developed or crystallized for cyberspace, or that this domain has been carved out from the scope of said obligations.[22]

Again, a good example of this line of thinking comes from the statement of Israel's Deputy Attorney General:

> There was wisdom in mentioning [due diligence] in the chapter covering norms of responsible State behavior, as it does not, at this point in time, translate into a binding rule of international law in the cyber context. . . .
>
> The inherent different features of cyberspace—its decentralization and private characteristics—incentivize cooperation between States on a voluntary basis, such as with the case of national Computer Emergency Response Teams (CERTs). . . . However, we have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching *opinio juris*, which would be indispensable for a customary rule of due diligence, or something similar to that, to form.[23]

In this article, we challenge those assumptions and conclude that all relevant existing rules of international law are *by default* applicable to the conduct of States with respect to ICTs. Such conclusion is based on five arguments, which will be developed in turn.

Part 2 starts by warning that the terminology of "domains" for the application of international law may be misguided. In fact, international law is *not* as a general matter domain-specific, and thus its applicability to a specific domain (traditionally, land, sea, air, and outer space) need not be specifically proven. Quite the contrary: any limitation imposed on the scope of general international law, whether framed around a subject matter, context, area, type of activity, or domain, cannot be assumed but must be drawn from specific evidence.

Next, Part 3 delves into the notion of "domain" and its development in the context of IHL. We demonstrate that, in this and other areas, the concept was never meant to function as a tool to carve out certain types of activity from existing rules or principles of international law. This in turn means that rules of international law, whether conventional or customary, which evince a general scope of application, can be interpreted and applied to new domains.

---

22. *See, e.g.,* U.K. Statement, *supra* note 11, ¶ 12.
23. Schondorf, *supra* note 15.

Part 4 then considers that, in any event, cyberspace is not per se a "space" or a singular domain, at least not in the sense that air, sea, or outer space are. Instead, it may be defined as an interactive medium—comprised of digital networks and technologies spread across national borders and made up of physical, logical, and personal elements—which is used to communicate, store, or modify information.

In this light, Part 5 explains that international law is technology-neutral in the sense that it applies to all technologies through which States and non-State actors operate, whether these are old or new, analog or digital, physical or virtual.

Lastly, Part 6 contends that the fact that a certain behavior has been the subject of a policy recommendation—like the so-called "voluntary norms of responsible state behavior in cyberspace"—by no means implies that the same behavior is not required as a matter of international law. Quite the opposite: political statements cannot deprive international obligations of their binding force but may be seen as reinforcing and complementing them.

The article concludes by acknowledging that international law can be rewritten, including for States' use of ICTs. However, any law-making effort in this respect is not built on a legal vacuum but on a wealth of existing rules which already apply to those technologies.

II. THE "GENERALITY" OF GENERAL INTERNATIONAL LAW

That *general* international law is, by definition, general is self-evident. But that does not tell us much about its extent or scope of application, that is, who is bound by general international law and to what matters it applies. For this reason, it is important to understand the different ways in which international law can be said to "apply generally," and, in particular, the extent to which this generality includes different subject matters, contexts, areas, or types of activity, including the use of ICTs.

First and foremost, "general international law" refers to international rules and principles that bind all States as a matter of customary international law, general principles of law, or universally ratified treaties.[24] Examples include the principles of sovereign equality of States and non-intervention, as

24. *See* Josef L. Kunz, *General International Law and the Law of International Organizations*, 47 AMERICAN JOURNAL OF INTERNATIONAL LAW 456, 456–457 (1953); Anastasios Gourgourinis, *General/Particular International Law and Primary/Secondary Rules: Unitary Terminology of a Fragmented System*, 22 EUROPEAN JOURNAL OF INTERNATIONAL LAW 993, 1004–7 (2011);

well as the UN Charter and its prohibition on the use of force, binding under conventional and customary international law.[25] Among those rules and principles generally applicable to all States, some deal with more specific matters than others. For instance, the four 1949 Geneva Conventions have been universally ratified and crystallized into customary international law, thereby applying to all States.[26] Yet their subject matter is limited to regulating the conduct of hostilities during armed conflict, that is, to the so-called "field" of IHL.[27] Likewise, the principle of non-intervention in the internal affairs of other States only covers coercive interference within another State's *domaine reservé*, that is, public or private matters over which the State possesses exclusive authority to regulate.[28] In fact, apart from a handful of very general and foundational principles of international law from which States' obligations seem to flow, such as sovereignty and *pacta sunt servanda*, international rules and principles tend to have a more or less defined subject matter.

In some instances, treaty texts or State practice and/or *opinio juris* indicate explicitly or implicitly that the application of an international rule or principle is limited to a particular context, area, or specific type of activity. For instance, this is the case with the centuries-old obligation of States to respect freedom of navigation in the high seas, where the practice and *opinio juris*

International Law Commission, Report of the Study Group on Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, ¶ 493, U.N. Doc. A/CN.4/L.682 (Apr. 13, 2006).

25. U.N. Charter art. 2(4).

26. *See* Theodor Meron, *The Geneva Conventions as Customary Law*, 81 AMERICAN JOURNAL OF INTERNATIONAL LAW 348 (1987).

27. See common article 2 of the Geneva Conventions of 1949.

28. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 202 (June 27); G.A. Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, princ. (c) (Oct. 24, 1970). *See also* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, cmt. to r. 4, ¶ 22 (Michael N. Schmitt gen. ed., 2017). *But see* Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* ¶¶ 105–107, CHATHAM HOUSE RESEARCH PAPER (Dec. 2, 2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/3-application-non-intervention-principle (advancing a broader scope for the principle).

clearly evince that the rule is restricted to the *high* seas.[29] The rule does not guarantee freedom of navigation throughout the seas, nor does it oblige States to guarantee freedom of movement in other maritime zones, such as States' territorial waters or their exclusive economic zones.[30] Similarly, the obligation to carry out an environmental impact assessment, although binding under customary international law, only applies to those activities that may cause physical harm to the natural environment.[31]

Nevertheless, in the absence of a limitation to a particular subject-matter, context, area, or type of activity, or where the existing expression of a rule is general (whether its text, or formative *opinio juris* and State practice), there is nothing in international law that suggests that one must seek to ascertain whether a rule applies across domains, as many have sought to characterize cyberspace or ICTs. For example, it is prohibited for States to arrest the serving head of another State. It matters not where or how the arrest takes place. To take another example, in the course of an armed conflict, it is prohibited for States to direct attacks against civilians. Again, it matters not where the civilians (or the attackers) are or what weapons are used. The same is true of the law relating to the use of force. It is prohibited to use force against another State and no inquiry needs be made about the domain in which a State using force is acting. These, and many other examples, show that we should be skeptical about a supposition that the application of international law rules is domain-specific.

The bottom line is that to ascertain the scope of application of general international law, each rule or principle must be assessed on its own terms. Thus, whether a limitation is based or framed around a subject matter, a

---

29. *See* United Nations Convention on the Law of the Sea art. 87, Dec. 10, 1982, 1833 U.N.T.S. 397; HUGO GROTIUS, THE FREEDOM OF THE SEAS; OR, THE RIGHT WHICH BELONGS TO THE DUTCH TO TAKE PART IN THE EAST INDIAN TRADE 28 (Ralph Van Deman Magoffin trans., Oxford Univ. Press 1916) (1609); Albert J. Hoffmann, *Freedom of Navigation*, MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶¶ 1–6 (last updated Apr. 2011), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1199; Douglas Guilfoyle, *The High Seas*, *in* THE OXFORD HANDBOOK OF THE LAW OF THE SEA 204, 207 (Donald Rothwell et al. eds., 2015).

30. Hoffmann, *supra* note 29, ¶ 6.

31. *See* Case Concerning Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, ¶ 204 (Apr. 20); Certain Activities Carried out by Nicaragua in the Border Area (Costa Rica v. Nicar.) and Construction of a Road in Costa Rica along the San Juan River (Nicar. v. Costa Rica), Judgment, 2015 I.C.J. 665, ¶ 104 (Dec. 16); Astrid Epiney, *Environmental Impact Assessment*, MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶¶ 1–4 (last updated Jan. 2009), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1581.

context, an area, a type of activity, a domain, or any other category we might conceive of, it must be somehow indicated in the rule or principle in question. Importantly, to undertake this assessment, traditional methods of *interpretation* of treaties or customary international law must be resorted to. These methods tell us that where a rule is *not* limited to a certain area, context, type of activity, or domain, such limitations cannot be read into its scope of application.

III. THE MEANING AND FUNCTION OF A "DOMAIN" IN INTERNATIONAL LAW

It is often assumed that, unlike the physical domains of air, land, sea, and outer space, cyberspace is an inherently different, *virtual* domain, where activities may take place without meaningful physical manifestations. But while belonging to one domain or another is thought to be decisive as to the applicability of international law to a certain activity, the actual meaning and function of the concept have been largely overlooked.

In common parlance, "domain" has a variety of meanings in different contexts. More traditionally, the word has been associated with "a territory over which dominion is exercised" or a "region distinctively marked by some physical feature."[32] However, a domain may also refer to a "sphere of knowledge, influence, or activity,"[33] "a particular interest, activity, or type of knowledge"[34] or "an area of interest or an area over which a person has control."[35] Indeed, the so-called "domains of public international law" seem to refer to the different branches of this legal system and their corresponding academic fields.[36] And these might cover one, more, or all physical spaces, depending on the rule or set of rules in question. For example, international environmental law, a field of international law and academic study, applies to land, sea, and airspace.

The idea that international law applies to or corresponds to different domains, whether these are areas of knowledge or physical spaces, seems to be

32. *Domain*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/domain (last visited Jan. 6, 2022).

33. *Id.*

34. *Domain*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/dictionary/english/domain (last visited Jan. 6, 2022).

35. *Id.*

36. *International Law*, LEGAL INFORMATION INSTITUTE, CORNELL LAW SCHOOL, https://www.law.cornell.edu/wex/international_law (last visited Jan. 6, 2022).

derived from the context of armed conflict. There, the concept "serves as a fundamental organizing idea, reflecting the way we conceptualize the battlefield and categorize actions taking place during armed conflict."[37] Importantly, even in this context, categorizing a certain activity as falling within this or that domain, such as land, sea, air, or other types of battlefield or warfare, does not exclude or carve out activity in the given domain from the scope of application of generally applicable rules of IHL. To be sure, some rules of IHL are specifically designed for application to particular areas, for example, the First Geneva Convention of 1949 applies to wounded and sick in armies on land, while the Second Geneva Convention of 1949 applies to the wounded, sick, and shipwrecked at sea. However, "much of IHL is not domain-specific and applies generally."[38] This means that many rules of IHL apply regardless of whether the act in question takes place on land, the sea, in the air, or any other space for that matter, and irrespective of other specific features of the battlefield or act of warfare. This is true of much of the rules regarding the protection of civilians and the regulation of means and methods of warfare to be found in the Additional Protocols to the Geneva Conventions and in customary international law.

In sum, the application of rules of international law will sometimes depend on the physical space in which the relevant activity takes place. However, it should not be assumed that a rule first developed in the context of a particular physical space or domain only applies there, especially when there is nothing implicit or explicit in the rule or principle in question to suggest this. Instead, each rule of international law, general or specific, must be interpreted on its own terms and applied to all persons, objects, or events that fall within its scope.

Indeed, legal interpretation is the most intuitive way to ascertain the scope of a certain rule or principle of conventional or customary international law and any potential limitation thereto. That treaties must be inter-

37. Sarah McCosker, *Domains of Warfare, in* OXFORD GUIDE TO INTERNATIONAL HUMANITARIAN LAW 77, 97 (Ben Saul & Dapo Akande eds., 2020).

38. *Id.* at 78.

preted in accordance with their text, context, and object and purpose is beyond doubt.[39] But much controversy surrounds the interpretability of unwritten rules of international law, including custom and general principles.[40] In what follows, we explain why, in the absence of specific limitations, both written and unwritten rules of international law *of general scope* are susceptible to identification and/or interpretation, as well application, in the cyber context, that is, to ICTs.[41] In particular, we tackle the controversial question of whether it is necessary to prove specific State practice and *opinio juris* for existing rules of international law to apply in cyberspace.

While the interpretability of customary international law is beyond the scope of this article, it suffices to note that, no matter how international lawyers frame the process or methodology for ascertaining the existence, content, and scope of customary international law, there is always room for interpretation in every step of the way.[42] This is because interpretation, understood here as the process of assigning meaning to subjects, objects, or events, is inherent to human cognition. Simply put, it is by assimilating specific things to abstract concepts that we understand and communicate about the world around us.[43] And in this process of "framing," there is inevitably room for over or under-inclusion, at the very least when it comes to human, non-deterministic concepts or ideas such as law.[44] Of course, questions remain as to whether it is even possible to separate the stages of ascertainment of State

39. Vienna Convention on the Law of Treaties arts. 31–33, May 23, 1969, 1155 U.N.T.S. 331 [hereinafter VCLT].

40. International Law Association, Preliminary Report of the Study Group on the Content and Evolution of the Rules of Interpretation (Aug. 11, 2016), https://ila.vettoreweb.com/Storage/Download.aspx?DbStorageId=1401&StorageFileGuid=bcaa951e-ae3e-4ccb-9c80-248c98c741e3 [hereinafter ILA Study on Interpretation]. *See also* ROBERT KOLB, INTERPRÉTATION ET CRÉATION DU DROIT INTERNATIONAL: ESQUISSES D'UNE HERMÉNEUTIQUE JURIDIQUE MODERNE POUR LE DROIT INTERNATIONAL PUBLIC 219–22 (2006); Panos Merkouris, Interpreting the Customary Rules on Interpretation, University of Groningen Faculty of Law Research Paper (last revised July 18, 2017), https://papers.ssrn.com/abstract=2749066; Duncan B. Hollis, Sources and Interpretation Theories: An Interdependent Relationship, Temple University Legal Studies Research Paper (last revised Oct. 8, 2016), https://papers.ssrn.com/abstract=2836691.

41. Orfeas Chasapis Tassinis, *Customary International Law: Interpretation from Beginning to End*, 31 EUROPEAN JOURNAL OF INTERNATIONAL LAW 235, 236 (2020).

42. *See, e.g., id.* at 237, 241.

43. *Id.* at 242–43.

44. *See id.* at 244; Matthias Herdegen, *Interpretation in International Law*, MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 1 (last updated Nov. 2020), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e723.

practice and *opinio juris*, and the interpretation of an identified rule of custom.[45] As others have noted, even the exercises of selecting, describing, and evaluating State practice and *opinio juris* are pervaded by subjectivity and are thus subject to different interpretations.[46] Either way, it is sensible to assume that custom or its separate elements are interpretable,[47] that is, that the original, abstract "frame" can always be extended to cover new and more specific phenomena, like those that implicate digital technologies. For instance, it could be argued that the rule according to which States must exercise due diligence and not knowingly allow their territory to be used for acts contrary to the rights of other States, spelled out by the International Court of Justice (ICJ) in the *Corfu Channel* case,[48] is sufficiently general to find application, by way of interpretation, in the use of ICTs.[49]

An alternative way to frame and conceptualize the application of general rules of customary international law to new types of scenarios is the identification of new customary rules that are specifically tailored to the situation, context, or domain at hand. This is, according to some scholars,[50] what the ICJ did with the more general due diligence principle and Albania's specific

45. *See* Tassinis, *supra* note 41, at 246; Hollis, *supra* note 40, at 2, 4–6, 8; Duncan B. Hollis, *The Existential Function of Interpretation in International Law*, *in* INTERPRETATION IN INTERNATIONAL LAW 80 (Andrea Bianchi et al. eds., 2015); Jean D'Aspremont, *The Multidimensional Process of Interpretation*, *in* INTERPRETATION IN INTERNATIONAL LAW 112, 117–18 (Andrea Bianchi et al. eds., 2015).

46. Tassinis, *supra* note 41, at 257; Frederick Schauer, *Pitfalls in the Interpretation of Customary International Law*, *in* THE NATURE OF CUSTOMARY LAW: LEGAL, HISTORICAL AND PHILOSOPHICAL PERSPECTIVES 13, 21 (Amanda Perreau-Saussine & James B. Murphy eds., 2007); Nadia Banteka, *A Theory of Constructive Interpretation for Customary International Law Identification*, 39 MICHIGAN JOURNAL OF INTERNATIONAL LAW 301, 316 (2018).

47. *See* North Sea Continental Shelf (F.R.G. v. Den., F.R.G. v. Neth.), Judgment, 1969 I.C.J. 3, 181 (Feb. 20) (Tanaka, J., dissenting); Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 178 (June 27); Report of the Panel Appointed by the Director-General of the World Trade Organization to Investigate Complaints of the United States, Canada, and Argentina: European Communities—Measures Affecting the Approval and Marketing of Biotech Products, ¶¶ 7.68–7.72, (Nov. 21, 2006), https://www.wto.org/english//tratop_e/dispu_e/291r_3_e.pdf (located at pages 333–335 of the report).

48. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 839 (Apr. 9).

49. *See* Antonio Coco & Talita de Souza Dias, *"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law*, 32 EUROPEAN JOURNAL OF INTERNATIONAL LAW 771, 778–83 (2021).

50. *See*, *e.g.*, Stefan Talmon, *Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion*, 26 EUROPEAN JOURNAL OF INTERNATIONAL LAW 417, 424 (2015); Banteka, *supra* note 46, at 303, 311–12.

duty to notify British vessels about mines in the Corfu Channel.[51] This approach seems to have been followed by some States and scholars in relation to a rule of due diligence in cyberspace: it is often assumed that a new and cyber-specific rule of due diligence must be specifically identified and applied to ICTs.[52]

However, and crucially, even if one frames the applicability of international law to new domains as custom-identification or ascertainment, there is usually no need to collate specific instances of State practice and *opinio juris* from scratch by induction. This is because whenever a more general rule or principle of international law already exists whose scope would already cover a new situation, it is possible to deduce one or more specific rules from the more general one.[53] As Orfeas Chasapis Tassinis notes, this can be explained by the nature of customary international law as "an organic body of legal rules that gradually branches out as opposed to an assemblage of self-standing rules."[54] Granted, it may not be that every rule of custom is *directly* rooted in a pre-existing one. This may be the case of certain rules of procedure, such as the requirement that instruments of ratification of treaties be exchanged or deposited with or notified to the other party(ies).[55]

Nevertheless, all rules of custom are ultimately grounded or at least informed by foundational international legal principles, such as sovereignty,

---

51. Corfu Channel, 1949 I.C.J. at 22.

52. *See, e.g.,* Eric Talbot Jensen & Sean Watts, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?*, 95 TEXAS LAW REVIEW 1555, 1573–74 (2017); TALLINN MANUAL 2.0, *supra* note 28, at 45 (referring to the views expressed by some scholars among the Manual's international group of experts); Luke Chircop, *A Due Diligence Standard of Attribution in Cyberspace*, 67 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 643, 660, 662 (2018). *See also* Michael Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE LAW JOURNAL FORUM 68, 73 (2015); Duncan B. Hollis, Improving Transparency—International Law and State Cyber Operations: Fourth Report to the Organization of American States, OEA/Ser.Q CJI/doc. 615/20 rev.1, ¶ 7 (Aug. 7, 2020), http://www.oas.org/en/sla/iajc/docs/themes_recently_concluded_International_law_State_cyber_operations_FINAL_REPORT.pdf (referring generally to the need for evidence of State practice and *opinio juris* to assess the applicability of international law in cyberspace) [hereinafter Improving Transparency].

53. Talmon, *supra* note 50, at 421–23. *See also* Anthea Elizabeth Roberts, *Traditional and Modern Approaches to Customary International Law: A Reconciliation*, 95 AMERICAN JOURNAL OF INTERNATIONAL LAW 757, 758–59 (2001); Dapo Akande, *The Jurisdiction of the International Criminal Court over Nationals of Non-Parties: Legal Basis and Limits*, 1 JOURNAL OF INTERNATIONAL CRIMINAL JUSTICE 618, 626 (2003).

54. Tassinis, *supra* note 41, at 262.

55. VCLT, *supra* note 39, art. 11.

consent, and good faith.[56] Although deduction from general rules or principles alone may not always suffice to prove the existence of a more specific rule of custom, it does raise a strong presumption that such a rule does exist, in turn lowering the threshold of State practice and *opinio juris* that would be necessary to prove its existence.[57] According to Stefan Talmon, in those instances, the outcome of the deductive process is simply *confirmed* by induction from a sufficient amount of State practice and *opinio juris*.[58] If this reasoning were to be followed in our earlier example, one would conclude that the general due diligence rule has a more specific counterpart applying *mutatis mutandis* to the use of ICTs, as confirmed by relevant State practice and expressions of *opinio juris*.

In practice, there is little difference between this process of custom-identification and the interpretation and application of general customary rules to new phenomena. Admittedly, it remains unclear what canons of interpretation should be applied to customary international law, whether reflected in textual form or drawn from a set of behaviors.[59] But any type of legal interpretation, whether in domestic or international law, can only be informed by a handful of legal reasoning techniques. As made explicit in the context of treaty interpretation, these include the ordinary meaning of the words by which a rule is expressed, its context, its function or objective, and its history (textual, systematic, teleological, and historical methods of interpretation, respectively).[60] Other methods of interpretation that also apply to written and unwritten legal rules include analogy, *a contrario*, *in dubio mitis*, and other techniques of logical reasoning.[61]

That customary international law can be interpreted by these and other techniques has long been acknowledged before human rights bodies and international criminal courts.[62] These have sought to clarify the extent to which

---

56. *See* Banteka, *supra* note 46, at 316.

57. Talmon, *supra* note 50, at 427.

58. *Id.*

59. ILA Study on Interpretation, *supra* note 40, at 9.

60. VCLT, *supra* note 39, arts. 31, 32. *See also* ODILE AMMANN, DOMESTIC COURTS AND THE INTERPRETATION OF INTERNATIONAL LAW METHODS AND REASONING BASED ON THE SWISS EXAMPLE, ch. 6 (2019).

61. Mark E. Villiger, *The Rules on Interpretation: Misgivings, Misunderstandings, Miscarriage? The "Crucible" Intended by the International Law Commission*, *in* THE LAW OF TREATIES BEYOND THE VIENNA CONVENTION 115, 112 (Enzo Cannizzaro ed., 2011).

62. *See, e.g.*, Prosecutor v. Vasiljević, Case No. IT-98-32-T, Judgment, ¶¶ 193, 196, 201–2 (Int'l Crim. Trib. for the former Yugoslavia Nov. 29, 2002); Vasiliauskas v. Lithuania*,* App. No. 35343/05, Judgment, ¶¶ 171–86 (2015) (ECtHR).

more general customary prescriptions or prohibitions apply to specific factual scenarios, often unforeseen at the time the rule was conceived, by using different interpretative techniques.[63] Notably, in various international courts and tribunals, as well as diplomatic settings, a key technique to interpret treaty and customary rules—and trace their evolution over time—is to look at the subsequent practice of States, which implicitly or explicitly establishes their agreement.[64] This technique can be used to guide the interpretation of rules of international law in their application to ICTs, looking at whether States have considered themselves to be bound by those rules in cyberspace and other so-called domains.

In short, rules of general international law are not domain-specific, at least not by default. Instead, the starting point is that they apply across the board to different matters, contexts, areas, activities, and domains, unless, and in so far as, their scope is implicitly or explicitly limited to one or more of these categories. Furthermore, rules or principles that lack such limitations and thereby are of general applicability can be interpreted and applied to cover cyberspace.

IV. IS CYBERSPACE A NEW DOMAIN?

In any event, there are good reasons to challenge the idea that cyberspace is a new domain requiring domain-specific State practice and *opinio juris*.

Understanding what cyberspace is requires us to briefly go back to the origin of the term, its purpose, and the background against which it was originally employed in legal discourse, before turning to its technical features. As others have noted, the prefix "cyber" comes from the Greek word *kybernetes*, which means one who steers or governs, and alludes to the field of

63. *See, e.g.*, Prosecutor v. Hadzihasanović et al., Case No. IT-01-47-PT, Interlocutory Appeal on Decision on Joint Challenge to Jurisdiction, ¶ 142–78 (Int'l Crim. Trib. for the former Yugoslavia Nov. 27, 2002) (finding that the doctrine of command responsibility under customary international law could be interpreted to apply to both international and non-international armed conflict, based on the text of relevant legal instruments, their context, and object and purpose).

64. On subsequent practice and customary international law interpretation, see, e.g., North Sea Continental Shelf Case (F.R.G. v. Den., F.R.G. v. Neth.), Judgment, ¶¶ 44–56, 1969 I.C.J. 3 (Feb. 20); Vasiliauskas v. Lithuania, App. No. 35343/05, Judgment, ¶¶ 176–77 (2015) (ECtHR). On the role of subsequent practice in the context of treaty interpretation, see VCLT, *supra* note 39, art. 31(3)(c); International Law Commission, Report on the Work of the Sixty-Eighth Session, ch. 6, U.N. Doc. A/71/10 (2016) ("Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties").

"cybernetics"—defined as the study of remote control through devices[65] or "command and control and communications in the animal . . . or the mechanical world."[66] In contrast, the word "space" not only has physical or geographical meanings but also philosophical, mathematical, social, and psychological ones.[67] Quite telling but generally overlooked in the literature is the first use of the term in the 1960s to designate the so-called "Atelier Cyberspace," an artistic partnership forged between architect Carsten Hoff and artist Susanne Ussing.[68] Their work comprised a series of visual arts exhibitions containing sensory installations and images that depicted "open systems," that is, architectural spaces adaptable to various influences, such as human movement and new material. According to Hoff: "To us, 'cyberspace' was simply about managing spaces. There was nothing esoteric about it. Nothing digital, either. It was just a tool. The space was concrete, physical."[69]

It was only in the 1980s that the term started to be associated with computers and digital networks, following the publication of two works of science fiction by William Gibson,[70] who confessed that "the word 'cyberspace' . . . seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning . . . ."[71]

Gibson's buzzword was subsequently taken up, quite effectively, in the early days of the Internet by American political activists, such as John Perry Barlow, and legal theorists, among whom were David Johnson and David Post. As Julie Cohen notes, this is when the idea of cyberspace *as a space* started to take shape. Back then, labeling the Internet and other networks as *another* space, different from the "real world," was an attempt to treat it as a

65. LAURENCE LESSIG, CODE: VERSION 2.0, at 3 (2006).

66. Lior Tabanski, *Basic Concepts in Cyber Warfare*, 3 MILITARY AND STRATEGIC AFFAIRS 75, 76 (2011) (citing NORBERT WIENER, CYBERNETICS OR CONTROL AND COMMUNICATION IN THE ANIMAL AND THE MACHINE (1955)).

67. *Id.* at 76.

68. Jacob Lillemose & Mathias Kryger, *The (Re)invention of Cyberspace*, KUNSTKRITIKK (Aug. 24, 2015), http://www.kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/.

69. *Id.*

70. WILLIAM GIBSON, BURNING CHROME (1982); WILLIAM GIBSON, NEUROMANCER (1984).

71. NO MAPS FOR THESE TERRITORIES (Docurama 2000) (documentary film featuring William Gibson).

separate jurisdiction to which State power, laws, and regulations did not apply.[72]

Yet, even in American legal discourse, where the debate about Internet governance and regulation was most fervent, the idea of an ungovernable or uncontrollable cyberspace was soon debunked. As early as 1996, in his controversial conference address, Frank Easterbrook immortalized the analogy according to which the law of cyberspace was as real as the "law of the horse."[73] For him, there was neither need nor wisdom to conceive of new rules for the Internet and other digital networks, as general rules continued to apply.[74] And in his comprehensive work on "code as law," Lawrence Lessig notes that, as a human and thus political project,[75] cyberspace "will be regulated by real space regulation to the extent that it affects real space life, and it will quite dramatically affect real space life."[76]

In short, cyberspace is nothing but a metaphor to express simulated spaces or experiences, such as online gaming, dating, or social media; or the virtual prolongation or manifestation of real spaces, such as shops, public murals, government institutions, or mailboxes, where the Internet and other networks serve as tools for the performance of regular, "real world" activities.[77] It is no more real than the worlds or places (re)created by books and films, or conversations over traditional means of communication, such as letters or telephone calls. In the same vein, just as global transportation networks do not give rise to a new "world" or "domain," so does cyberspace not constitute a new "space."

This view is corroborated by the more technical definition of the Internet and other networks that are considered to be part of cyberspace. These are constituted by a range of digital technologies which enable us to communicate and process different types of data or information. And these technologies, such as computer applications, network links, and digital devices, are themselves made up of complex layers of software, hardware, and the

---

72. Julie E. Cohen, *Cyberspace As/And Space*, 107 COLUMBIA LAW REVIEW 210, 216 (2007).

73. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 UNIVERSITY OF CHICAGO LEGAL FORUM 207, 208 (1996).

74. *Id.* at 210.

75. LESSIG, CODE 2.0, *supra* note 65, at 85–88.

76. Laurence Lessig, *The Zones of Cyberspace*, 48 STANFORD LAW REVIEW 1403, 1406 (1996). *See also* Cohen, *supra* note 72, at 217–18.

77. LESSIG, CODE 2.0, *supra* note 65, at 9, 83.

data they process.[78] But as much as software and data—the "virtual" or "logic" layers of cyberspace—play a significant role in allowing one to control how these technologies operate, the input, processing, and output of data through code depend on a physical substrate, just like human intelligence and reasoning depends on the human body and brain. Thus, hardware components such as cables, satellites, radio waves, computers, and millions of silicon circuits, all located somewhere in the "real world," are part and parcel of ICTs or cyberspace. Even if advancements in computer power and programming languages have greatly improved connectivity and speed across national boundaries and enhanced our perception of imaginary spaces such as the World Wide Web, the Cloud,[79] or the Metaverse,[80] these remain very much grounded in tangible physical infrastructure somewhere in the world.

However, it would also be too simplistic to stop there and reduce cyberspace, or ICTs, to their physical and logical layers. This is because perhaps the most important dimension or layer of what we call cyberspace consists of the human beings and social structures that create, control, and use ICTs, including their software, hardware, and data. In this sense, cyberspace—or, more accurately, a multitude of cyberspace*s*, whether perceived differently or similarly to other spaces and technologies—is very much a human and social experience with real-world impact.[81]

To give but one example, let us take the SolarWinds hack of late 2020. This was a malicious cyber operation against a globally supplied network monitoring software that was carried out by inserting malicious code in the software's update system, enabling the hackers to breach the confidentiality

78. On the various layers of cyberspace, see Clare Sullivan, *The 2014 Sony Hack and the Role of International Law*, 8 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 437, 454 n.88 (2015).

79. *The World Wide Web: A Global Information Space*, THE SCIENCE MUSEUM (Nov. 14, 2018), https://www.sciencemuseum.org.uk/objects-and-stories/world-wide-web-global-information-space.

80. *Metaverse,* WIKIPEDIA, https://en.wikipedia.org/wiki/Metaverse (last visited Feb. 1, 2022).

81. LESSIG, CODE 2.0, *supra* note 65, at 84–85. *See also* U.N. GGE Report 2021, *supra* note 5, ¶ 9 (finding that malicious use of ICT-enable covert information campaigns "pose direct and indirect harm to individuals"); OEWG Final Substantive Report, *supra* note 4, ¶¶ 4, 19 (noting the need to maintain a "human-centric approach" to ICTs and that unlawful ICT activity "could pose a threat not only to security but also to State sovereignty, as well as economic development and livelihoods, and ultimately the safety and wellbeing of individuals").

of public and private data.[82] Even assuming that the hack was limited to a "mere" digital data breach,[83] it led to concrete financial losses and reputational damage to companies, government agencies, and individuals around the world.[84] This cyber operation also allegedly gave the perpetrators remote control over certain critical infrastructure systems, at least in the United States, such as power stations and distribution grids, posing a very real risk of serious damage to critical public services, such as hospitals and schools.[85]

Thus, the term "cyberspace," with its chiefly virtual connotation, may be somewhat misleading, as it fails to capture the physical, human, and social dimensions of ICTs. The term has also been used to purposefully sever these more tangible dimensions from the software and data layers, and in doing

---

82. *See, e.g.*, Kate O'Flaherty, *SolarWinds: Microsoft Reveals New Details About Sophisticated Mega-Breach*, FORBES (Feb. 16, 2021, 6:54 AM), https://www.forbes.com/sites/kateoflahertyuk/2021/02/16/solarwinds-microsoft-reveals-new-details-about-sophisticated-mega-breach/; Kari Paul, *SolarWinds Hack was Work of "at least 1,000 engineers", Tech Executives Tell Senate*, THE GUARDIAN (Feb. 23, 2021, 7:39 PM), https://www.theguardian.com/technology/2021/feb/23/solarwinds-hack-senate-hearing-microsoft; Christopher Bing, *Suspected Russian Hackers Spied on U.S. Treasury Emails—Sources*, REUTERS (Dec. 13, 2020, 1:56 PM), https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0PG?edition-redirect=uk.

83. Jack Goldsmith, *Quick Thoughts on the Russian Hack*, LAWFARE (Dec. 14, 2020, 11:04 AM), https://www.lawfareblog.com/quick-thoughts-russia-hack; Kristen Eichensehr, *"Strategic Silence" and State-Sponsored Hacking: The US Gov't and SolarWinds,* JUST SECURITY (Dec. 18, 2020), https://www.justsecurity.org/73921/strategic-silence-and-state-sponsored-hacking-the-us-govt-and-solarwinds/; Asaf Lubin, *SolarWinds as a Constitutive Moment: A New Agenda for the International Law of Intelligence*, JUST SECURITY (Dec. 23, 2020), https://www.justsecurity.org/73989/solarwinds-as-a-constitutive-moment-a-new-agenda-for-the-international-law-of-intelligence/; Ciaran Martin, *Cyber "Deterrence": A Brexit Analogy*, LAWFARE (Jan. 15, 2021, 3:37 PM), https://www.lawfareblog.com/cyber-deterrence-brexit-analogy.

84. Isabella Jibilian & Katie Canales, *The US is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive SolarWinds Hack Happened and Why it's Such a Big Deal*, BUSINESS INSIDER (updated Apr. 15, 2021, 1:25 PM), https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cybersecurity-2020-12?r=US&IR=T; Kevin Poulsen, Robert McMillan & Dustin Volz, *SolarWinds Hack Victims: From Tech Companies to a Hospital and University,* THE WALL STREET JOURNAL (Dec. 21, 2020, 6:00 AM), https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402?page=1.

85. Joe Weiss & Bob Hunter, *The SolarWinds Hack Can Directly Affect Control Systems*, LAWFARE (Jan. 22, 2021, 12:16 PM), https://www.lawfareblog.com/solarwinds-hack-can-directly-affect-control-systems; Software Engineering Institute, CERT Coordination Center Vulnerability Note #843464, *SolarWinds Orion API Authentication Bypass Allows Remote Command Execution*, CARNEGIE MELLON UNIVERSITY (last revised Jan. 28, 2021), https://kb.cert.org/vuls/id/843464.

so, to exclude the latter from domestic and international regulation. For those reasons, it is perhaps more accurate to refer to cyberspace not as a virtual or separate space, but as a set of multidimensional digital technologies—or ICTs—which are fully integrated with human activities that take place in different physical domains or "real life" spaces. As States themselves noted in the 2021 OEWG Final Substantive Report, "the international security dimension of ICTs cuts across multiple domains and disciplines."[86] After all, online resources and activities are not an end in themselves, but a means to achieve different aims or effects that will usually manifest themselves, in different ways, in one or more of the traditional physical domains.

For present purposes, this means that those technologies remain fully subject to the rules and principles of international law to the extent that they are relevant and applicable, and in so far as they have not been carved out by consistent State practice and *opinio juris*.[87] Tellingly, that cyberspace is better framed as a set of digital technologies was already reflected in the language used in the various GGE reports, as well as the OEWG's mandate and documents, which refer precisely to "information and communication technologies." Similar framings, such as cyberspace as a "medium,"[88] or "the interdependent network of information technology infrastructures and resident data,"[89] have been adopted by several States. Thus, when it comes to cyber operations, it is more appropriate to frame questions of applicability of international law to new technological developments.

V. INTERNATIONAL LAW IS TECHNOLOGY-NEUTRAL

If cyberspace is not a separate space or domain, and international law applies in principle to all domains, are ICTs so different from other technologies that they are not or cannot be governed by existing international law? In other words, is there something *inherently different* about ICTs that carves them out from existing international law and, in particular, general international

86. OEWG Final Substantive Report, *supra* note 4, ¶ 10.

87. For a similar point, see Schmitt, *supra* note 52, at 73; Chircop, *supra* note 52, at 650.

88. *See* Brazil, Statement at the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Second Substantive Session on International Law (Feb. 11, 2020), https://media.un.org/en/asset/k18/k18w6jq6eg (comments at timestamp 0:15:45 referring to cyberspace as a "medium" of communications).

89. *Definition of Cyberspace*, Joint Chiefs of Staff, Joint Publication 1-02, DOD Dictionary of Military and Associated Terms 55, (current through Nov. 2021), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

law? Alternatively, do technologies whose impact was unforeseen until a few decades ago fall within the scope of traditional rules and principles of international law, such as sovereignty, the prohibition on the use of force, non-intervention, and no-harm? Have these continued to stand the test of time? The answer to these and other similar questions seems to lie in a simple yet overlooked feature of international law, namely, that it is, by necessity, a technology-neutral system.[90]

Technological—or "tech"—neutrality, in this sense, is not coterminous with political or economic neutrality in the "tech world." It is undeniable that a few major corporations own or control a significant part of the Internet's logical and physical infrastructure and provide the necessary software and hardware technologies that keep public and private online communications and information processing going. Thus, there is no neutrality when it comes to the economic and political forces that shape the use and distribution of ICTs around the world. But international law's "tech neutrality" is something else: it refers to the fact that international rules and principles apply across the board to all technologies, old and new, at least by default and to the extent relevant.

In international as in domestic law, the fact that human beings have developed new technologies over time, such as trains, cars, telephones, televisions, and mobile phones, has never been reason enough to exclude them from the scope of application of existing rules or principles, especially those of general application, such as tort, contract, or criminal law. At the international level, the International Court of Justice recognized as much in its *Nuclear Weapons Advisory Opinion* when it held that:

> 39. These provisions [Articles 2(4), 42 and 51 of the UN Charter] do not refer to specific weapons. They apply to *any* use of force, *regardless of the weapons employed*. The Charter neither expressly prohibits, nor permits, the use of *any specific weapon*, including nuclear weapons. . . .
>
> 85. . . . In the view of the vast majority of States as well as writers there can be no doubt as to the applicability of humanitarian law to nuclear weapons.

---

90. Second "Pre-draft" of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security ¶ 21 (May 27, 2020), https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf [hereinafter Second OEWG Pre-draft]. *See also* TALLINN MANUAL 2.0, supra note 28, at 31 (¶ 4), 46 (¶ 12); Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area, Advisory Opinion of 1 February 2011, ITLOS Reports 2011, at 10, ¶ 117.

> 86. The Court shares that view. Indeed, nuclear weapons were *invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence*; the Conferences of 1949 and 1974–1977 left these weapons aside, *and there is a qualitative as well as quantitative difference between nuclear weapons and all conventional arms*. However, *it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons*. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the *entire* law of armed conflict and applies to *all forms of warfare and to all kinds of weapons*, those of the *past, those of the present and those of the future*. [91]

Similarly, in its Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, the International Law Commission noted that new technologies are also subject to *positive* duties to prevent transboundary harm, requiring States to employ scientific and technological developments to detect, prevent, and redress harm, as well as ensure the safe use of those technologies:

> (11) The standard of due diligence against which the conduct of the State of origin should be examined is that which is generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance. . . . What would be considered *a reasonable standard of care or due diligence may change with time*; what might be considered an appropriate and reasonable *procedure*, standard or rule at one point in time *may not be considered as such at some point in the future*. Hence, due diligence in ensuring safety *requires a State to keep abreast of technological changes and scientific developments*.
>
> . . .
>
> (14) Article 3 imposes on the State a duty to take all necessary measures to prevent significant transboundary harm or at any event to minimize the risk thereof. This could involve, inter alia, taking such measures as are appropriate by way of abundant caution, *even if full scientific certainty does not exist*, to avoid or prevent serious or irreversible damage. . . . An efficient implementation of the duty of prevention may well *require upgrading the input of*

91. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶¶ 39, 85–86 (July 8) (emphasis added).

> *technology in the activity as well as the allocation of adequate financial and manpower resources with necessary training for the management and monitoring of the activity.*[92]

Even more tellingly, the Chairs' Summary of discussions held at the UN OEWG, issued in May 2021 alongside the Group's Final Substantive Report, notes that "States emphasized that measures to promote responsible State behaviour *should remain technology-neutral, underscoring that it is the misuse of technologies, not the technologies themselves, that is of concern*."[93]

International law's tech neutrality, in turn, means that existing international law writ large regulates State conduct with respect to ICTs, at least by default and to the extent relevant. Accordingly, international legal rules or principles *of general applicability*—whether these are rules of customary international law, general principles, or generally-framed treaty provisions—apply to *all technologies through* which States or non-State entities conduct their relevant activities. Importantly, this starting point means that there is no further need to prove the applicability of such rules or principles to ICTs or other technologies via State practice and *opinio juris* that *specifically* refer to ICTs. These rules and principles include the prohibition on the use of force, non-intervention, the *Corfu Channel* rule of "due diligence," the no-harm principle, international human rights law, and international humanitarian law. Their scope is sufficiently broad to cover ICTs, either via interpretation or deductive reasoning. It is the burden of those advocating for the exclusion of ICTs from the scope of these rules to present evidence to the contrary. In other words, they must prove that States, in their general practice accepted as law, have actively carved out ICTs from the scope of what are otherwise general rules and principles.

This conclusion does not deny that when applying general rules of existing international law to new technologies some loose ends may need to be tied and adjusted with best implementation practices.[94] These are necessary to account for certain specific features of digital technologies, such as their speed, connectivity, reach, pervasiveness, and transboundary nature. That notwithstanding—and in line with the views expressed on the issue by an

---

92. International Law Commission, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, *in* REPORT OF THE INTERNATIONAL LAW COMMISSION ON THE WORK OF ITS FIFTY-THIRD SESSION, U.N. Doc. A/56/10 (July 7, 2001), at 154–55, cmt. to draft art. 3, ¶¶ 11, 14 (emphasis added).

93. Chair's Summary, *supra* note 18, ¶ 8 (emphasis added). See also very similar language in Second OEWG Pre-draft, *supra* note 90, ¶ 21.

94. Laurence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARVARD LAW REVIEW 501, 503 (1999).

overwhelming majority of States—the starting point is the applicability of existing international law to *any* technology, rather than a legal vacuum.

As Frank Easterbrook suggests in *Cyberspace and the Law of the Horse*, to rely on well-established general rules and principles, such as contract, tort, and property law, that one can *apply* to cyberspace, as opposed to seeking specifically tailored cyber law, is not antithetical to good tech-governance.[95] Quite the opposite. As he notes, "the best way to learn the law applicable to specialized endeavors is to study general rules."[96] This is not to say that specific rules or regimes are unnecessary or irrelevant. But the point is that specialized regimes for ICTs and other technologies do not necessarily displace more general rules of international and domestic law. These remain valid, are applicable, and inform the interpretation of more specific rules for "cyberspace" and beyond. And there is a very good reason for that: in Easterbrook's words, we lawyers and policy makers "don't know much about cyberspace; [and] what [we] do know will be outdated in five years (if not five months!)."[97]

In short, the applicability and flexibility of general rules and principles of international law are all the more important in the context of ICTs and new technologies, given their rapid development and complexity, which many of us cannot fully grasp. New, specific, and detailed treaty instruments would struggle to keep up to speed with the technical and scientific complexity of new technologies. As a 2020 statement by the Czech Republic summarizes, in guiding the applicability of international law to ICTs, a "technology-neutral approach . . . provides a safeguard against rapidly evolving nature of ICT technologies."[98]

95. Easterbrook, *supra* note 73, at 207–8.

96. *Id.* at 207.

97. *Id.* at 208.

98. Czech Republic Ministry of Foreign Affairs, Comments Submitted in Reaction to the Initial "Pre-Draft" Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security 2 (Mar. 11, 2020), https://front.un-arm.org/wp-content/uploads/2020/04/czech-republic-oewg-pre-draft-suggestions.pdf.

VI. THE RELATIONSHIP BETWEEN INTERNATIONAL LAW AND NON-BINDING RECOMMENDATIONS, NORMS, AND PRINCIPLES

As seen earlier, one objection to the applicability of certain general rules of international law to ICTs is that they have, at times, been framed in normative or hortatory terms in official government statements. Two of these documents—and perhaps the most significant among them—are the 2013[99] and 2015[100] GGE consensus reports, which contain recommendations on norms, rules, and principles of responsible behavior by States in their use of ICTs, fleshed out in more detail in the 2021 GGE Report.[101] For instance, the 2013 GGE report makes the following recommendations for States, some of which seem to mirror existing rules or principles of international law:

> 22. States *should* intensify cooperation against criminal or terrorist use of ICTs, harmonize legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies.
>
> 23. States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States *should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs*.
>
> 24. States *should* encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services.
>
> 25. Member States *should* consider how best to cooperate in implementing *the above norms and principles of responsible behaviour*, including the role that may be played by private sector and civil society organizations.[102]

More elaborately, the 2015 GGE report contains separate sections on "How international law applies to the use of ICTs"[103] and "Norms, rules and principles for the responsible behaviour of States."[104] In the latter section,

---

99. U.N. GGE Report 2013, *supra* note 1.
100. U.N. GGE Report 2015, *supra* note 2.
101. U.N. GGE Report 2021, *supra* note 5, ¶¶ 15–68.
102. U.N. GGE Report 2013, *supra* note 1, ¶¶ 22–25 (emphasis added).
103. U.N. GGE Report 2015, *supra* note 2, ¶¶ 24–29.
104. *Id.* at ¶¶ 9–15.

we find an even longer list of recommendations. Like the 2013 GGE recommendations, they also seem to reflect a range of existing international rules and principles:

> (a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States *should cooperate* in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;
>
> . . .
>
> (c) States *should not knowingly allow their territory to be used for internationally wrongful acts using ICTs*;
>
> (d) States *should consider how best to cooperate* to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;
>
> (e) States, in ensuring the secure use of ICTs, *should* respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, *to guarantee full respect for human rights, including the right to freedom of expression*;
>
> (f) A State *should not conduct or knowingly support ICT activity contrary to its obligations under international law* that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
>
> (g) States *should take appropriate measures to protect their critical infrastructure from ICT threats*, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;
>
> . . .
>
> (k) States *should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams* (sometimes known as computer emergency response teams or cybersecurity incident response teams) *of another State*. A State *should not* use authorized emergency response teams to engage in *malicious international activity*.[105]

The fact that both reports distinguish between the application of international law to ICTs and "voluntary, non-binding norms" might at first glance be taken as an argument that none of the latter "norms" are to be complied with as a matter of legal obligation. To be sure, some of those

105. *Id.* at ¶ 13 (emphasis added).

norms do not reflect binding international law obligations *per se*. However, some of them do use, explicitly or implicitly, the language of law, and it is in those instances that questions arise about the legal status of the provision in question. Arguments that these "norms" do not reflect international legal obligations in cyberspace have been made, most notably, with respect to a rule of due diligence, which, as others have pointed out,[106] seems to be encapsulated in paragraph 13(c) of the 2015[107] report and paragraph 26 of the 2013 report. The UK, for example, has stated that "the fact that States have referred to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace."[108] Similar doubts might arise with respect to other rules that seem to be reflected in the voluntary, non-binding norms, such as duties to cooperate with other States in some circumstances, or the duty not to engage in or support activity contrary to international law, which seems to be subsumed within the broader rule of sovereignty.

In this light, one may wonder whether certain well-established rules of international law have been reduced to non-binding recommendations by effect of the GGE's work. Is it possible that, though these rules are generally applicable, they do not survive as legal obligations in the cyber context because States have chosen to articulate them, in that context, as only voluntary and non-binding? This argument fails to observe that the articulation of these norms is without prejudice to States' rights and obligations under international law. The point has been eloquently raised by Finland during the

106. Schmitt, *Grey Zones*, *supra* note 52, at 53–54. *See also* Australian Department of Foreign Affairs and Trade, Public Consultation: Responsible State Behaviour in Cyberspace in the Context of International Security (June 2020), https://www.dfat.gov.au/sites/default/files/compilation-norm-implementation-guidance.pdf (submission of Global Partners Digital at the fourth and fifth pages); Johanna Weaver, Submission of Australia's Independent Expert to the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (May 29, 2020), https://www.dfat.gov.au/sites/default/files/submission-by-australias-representative-to-the-gge-norm-implementation-may-2020.pdf (noting that "[t]his norm is sometimes referred to as the 'due diligence norm'"); Republic of Korea, Comments on the Pre-Draft of the OEWG Report (Apr. 14, 2020), https://front.un-arm.org/wp-content/uploads/2020/04/200414-rok-comment-on-pre-draft-of-oewg.pdf.

107. U.N. GGE Report 2015, *supra* note 2.

108. U.K. Statement, *supra* note 11, ¶ 12.

OEWG's second session,[109] and Japan at the 2021 GGE meeting.[110] Indeed, paragraph 10 of the 2015 GGE Report makes it clear that these "norms do not seek to limit or prohibit action that is otherwise consistent with international law." As aptly noted in the recent OEWG Final Substantive Report: "norms *do not replace or alter* States' obligations or rights under international law, which are binding, but rather provide *additional specific guidance* on what constitutes responsible State behaviour in the use of ICTs."[111]

Thus, the mere fact that States have decided, for whatever political or diplomatic reason, to mirror existing rules of international law in their policy recommendations cannot deprive those rules of their binding legal force. Otherwise, recommendations such as the one in paragraph 13(f) of the 2015 GGE Report, establishing that a "State should not conduct or knowingly support ICT activity contrary to its *obligations under international law* that intentionally damages critical infrastructure," would become a contradiction in terms. Likewise, it would make little sense if the recommendation contained in paragraph 13(k) of the 2015 GGE Report—calling upon States not to conduct or knowingly support activity harming the information systems of other States' emergency response teams and not to use its own emergency response teams to engage in malicious international activity—were not reflective of an existing obligation under international law. And the recognition, in Norm 13(e), that States should "guarantee full respect for human

109. Janne Taalas, Finland's Ambassador to the U.N., Statement at the Second Session of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (Feb. 10–11, 2020), https://ccdcoe.org/uploads/2018/10/Statement-on-International-Law-by-Finnish-Ambassador-Janne-Taalas-at-2nd-session-of-OEWG.pdf [hereinafter Finland Statement].

110. Akahori Takeshi, Japan's Ambassador for United Nations Affairs and Cyber Policy, Statement on the Adoption of the Report by the Sixth GGE on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (May 28, 2021), https://www.un.emb-japan.go.jp/itpr_en/akahori052821.html (stating that "while some of the 11 norms are related to international law, they do not alter any rights and obligations under international law. At the same time, lack of mention in this report does not mean that international rights and obligations not covered in the document are not applicable in cyberspace.").

111. OEWG Final Substantive Report, *supra* note 4, ¶ 25. *See also* Draft Substantive Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/AC.290/2021/L.2, ¶ 54 (Jan. 19, 2021), https://digitallibrary.un.org/record/3899168?ln=en.

rights" online[112] would be hardly reconcilable with the inclusion of "human rights and fundamental freedoms" as part of the international law applicable to States' use of ICTs.[113]

This conclusion is also in line with how several States have characterized the non-binding, voluntary norms of responsible State behavior. First and foremost, the 2013 GGE Report explicitly notes that the norms are "derived from existing international law relevant to the use of ICTs by States."[114] In the same vein, the 2021 GGE Report recognizes that "[n]orms and existing international law sit alongside each other," and that "[n]orms do not seek to limit or prohibit action that is otherwise consistent with international law."[115] France has also made it clear that these norms are an essential part of the framework of responsible State behavior in cyberspace, and thereby are inseparable from the assessment of how binding international law applies in cyberspace.[116] Germany has also expressed the view that "existing international law, complemented by the voluntary, non-binding norms that reflect consensus among States, is currently sufficient for addressing State use of

112. U.N. GGE Report 2015, *supra* note 2, ¶ 13(e); U.N. GGE Report 2021, *supra* note 5, ¶¶ 36–41.

113. U.N. GGE Report 2013, *supra* note 1, ¶ 21; U.N. GGE Report 2015, *supra* note 2, ¶ 26; U.N. GGE Report 2021, *supra* note 5, ¶ 70.

114. U.N. GGE Report 2013, *supra* note 1, ¶ 16.

115. U.N. GGE Report 2021, *supra* note 5, ¶ 15. *See also* U.N. GGE Report 2015, *supra* note 2, ¶ 10.

116. France's Response to the Pre-Draft Report from the OEWG Chair, https://front.un-arm.org/wp-content/uploads/2020/04/contribution-fr-oewg-eng-vf.pdf (last visited Jan. 7, 2021) [hereinafter French Response].

ICTs."[117] Along similar lines, States such as the UK,[118] France,[119] Poland,[120] Australia,[121] Brazil,[122] and the Dominican Republic,[123] as well as the International Committee of the Red Cross[124] have all affirmed that non-binding norms are complementary rather than alternative to existing international law.

---

117. German Comments on Initial "Pre-draft" of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security and Non-paper Listing Specific Language Proposals Under Agenda Item "Rules, Norms and Principles" From Written Submissions Received Before 2 March 2020 (Apr. 6, 2020), https://front.un-arm.org/wp-content/uploads/2020/04/20200401-oewg-german-written-contribution-to-pre-draft-report-1.pdf.

118. James Roscoe, U.K. Representative to the U.N., Statement during U.N. Security Council Cyber Stability, Conflict Prevention and Capacity Building Meeting (May 22, 2020), https://www.youtube.com/watch?v=K704P5D1n3E#action=share (comments at timestamp 1:13:00); U.K. Government, Press Release, UK Condemns Cyber Actors Seeking to Benefit from Global Coronavirus Pandemic (May 5, 2020), https://www.gov.uk/government/news/uk-condemns-cyber-actors-seeking-to-benefit-from-global-coronavirus-pandemic; U.K. Foreign & Commonwealth Office, Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in U.N. Group of Government Expert Reports of 2010, 2013 and 2015 (Sept. 2019), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf.

119. French Response, *supra* note 116.

120. Tadeusz Chomicki, Poland's Ambassador for Cyber & Tech Affairs, Statement During Arria-Formula Meeting of the U.N. Security Council on Cyber Stability, Conflict Prevention and Capacity Building (May 22, 2020), https://vm.ee/sites/default/files/Estonia_for_UN/statement_of_poland_arria_un_sc_on_cyber_22.05.2020.pdf.

121. Australia's Comments on the Initial "Pre-draft" of the Report of the U.N. Open Ended Working Group in the Field of Information and Telecommunications in the Context of International Security (Apr. 16, 2020), https://front.un-arm.org/wp-content/uploads/2020/04/final-australia-comments-on-oewg-pre-draft-report-16-april.pdf.

122. Ronaldo Costa Filho, Permanent Representative of Brazil to the United Nations, Statement During the Security Council Arria-Formula Meeting "Cyber Stability, Conflict Prevention and Capacity Building" (May 22, 2020), https://vm.ee/sites/default/files/Estonia_for_UN/statement_-_brazil_-_arria_formula_on_cybersecurity_-_final.pdf.

123. José Singer Weisinger, Dominican Republic's Ambassador and Special Envoy to the Security Council, Statement During Arria-Formula Meeting of the U.N. Security Council on Cyber Stability, Conflict Prevention and Capacity Building (May 22, 2020), https://vm.ee/sites/default/files/Estonia_for_UN/22-5-2020_cyber_stability_and_conflict_prevention_-3.pdf.

124. Véronique Christory, Senior Arms Control Adviser for the International Committee of the Red Cross Delegation to the U.N., Statement to the U.N. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (Feb. 11, 2020), https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

In sum, the "voluntary, non-binding" norms of responsible State behavior in cyberspace, as well as similar policy recommendations are neither alternative to, nor do they limit or derogate from, pre-existing binding obligations under international law. On the contrary, norms or recommendations provide States with much welcome guidance on the interpretation, application, and implementation of their existing international obligations in the ICT environment. Therefore, although they are not binding per se, these norms are without prejudice to existing international law.[125] Moreover, they are not deprived of any legal significance as they lay out possible, timely, and widely accepted interpretations or understandings as to how existing international law applies to ICTs.

VII. CONCLUSION: THE WAY AHEAD FOR CYBER INTERNATIONAL LAW-MAKING

General rules of international law apply, by definition, to all persons, objects, events, and technologies that fall within their scope. Although some of these rules are limited to certain physical or natural spaces, such as air, land, sea, and outer space, such limitations cannot be presumed, as international law is not domain-specific. And whether or not such limitations are found, they cannot, in and of themselves, exclude what we often call "cyberspace."

For one thing, the concept of "domain" is not exclusionary, but fulfils a didactic function. For another, cyber is not a space or domain, at least not like traditional physical spaces. Instead, it is a set of digital technologies, spread across multiple territorial boundaries and domains, which have been built by human beings to address different individual, social, political, cultural, and economic needs. Even if their use has led to unique technical advances and human experiences, their impact remains very much grounded in the real world, ultimately affecting individuals and societies across the globe. Finally, as is the case with domestic legal systems, international law does not discriminate on the basis of technology: it applies to each and every tool employed by States or non-State actors in situations that fall under its extensive scope of application. As such, there is no question that international law applies to the Internet and other digital information and communications technologies—in their past, present, and future iterations.

125. *See* Finland Statement, *supra* note 109.

Granted, unlike history, international law can be re-written, provided that States agree to new rules by treaty or customary international law. However, the law that has been developed so far remains there, until such time as new rules are developed. General rules and principles of international law continue to govern State behavior, irrespective of the technologies used. Should States decide to engage in a law-making effort, either aimed at one or more new treaties, or at the creation of new rules of customary international law through general practice accepted as law, they must be aware that they are not building on a legal vacuum, but on the foundations of a wealth of existing, binding rules. These rules have not only been affirmed but continue to be overwhelmingly applied and respected by the vast majority of States in the ICT environment, whether they expressly admit it or not.