INTERNATIONAL LAW STUDIES

Published Since 1895

Neutrality and Cyberspace: Bridging the Gap between Theory and Reality

Noam Neuman

97 INT'L L. STUD. 765 (2021)

Volume 97

2021

Published by the Stockton Center for International Law

ISSN 2375-2831

Neutrality and Cyberspace: Bridging the Gap between Theory and Reality

Noam Neuman[*]

CONTENTS

[*]Colonel (res.), Senior Director, Law of Armed Conflict Division, Office of the Deputy Attorney General (International Law), Israeli Ministry of Justice. An earlier version of this paper was presented as part of the ESIL Kraków-Leiden Online Symposium on "Exploring the Frontiers of International Law in Cyberspace" held on December 4, 2020. The positions expressed in this article do not necessarily represent the views of the Government of Israel or the Ministry of Justice. The author thanks Mattan Gilboa and Yael Naggan for their invaluable support in writing this article.

I. INTRODUCTION

A considerable portion of legal scholarship concerning the application of international law to the cyber domain has focused on cyberspace as a "fifth domain of warfare."[1] While the application of international law to this new frontier is widely acknowledged, the details regarding how it is to be implemented in this domain are murky at best. Thus, discerning the *lex lata* in cyberspace is a challenging task, especially given the lack of relevant treaty law, and sufficient State practice and *opinio juris* regarding this domain. The challenge is further exacerbated when the legal regime in question was formulated based on very particular circumstances in the physical world that often have no obvious equivalent in cyberspace.

The law of neutrality, which regulates the relationship between parties to an international armed conflict (belligerent States) and neutral States, is one such regime. Gradually developed over centuries, this regime is rooted in an era where declarations of war were still prevalent, and the transition between war and peace was clear-cut. The law of neutrality was fashioned in a way that was highly attuned to and dependent upon the concrete attributes of the physical domains in which hostilities take place. As a result, the land, sea, and air domains are each the subject of particular neutrality rules.

The cyber domain also has its own unique characteristics. These include intangibility and the lack of significant physical manifestation, limited supervision and enforcement capabilities over activities taking place within it, and deliberate decentralization as a governance model. These unique features present inherent challenges when seeking to apply to cyberspace existing legal frameworks designed for the physical world. The law of neutrality, with its many domain-specific rules, is a salient example in this regard.

This article will explore whether and how the law of neutrality may be applied in the cyber domain in light of these challenges. Part II provides a brief overview of the law of neutrality and its key provisions as set forth in various instruments and customary law. Part III describes in greater detail the characteristics of the cyber domain noted above. Part IV explores the question of applicability of the law of neutrality to the cyber domain and presents the difficulties in ascertaining the *lex lata*. It then turns to assessing the possibility of applying specific neutrality rules to cyberspace by referring

1. The terms "cyber domain" and "cyberspace" will be used interchangeably throughout this article.

to analogies from other domains. In order to demonstrate what such application may entail, Part V examines the application of neutrality rules from non-cyber domains, *mutatis mutandis,* to three scenarios describing cyber activities in the context of an international armed conflict, and then discusses the legal, practical, and policy challenges that ensue. It concludes that a *mutatis mutandis* application of neutrality rules provides, at best, a limited contribution to the clarification of the legal framework. Finally, Part VI discusses other possible directions for bridging the gap between the law of neutrality and the reality of cyberspace. It specifically suggests conducting careful, norm-specific analyses when examining the possible applicability of rules, while focusing on concepts that do not inherently change from one domain to another. It then takes a broader perspective, pointing to the need to direct the spotlight back to States, taking into account their actual practice in cyberspace and their views on which rules they consider to be applicable as a matter of customary law.

II. THE LAW OF NEUTRALITY – A GENERAL OVERVIEW

Neutrality is considered one of the oldest and most fundamental principles of international law. The purpose of the law of neutrality is to regulate the relationship between parties to an international armed conflict (belligerent States) and States that are not parties to that conflict and remain impartial in respect thereof (neutral States).[2] The law of neutrality seeks to prevent the involvement of neutral States in armed conflicts and to maintain friendly

2. Michael Bothe, *The Law of Neutrality, in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 549 (Dieter Fleck ed., 3d ed. 2013); FEDERAL MINISTRY OF DEFENCE (GERMANY), ZDV 15/2, LAW OF ARMED CONFLICT MANUAL ¶ 1201 (May 1, 2013) [hereinafter GERMAN MANUAL]; UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 1.42 (2004) [hereinafter UK MANUAL]. *See also* 2 GEORG SCHWARZENBERGER, INTERNATIONAL LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS: THE LAW OF ARMED CONFLICT 549–50 (1968).

relations between the belligerents and neutral States,[3] while enabling the continuation of international trade and commerce.[4] In this regard, the law of neutrality has several underlying rationales: to protect neutral States from the harmful effects of armed conflict; to protect belligerent States from actions on the part of neutral States that would benefit their adversaries; and to discourage States from participation in armed conflicts, thus preventing further escalation.[5]

The law of neutrality is part of the legal framework applicable during armed conflict. As its focus is on the conduct of States, it only applies to international armed conflicts, i.e., between two or more States.[6] The applicability of the law of neutrality is determined on a factual basis for each armed conflict. States may declare their neutral status vis-à-vis a particular armed

3. OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL ¶15.1.3 (rev. ed. Dec. 2016) [hereinafter U.S. DOD MANUAL]. *See also* Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare,* 106 MICHIGAN LAW REVIEW 1427, 1442 (2008); Elizabeth Chadwick, *Back to the Future: Three Civil Wars and the Law of Neutrality*, 1 JOURNAL OF ARMED CONFLICT LAW 1, 2 (1996).

4. As such, the law of neutrality includes particular rules relating to monitoring neutral trade for the purpose of preventing contraband from reaching belligerents. *See generally* Elizabeth Chadwick, *Neutrality Revisited, in* ROUTLEDGE HANDBOOK OF THE LAW OF ARMED CONFLICT 455, 456 (Rain Liivoja & Tim McCormack eds., 2016); Bothe, *supra* note 2, at 549–50, 571; Hitoshi Nasu, *The Laws of Neutrality in the Interconnected World: Mapping the Future Scenarios*, *in* THE FUTURE LAW OF ARMED CONFLICT (Matthew Waxman & Thomas Oakley eds.) (forthcoming 2021); 2 LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE: WAR AND NEUTRALITY ¶ 314 (2d ed. 1912).

5. U.S. NAVY, U.S. MARINE CORPS & U.S. COAST GUARD, NWP 1-14M/MCTP 11-10B/COMDTPUB P5800.7A, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ¶ 7.1 (2017); Wolff Heintschel von Heinegg, *Neutrality in Cyberspace*, 2012 4th International Conference on Cyber Conflict 35, 37 (C. Czosseck, R. Ottis & K. Ziolkowski eds., 2012), https://ccdcoe.org/uploads/2012/01/1_3_von_Heinegg_NeutralityInCyberspace.pdf; AUSTRALIAN DEFENCE HEADQUARTERS, ADDP 06.4, LAW OF ARMED CONFLICT ¶ 11.1 (2006) [hereinafter AUSTRALIAN MANUAL].

6. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 553 (Michael N. Schmitt gen. ed., 2017) [hereinafter TALLINN MANUAL 2.0]; Bothe, *supra* note 2, at 557; UK MANUAL, *supra* note 2, ¶ 1.42. It should be noted that some are of the view that unlike the applicability of the law of international armed conflict, the law of neutrality would only be applicable to international armed conflicts that have reached a certain threshold of duration and intensity. This position is reflected in some military manuals as well. *See* U.S. DOD MANUAL, *supra* note 3, § 15.2.1.2; GERMAN MANUAL*, supra* note 2, ¶ 1202. *See also* Bothe, *supra* note 2, at 555.

conflict,[7] although neutrality can equally be deduced by virtue of a State's behavior even absent such a declaration.[8] Likewise, the neutral status of a State ceases with the end of the armed conflict, or prior to that, when that State becomes a party to the conflict.[9]

---

7. These should be distinguished from statements of policy, such as proclamations of permanent neutrality, made by States, which are beyond the scope of this article. *See* 4 NEW ZEALAND DEFENCE FORCE, DM 69 (2 ed), MANUAL OF ARMED FORCES LAW: LAW OF ARMED CONFLICT (2019); OFFICE OF THE JUDGE ADVOCATE GENERAL (CANADA), LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS ¶¶ 1302–3 (2001) [hereinafter CANADIAN MANUAL]; DANISH MINISTRY OF DEFENCE, MILITARY MANUAL ON INTERNATIONAL LAW RELEVANT TO DANISH ARMED FORCES IN INTERNATIONAL OPERATIONS 62 (2016) [hereinafter DANISH MANUAL]; U.S. DOD MANUAL, *supra* note 3, ¶ 15.2.1.4; GERMAN MANUAL, *supra* note 2, ¶ 1203; AUSTRALIAN MANUAL, *supra* note 5, ¶ 11.3; Bothe, *supra* note 2, at 554; David Turns, *Cyber War and the Law of Neutrality, in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 380, 382–83 (Nicholas Tsagourias & Russell Buchan eds., 2015); Paul Seger, *The Law of Neutrality*, *in* THE OXFORD HANDBOOK OF INTERNATIONAL LAW IN ARMED CONFLICT 248, 259–60 (Andrew Clapham & Paola Gaeta eds., 2014).

8. Bothe, *supra* note 2, at 556; CANADIAN MANUAL, *supra* note 7; U.S. DOD MANUAL, *supra* note 3, § 15.2.1.4; Turns, *supra* note 7, at 384.

9. GERMAN MANUAL, *supra* note 2, ¶ 1202; Bothe, *supra* note 2, at 557. Importantly, limited breaches of the law of neutrality would generally not result in the neutral State becoming a belligerent nor would actions taken in defense of a State's neutral status. *See id.* Traditionally, States were entitled to choose whether to participate in the conflict or remain neutral. *See, e.g.*, SCHWARZENBERGER, *supra* note 2, at 573. As discussed below, following the entry into force of the UN Charter, the law of neutrality was somewhat modified. Thus, the freedom to choose to *participate* in the conflict was significantly curtailed, as participation is only permitted insofar as it is taken in collective self-defense on part of a State that is the victim of aggression by another State. *See* Bothe, *supra* note 2, at 554. *See also* Chadwick, *Neutrality Revisited*, *supra* note 4, at 463. It is worth noting that, while controversial, some States consider that there is a status of "qualified neutrality," or of non-belligerence, in order to describe situations whereby a State avoids participation in hostilities yet does not strictly adhere to the impartiality requirement. These States rely on certain State practice in this regard, as well as on international conventions (namely, the Third Geneva Convention of 1949 and Additional Protocol I to the Geneva Conventions of 1977), which recognize the existence of such a status. *See, e.g.*, U.S. DOD MANUAL, *supra* note 3, §§ 15.1.2.3, 15.2.2; UK MANUAL, *supra* note 2, ¶¶ 1.42.1, 1.42.3; *contra* Bothe, *supra* note 2, at 550. The use of the term "qualified neutrality" as it appears in the U.S. DoD *Manual* should be distinguished from an earlier use of this term, intended to signify that a State "is neutral on the whole, but which is obligated by pre-existing treaty obligation to afford some kind of assistance to one of the belligerents." *See* Chadwick, *Neutrality Revisited*, *supra* note 4, at 458 n.19; 2 OPPENHEIM, *supra* note 4, ¶ 305. Note however that in the updated commentaries to the Geneva Conventions, the International Committee of the Red Cross does not distinguish between the two terms (neutrality and non-belligerency) and considers them substantively identical.

The emergence of neutrality as a legal concept can be traced back to the Middle Ages,[10] though its most notable articulation as an international norm was made by Grotius in the seventeenth century.[11] In the eighteenth and nineteenth centuries, when wars were still seen as permissible tools for conducting international affairs, States frequently relied on their neutral status to keep them out of unwanted conflicts.[12] It is during this period that particular neutrality rules began to take shape and were enshrined in early instruments, such as the Paris Declaration of 1856.[13]

The most significant codification of rules regulating the relationship between neutral and belligerent States during war, and their consequent rights and duties in this regard, is found in Hague Conventions V (HC-V) and XIII (HC-XIII) from 1907,[14] which relate to the land and sea domains, respectively. As for the air domain, the Hague Rules of Air Warfare were drafted in 1923 but were never concluded as part of a treaty by States.[15] However, many of the rules pertaining to neutrality are considered to reflect customary

---

See Lindsey Cameron et al., *Article 4: Prisoners of War, in* COMMENTARY ON THE THIRD GENEVA CONVENTION 1084 (Jean-Marie Henckaerts et al. eds., 2020).

10. 2 OPPENHEIM, *supra* note 4, ¶ 286; Seger, *supra* note 7, at 250. Some trace the concept of neutrality back to ancient times. *See* Simon Hornblower, *Neutrality, in* THE OXFORD CLASSICAL DICTIONARY 1011 (Simon Hornblower, Antony Spawforth & Esther Eidinow eds., 4th ed. 2012).

11. 2 OPPENHEIM, *supra* note 4, ¶ 287; Heinz Duchhardt, *From the Peace of Westphalia to the Congress of Vienna, in* THE OXFORD HANDBOOK OF THE HISTORY OF INTERNATIONAL LAW 628, 637 (Bardo Fassbender & Anne Peters eds., 2012).

12. Chadwick, *Neutrality Revisited*, *supra* note 4, at 456–457, 464; Turns, *supra* note 7, at 380–81, 385. *See also* Detlev F. Vagts, *The Traditional Legal Concept of Neutrality in a Changing Environment*, 14 AMERICAN UNIVERSITY INTERNATIONAL LAW REVIEW 83, 85–87 (1998).

13. Declaration Respecting Maritime Law, Apr. 16, 1856, 115 Consol. T.S. 1, 15 Martens Nouveau Recueil (ser. 1) 791, *reprinted in* 1 American Journal of International Law Supplement 89 (1907). *See* 2 Oppenheim, *supra* note 4, ¶¶ 288–91; Bothe, *supra* note 2, at 551; Chadwick, *Neutrality Revisited*, *supra* note 4, at 458–59; Schwarzenberger, *supra* note 2, at 592–93.

14. Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310, 205 Consol. T.S. 299 [hereinafter HC-V]; Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415, 205 Consol. T.S. 395 [hereinafter HC-XIII].

15. Commission of Jurists to Consider and Report Upon the Revision of the Rules of Warfare, Rules of Air Warfare art. 12, Feb. 19, 1923, *reprinted in* 32 American Journal of International law Supplement 12 (1938) [hereinafter Hague Rules of Air Warfare].

international law.[16] The law of neutrality has thus, for the most part, been formulated in light of the specific characteristics of each of these domains.[17]

Under the Hague Conventions, belligerents must respect the sovereign rights of the neutral State and, in particular, the inviolability of a neutral State's territory.[18] The neutral State may enforce this right, and actions to that effect will not be considered by the belligerents as an "unfriendly act."[19] In the land domain, such inviolability means, for example, that belligerents are not allowed to move troops or convoys of munitions or supplies on the territory of a neutral State.[20] In the air domain, belligerent military aircraft are forbidden from entering the jurisdiction of a neutral State,[21] and the regulation of other aircraft is subject to the discretion of the neutral State.[22] Nevertheless, with regard to the sea domain, belligerent ships are allowed, under certain restrictions, to safely pass through the territorial waters of a neutral State.[23]

The law of neutrality not only bestows rights upon neutral States, but also entails certain obligations, such as the requirement to remain impartial and to refrain from participating in the conflict. For example, a neutral State must not supply a belligerent State with ammunition or "war material of any kind."[24] However, a neutral State is not required to prevent the "export or transit" of arms or "anything which can be of use to an army or a fleet" to

16. Program on Humanitarian Policy and Conflict Research at Harvard University, Commentary to the HPCR Manual on International Law Applicable to Air and Missile Warfare 307, 310, 312 (2013) [hereinafter Commentary to the HPCR Manual]; UK MANUAL, *supra* note 2, ¶ 1.26.3; GERMAN MANUAL, *supra* note 2, ¶ 1101, DANISH MANUAL, *supra* note 7, at 545. *See also* von Heinegg, *Neutrality in Cyberspace*, *supra* note 5, at 38 n.27; Seger, *supra* note 7, at 252.

17. *See generally* Chadwick, *Neutrality Revisited*, *supra* note 4, at 459; Schwarzenberger, *supra* note 2, at 573.

18. HC-V, *supra* note 14, art. 1; HC-XIII, *supra* note 14, art. 1.

19. HC-XIII, *supra* note 14, art. 26.

20. HC-V, *supra* note 14, art. 2.

21. Hague Rules of Air Warfare, *supra* note 15, art. 40; Commentary to the HPCR Manual, *supra* note 16, r. 170.

22. Hague Rules of Air Warfare, *supra* note 15, arts. 12, 39. *See also* the commentary, *id.* at 16, 34, 36; Yoram Dinstein & Arne Willy Dahl, Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary rr. 87–88 (2020) [hereinafter Oslo Manual Rules and Commentary].

23. HC-XIII, *supra* note 14, art. 10. *See also* Turns, *supra* note 7, at 387.

24. HC-XIII, *supra* note 14, art. 6; Hague Rules of Air Warfare, *supra* note 15, art. 44. HC-V does not address this obligation in specific terms, however, such an obligation in the land domain may be deduced from the terms of Article 6 of HC-XIII (*see* 2 Oppenheim, *supra* note 4, ¶ 321), or from Article 7, HC-V, *supra* note 14.

belligerents by private entities.[25] Similarly, while belligerents are prohibited from erecting telegraphy stations or other apparatuses on neutral territory or in neutral waters for the purpose of communicating with belligerent forces on land or sea,[26] a neutral State is not required to forbid or restrict the belligerents' use of certain forms of communication belonging to it or to private companies or individuals.[27] Insofar as a neutral State introduces restrictions to either exports or communications such as those described, these restrictions must be applied impartially.[28]

Finally, neutral States must also prevent belligerents from conducting hostile actions from their territory, in the land domain,[29] or in their ports or waters, in the sea domain.[30] In the air, additional unique requirements are imposed, such as the duty to prevent "aerial observation of the movements, operations or defences of one belligerent, with the intention of informing the other belligerent."[31]

HC-V and HC-XIII and the rules regarding the aerial domain are generally considered as still reflective of customary international law.[32] However, the continued relevance of the law of neutrality, at least as it was formed more than a century ago, has been called into question.[33]

Perhaps the most apparent reason for this skepticism is the establishment of the United Nations (UN) in 1945, and the limits on the use of force imposed by its Charter.[34] Under the UN Charter, States may not use force in their international relations unless the Security Council authorizes the use of force as part of collective self-defense,[35] or where the use of force is in self-

25. HC-V, *supra* note 14, art. 7; HC-XIII, *supra* note 14, art. 7; Hague Rules of Air Warfare, *supra* note 15, art. 45.

26. HC-V, *supra* note 14, art. 3; HC-XIII, *supra* note 14, art. 5.

27. HC-V, *supra* note 14, art. 8.

28. *Id.* art. 9; HC-XIII, *supra* note 14, art. 9.

29. HC-V, *supra* note 14, art. 5.

30. HC-XIII, *supra* note 14, art. 25. Some sources also discuss a fundamental principle of acquiescence: if the neutral State fails to prevent breaches of the law of neutrality in its territory, it must acquiesce in enforcement actions taken by belligerents in response. *See* U.S. DoD Manual, *supra* note 3, § 15.3.2; Nasu, *supra* note 4, at 4.

31. Hague Rules of Air Warfare, *supra* note 15, arts. 42, 47 (see additional requirements in Article 46).

32. GERMAN MANUAL, *supra* note 2, ¶ 132; *supra* note 16 and references therein. *See also* U.S. DOD MANUAL, *supra* note 3, § 15.1.4.

33. Bothe, *supra* note 2, at 552; Seger, *supra* note 7, at 251; Nasu, *supra* note 4, at 6.

34. U.N. Charter art. 2 ¶ 4.

35. *Id.* art. 42.

defense against an armed attack.[36] Thus, a Security Council resolution requiring UN Member States to participate in collective self-defense efforts would generally override a neutral State's impartiality obligations, while States seeking to enforce a violation of neutrality are subject to the limitations imposed by the law on the use of force. Nevertheless, the dominant approach taken by States, as well as in academic writing, is that the UN Charter has not rescinded the law of neutrality but rather has modified it in certain aspects.[37]

The development of new technologies and, in turn, the creation of new domains of warfare—outer space and the cyber domain[38]—have also led to compatibility questions with respect to the law of neutrality. This inevitably leads to the question of whether and how customary neutrality rules, developed for the land, maritime, and aerial domains, apply to these new frontiers.

The following parts will examine the possible application of various neutrality rules to cyberspace. In order to do so, it is essential to understand the unique characteristics of the cyber domain. The next Part will, therefore, highlight some of them.

---

36. *Id.* art. 51.

37. UK MANUAL, *supra* note 2, ¶ 1.42.2; GERMAN MANUAL, *supra* note 2, ¶ 1204; U.S. DOD MANUAL, *supra* note 3, § 15.2.3.2; AUSTRALIAN MANUAL, *supra* note 5, ¶ 11.7. While the UK and German manuals appear to diverge regarding whether the UN Charter has superseded the law of neutrality, both conclude that the Charter has, at the very least, modified this body of law. *See also* Bothe, *supra* note 2, at 552–54; COMMENTARY TO THE HPCR MANUAL, *supra* note 16, r. 165; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J Rep. 226, ¶ 89 (July 8). For an in-depth exploration of this issue, see Chadwick, *Neutrality Revisited*, *supra* note 4.

38. Regarding the cyber domain, see, e.g., Press Release, Warsaw Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8–9 July 2016, ¶ 70, NATO Press Release (2016) 100 (July 9, 2016), https://www.nato.int/cps/en/natohq/official_texts_133169.htm; U.S. DOD MANUAL, *supra* note 3, § 16.1.1; U.S. Department of Defense, Summary: Cyber Strategy 2018, at 2, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; Louise Marie Hurel, *Brazil's First National Cybersecurity Strategy: An Analysis of its Past, Present and Future*, INTERNETGOVERNANCEPROJECT (Apr. 5, 2020), https://www.internetgovernance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-past-present-and-future/. Regarding the space domain, see, e.g., *UK Poised for Take-Off on Ambitious Defence Space Strategy with Personnel Boost* (May 21, 2018), https://www.gov.uk/government/news/uk-poised-for-take-off-on-ambitious-defence-space-strategy-with-personnel-boost; *About the United States Space Force*, UNITED STATES SPACE FORCE (May 15, 2020), https://www.spaceforce.mil/About-Us/About-Space-Force/; London Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in London 3–4 December 2019, 115 NATO Press Release (2019) 115 (Dec. 4, 2019), https://www.nato.int/cps/en/natohq/official_texts_171584.htm.

III. THE NATURE OF CYBERSPACE

Cyberspace has come to be known as the "fifth domain" of warfare.[39] While there are several possible definitions of cyberspace, they all have common elements: an information environment, which includes physical and non-physical components, whereby data is exchanged via communication networks.[40] This Part will briefly describe three key features of cyberspace: its intangibility, the limited supervision and enforcement capabilities available within it, and its decentralized model of governance.

A. Intangibility

The cyber domain is often described as intangible. While activities in the cyber domain are carried out through physical infrastructure in sovereign territories—*inter alia,* via computers, servers, cables, and transmitters—the communication of data from one computer to another, as such, lacks significant physical manifestation.[41] Indeed, data is often distributed by different

39. Ronald R. Fogleman, *Information Operations: The Fifth Dimension of Warfare*, 10 DEFENSE ISSUES 1 (1995), https://www.hsdl.org/?view&did=439942. *See also* Wolff Heinstchel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INTERNATIONAL LAW STUDIES 123 (2013). However, some have questioned this characterization. *See* DANISH MANUAL*, supra* note 7, at 82. *See also* Sarah McCosker, *Domains of Warfare, in* THE OXFORD GUIDE TO INTERNATIONAL HUMANITARIAN LAW 77 (Ben Saul & Dapo Akande eds., 2020); Dapo Akande, Antonio Coco & Talita de Souza Dias, *Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond*, EJIL:TALK!, (Jan. 5, 2021), https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/.

40. *Tallinn Manual 2.0* defines cyberspace as "the environment formed by physical and non-physical components to store, modify, and exchange data using computer networks." Tallinn Manual 2.0, *supra* note 6*,* at 564. The U.S. DoD *Manual*, for instance, provides the following definition: "[a] global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." U.S. DoD Manual, *supra* note 3, ∫ 16.1.1. The United Kingdom's MI5 defines cyberspace as a "term used to describe the electronic medium of digital networks used to store, modify and communicate information. It includes the Internet but also other information systems that support businesses, infrastructure and services." *See Cyber*, MI5, https://www.mi5.gov.uk/cyber (last visited Apr. 2, 2021).

41. Turns, *supra* note 7, at 391; von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, *supra* note 39, at 125–26; Mark A. Lemley, *Place and Cyberspace*, 91 CALIFORNIA LAW

servers and service providers, scattered over various locations and jurisdictions,[42] while cyberspace is only the means for transmitting that data.[43] To this extent, the physical location of the infrastructure enabling cyber activity is mainly of technical importance.[44]

The cyber domain is, therefore, generally unaffected by territorial boundaries, and data can flow from one physical location to another seamlessly and without any delay or barriers, unlike limitations imposed on travel or transportation of physical objects.[45] Thus, the cyber domain is characterized by ubiquitous interconnectivity.[46]

B. Limited Supervision and Enforcement Capabilities

In the cyber domain, and the Internet especially, States are not the only prominent stakeholders and do not necessarily fully control cyber infrastructure, including that which is located in their territory.[47] Accordingly, the routing of data within or between networks is not usually controlled by States and often does not occur in one particular central geographical location. Moreover, insofar as the routing of data can be traced and isolated to a particular source within the territory of a State, that State's ability to prevent the

---

REVIEW 521, 523 (2003). *But see* Laura Denardis & Mark Raimond, *The Internet of Things as a Global Policy Frontier*, 51 UC DAVIS LAW REVIEW 475, 477–78 (2017) (expressing the view that in recent years cyberspace has come to include many tangible objects as well).

42. CYBERCRIME CONVENTION COMMITTEE (T-CY), CRIMINAL JUSTICE ACCESS TO ELECTRONIC EVIDENCE IN THE CLOUD: RECOMMENDATIONS FOR CONSIDERATION BY THE T-CY: FINAL REPORT OF THE T-CY CLOUD EVIDENCE GROUP (2016), https://www.coe.int/en/web/cybercrime/t-cy-reports (choose "TCY(2016)5" from the menu) [hereinafter CEG REPORT]; Jennifer Daskal, *Borders and Bits*, 71 VANDERBILT LAW REVIEW 179, 223 (2018); von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, *supra* note 39, at 149.

43. Lemley, *supra* note 41*,* at 523; David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STANFORD LAW REVIEW 1367, 1378 (1996).

44. Daskal, *supra* note 42, at 180, 224. Note that in certain contexts, legal concepts have been introduced in order to accommodate this feature. For example, in relation to cybercrimes, the concept of subjective territoriality was introduced, see Jean-Baptiste Maillart, *The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime,* 19 ERA FORUM 375 (2019).

45. Turns, *supra* note 7, at 398; Lemley, *supra* note 41*,* at 524; Aron Mefford, Lex Informatica*: Foundations of Law on the Internet*, 5 INDIANA JOURNAL OF GLOBAL LEGAL STUDIES 211, 214 (1997); Johnson & Post, *supra* note 43, at 1370–71, 1378.

46. Danielle Higson, *Applying the Law of Neutrality While Transiting the Seas of Cyberspace*, 6 National Security Law Brief 1, 8 (2016).

47. Daskal, *supra* note 42, at 181–82.

transmission of that data or otherwise restrict such transmission through enforcement mechanisms is limited by at least three factors.

First, prevention or restriction would entail significant technological hurdles. For instance, data is often transmitted from one computer to another through multiple servers simultaneously, with the data being divided into numerous "packets."[48] A State may not be aware that a certain packet is part of a larger transmission that should be blocked or prevented.[49] Even if it is aware of the larger communication and attempts to prevent the packet from traveling through its jurisdiction, such an act may prove ineffective since one packet may be easily re-routed through other servers.[50]

Second, restrictions on data transmissions may encounter various legal limitations. In terms of domestic legislation, with limited extraterritorial jurisdictional reach, a State may be prohibited from exercising jurisdiction over a data packet that is merely passing through its servers.[51]

Third, States may have limited capabilities to control or monitor the transmission of data because most of the infrastructure through which the information is routed is owned and operated by private entities.[52] As such, States' enforcement mechanisms are at times dependent on these private entities providing assistance or granting access to the required information.[53]

---

48. *Id.* at 223; Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INTERNATIONAL LAW JOURNAL 815, 824 (2012).

49. von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, *supra* note 39, at 149.

50. Jeffrey T. Biller & Michael N. Schmitt, *Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare*, 95 INTERNATIONAL LAW STUDIES 179, 194–95 (2019); von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, *supra* note 39, at 147; Mefford, *supra* note 45, at 214.

51. *See*, *e.g.*, Daskal, *supra* note 42, at 220; Maillart, *supra* note 44, at 380–82.

52. Daskal, *supra* note 42, at 181; Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEORGETOWN LAW JOURNAL 317, 338, 340 (2015); U.S. Government Accountability Office, GAO-10-606, United States Faces Challenges in Addressing Global Cybersecurity and Governance 3 (2010), https://www.gao.gov/assets/gao-10-606.pdf [hereinafter GAO Report].

53. A few examples are mentioned in the CEG Report; for instance, the ability of service providers to require government authorities to provide lawful orders directed at the owners of the data themselves (*see* CEG REPORT, *supra* note 42, ¶ 16, at 8), to notify customers about investigations of their data (potentially affecting the criminal proceeding) (*id.* ¶ 75, at 28), and, more generally, to determine which government request they should cooperate with, (*id.* at 29). *See also* Jack Nicas & Katie Benner *F.B.I. Asks Apple to Help Unlock Two iPhones*, NEW YORK TIMES (Jan. 7, 2020), https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html; Leander Kahney, *The FBI Wanted a Back Door to the iPhone. Tim Cook Said No*, WIRED (Apr. 16, 2019), https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/.

Furthermore, in cases where data is encrypted, States would have to acquire invasive technical capabilities in order to ascertain the origin, destination, and purpose of the transmission.[54]

This is not to say that there are no attempts to regulate certain cyber activities at the domestic level. Privacy protection regulations are but one example of rules that may limit or restrict the flow of information.[55] Additionally, States are more inclined to exercise jurisdiction over data transmissions when it pertains to their national security or their law enforcement efforts, for example, by issuing search warrants to Internet service providers and platforms.[56] Yet even such efforts are, at times, subject to criticism,[57] and the legal contours regarding remote access warrants are still being discussed by the international community.[58] Therefore, the ability of States to supervise or enforce cyber activities may, for the most part, be of very limited effect.

C. A Decentralized Model of Governance

International governance of cyberspace and the Internet, in particular, has developed rather organically in a decentralized manner, with multiple stakeholders taking part in shaping standards, protocols, and norms. This unique model of governance is not the product of a formal decision by a particular

54. *See*, *e.g.,* CEG Report, *supra* note 42, ¶ 41, at 15; Tim Maurer & Garrett Hinck, *The Trump Administration Wants to be Able to Break into Your Encrypted Data. Here's What You Need to Know*, WASHINGTON POST (July 29, 2019), https://www.washingtonpost.com/politics/2019/07/29/trump-administration-wants-be-able-break-into-your-encrypted-data-heres-what-you-need-know/.

55. For example, the European Union enacted the General Data Protection Regulation to guarantee "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data." *See* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 32, art 1, ¶ (2). *See also* Daskal, *supra* note 42, at 209.

56. Daskal, *supra* note 42, at 205.

57. Such criticism may relate to effects on innovation and competitiveness. S*ee*, *e.g.*, Nicholas Martin et al., *How Data Protection Regulation Affects Startup Innovation*, 21 INFORMATION SYSTEMS FRONTIERS 1307, 1308 (2019). Or it may relate to infringement of human rights. *See*, *e.g.*, Daskal, *supra* note 42, at 185-187.

58. For a discussion on formulating a second additional protocol to the Budapest Convention on Cybercrime, see, e.g., *Enhanced International Cooperation on Cybercrime and Electronic Evidence: Towards a Protocol to the Budapest Convention,* Council of Europe (Sept. 5, 2019), https://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07; more specifically, see CEG Report, *supra* note 42.

State or the international community as a whole—it is the product of decades of evolution and adaptation by governments, standard-setting organizations, and the private sector. The result is that no single body can exert control over cyberspace in its entirety. Instead, the Internet is governed through a multitude of organizations, standard-making bodies,[59] and private entities,[60] alongside domestic governance organizations.

For many States, decentralization is not only an accurate description of the Internet in its current form but rather a desirable model of governance.[61] For those States, this model, based on limited government interference, gen-

59. These include the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for development of policies related to the global Internet system, domain registration, and DNS; the Internet Engineering Task Force (IETF), which is "a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of Internet architecture and the smooth operation of the Internet," which works through various working groups; the World Wide Web Consortium (W3C) that develops certain Internet standards; and other Internet service providers. In standard-setting bodies such as ICANN and the IETF, the decision-making process involves the input of many stakeholders, and governments do not wield decisive authority. *See generally* Laura DeNardis, *The Emerging Field of Internet Governance*, *in* THE OXFORD HANDBOOK OF INTERNET STUDIES 555, 558–63 (William H. Dutton, ed., 2013); *About*, IETF, https://www.ietf.org/about/ (last visited Apr. 2, 2021).

60. Daskal, *supra* note 42, at 235–37. For example, see *Policy Paper: A Digital Geneva Convention to Protect Cyberspace in Times of Peace,* Microsoft, https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace (last visited Apr. 2, 2021).

61. For reports on the positions of the United States and Germany, see Adam Segal, *Holding the Multistakeholder Line at the ITU: The U.S. Perspective*, COUNCIL ON FOREIGN RELATIONS (Oct. 21, 2014), https://www.cfr.org/report/holding-multistakeholder-line-itu; Johannes Thimm & Christian Schaller, *Internet Governance and the ITU: Maintaining the Multistakeholder Approach: The German Perspective*, COUNCIL ON FOREIGN RELATIONS (Oct. 22, 2014), https://www.cfr.org/report/internet-governance-and-itu-maintaining-multistakeholder-approach; GAO REPORT, *supra* note 52, at 1.

erally fosters innovation and growth and enables greater freedom of expression.[62] It should be noted, however, that some States do not necessarily subscribe to this model.[63]

With these characteristics in mind, the following parts will explore the applicability of the law of neutrality to the cyber domain.

IV. APPLICABILITY OF THE LAW OF NEUTRALITY IN THE CYBER DOMAIN

As noted earlier, the law of neutrality gradually developed to address legal issues arising in particular contexts. Accordingly, many of its rules relate specifically to the domain for which they were created. Against this backdrop, this Part will focus on the question of whether the law of neutrality—or particular norms therein—can be applied in the cyber domain.

The common view held by the vast majority of States is that international law generally applies to cyberspace.[64] This approach is also evident in the

62. DeNardis, *supra* note 59, at 568–69. *See also, e.g.,* WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; 2 GLOBAL COMMISSION ON INTERNET GOVERNANCE, WHO RUNS THE INTERNET?: THE GLOBAL MULTI-STAKEHOLDER MODEL OF INTERNET GOVERNANCE (2016), https://www.cigionline.org/publications/who-runs-internet-global-multi-stakeholder-model-internet-governance.

63. Specifically, in recent years there have been attempts by China and Russia to expand the mandate of the International Telecommunications Union in order to empower this body to have a greater role in Internet governance; efforts that have been rejected and subjected to criticism by States such as the United States, United Kingdom, Australia, Estonia, and the Netherlands. *See, e.g.*, Samuele De Tomas Colatin, *A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace*, CCDCOE, https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/ (last visited Apr. 2, 2021).

64. For the positions of individual States, see, e.g., Harold Hongju Koh, Legal Adviser, U.S. Department of State, Remarks at the USCYBERCOM Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL 7 (2012), https://2009-2017.state.gov/s/l/releases/remarks/197924.htm; Jeremy Wright, UK Attorney General, Keynote Address at the Chatham House Royal Institute for International Affairs: Cyber and International Law on the 21st Century, Gov.UK (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [hereinafter UK Attorney General]; Eesti Vabariigi, President, Republic of Estonia, Remarks at the International Conference on Cyber Conflict (May 29, 2019), https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-

ongoing discussions of the UN Governmental Group of Experts (GGE), during which, in 2013, States recognized that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment"—an approach that was reaffirmed in 2015.[65]

While some States have expressed strong opposition to the applicability of the law of armed conflict (LOAC) to cyberspace,[66] the prevalent view is

---

at-the-opening-of-cycon-2019/index.html; Ministry of Foreign Affairs, Government of the Netherlands, Letter to the President of the House of Representatives on the International Legal Order in Cyberspace, app., International Law in Cyberspace 5 (July 5, 2019), https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [hereinafter The Netherlands, International Law in Cyberspace]; Department of Foreign Affairs and Trade, Commonwealth of Australia, Australia's International Cyber Engagement Strategy, Annex A: Australia's Position on how International Law Applies to State Conduct in Cyberspace (2017), https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/annexes.html [hereinafter Australia's Position on how International Law Applies to State Conduct in Cyberspace]; Ministry of Foreign Affairs and Trade, Government of New Zealand, The Application of International Law to State Activity and Cyberspace ¶ 25 (2020), https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf; Ministry of Foreign Affairs, Government of Finland, International Law and Cyberspace: Finland's National Positions 7 (2020), https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727. *See also* Roy S. Schöndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INTERNATIONAL LAW STUDIES 395 (2021). NATO members have adopted cyber operations doctrine. *See* North Atlantic Treaty Organization, AJP-3.20 (ed. A, v. 1), Allied Joint Doctrine for Cyberspace Operations (2020), https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320.

65. Rep. 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); Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ¶¶ 24–28, U.N. Doc. A/70/174 (July 22, 2015); G.A. Res. 70/237 (Dec. 30, 2015) [hereinafter 2015 GGE Report] (the 2015 report was adopted by consensus).

66. Following the 2015 GGE Report, some States expressed a strong opposition to the applicability of LOAC in the cyber context. This was, in fact, one of the grounds for the failure to reach a consensus report in the 2017 meeting of this forum. *See*, *e.g.*, The Ministry of Foreign Affairs of the Russian Federation, Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in

that this regime applies as well.[67] This discourse notwithstanding, specific references to the applicability of the law of neutrality, as such, to cyberspace,

This Sphere (June 29, 2017), https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288; Michael Rodríguez, Representative Of Cuba, Declaration at the Final Session Of Group Of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, JUST SECURITY, (June 23, 2017), https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf; De Tomas Colatin*, supra* note 63; Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norm,* JUST SECURITY (June 30, 2017)*,* https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/; Michael Schmitt, *Norm-Skepticism in Cyberspace? Counter-Factual and Counterproductive*, JUST SECURITY, (Feb. 28, 2020), https://www.justsecurity.org/68892/norm-skepticism-in-cyberspace-counter-factual-and-counter-productive/.

67. The Netherlands, International Law in Cyberspace, *supra* note 64; Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY JOURNAL OF INTERNATIONAL LAW 169 (2017), https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf; UK Attorney General, *supra* note 64; MINISTÈRE DES ARMÉES DE FRANCE, DROIT INTERNATIONAL APPLIQUÉ AUX OPÉRATIONS DANS LE CYBERSPACE [MINISTRY OF THE ARMIES OF FRANCE, INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE] 12–16 (2019), https://www.defense.gouv.fr/content/download/567648/9770527/file/international +law+applied+to+operations+in+cyberspace.pdf [hereinafter MINISTRY OF THE ARMIES OF FRANCE]; Australia's Position on how International Law Applies to State Conduct in Cyberspace, *supra* note 64; Schöndorf, *supra* note 64, at 399; Duncan B. Hollis, Improving Transparency – International Law and State Cyber Operations: Fourth Report ¶¶ 19–20, CJI/doc. 603/20 rev.1 corr.1 (Mar. 5, 2020), http://www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1_corr1_eng.pdf (indicating that Chile and Bolivia are also of this view). The 2015 GGE Report does not address LOAC applicability as such, though it does apply basic principles of LOAC to cyberspace. *See* 2015 GGE Report, *supra* note 65*,* ¶ 28(d). Some have noted that regardless of the matter of applicability, there remains the question of how these rules are to be applied in cyberspace. *See, e.g.,* UK Attorney General, *supra* note 64; Schöndorf, *supra* note 64, at 398. *See also* McCosker, *supra* note 39, at 89.

remain quite limited.[68] Thus, the question of whether and how this legal regime can be applied in cyberspace has yet to be concretely determined.[69]

As indicated above, the main treaties setting forth the law of neutrality, HC-V and HC-XIII, deal with specific domains: HC-V regulates the "Rights and Duties of Neutral Powers and Persons *in Case of War on Land*" and HC-XIII deals with "Rights and Duties of Neutral Powers *in Naval War*."[70] Quite apart from their domain-specific nature, it is also understandable that treaties drafted at the beginning of the twentieth century do not refer to the cyber domain. Therefore, since they are not applicable as such, we must turn to examine whether parts of these instruments reflect applicable rules of customary international law.

As is well known, under international law the identification of a customary rule and its precise content requires an examination of whether there is State practice accompanied by *opinio juris* supporting the existence of such a

68. The Netherlands, Denmark and France are notable exceptions. *See* The Netherlands, International Law in Cyberspace, *supra* note 64, at 5; DANISH MANUAL*, supra* note 7, at 60; MINISTRY OF THE ARMIES OF FRANCE, *supra* note 67, at 16. *See also* U.S. DOD MANUAL, *supra* note 3, § 16.4. The *Commentary* to the *Oslo Manual* is instructive in this regard, noting that:

> [i]t is unclear whether and to what extent the law of neutrality applies in the cyber context. Divergent views exist with respect to this question. Some States believe that the raison d'être of the law of neutrality, and its reliance on the concept of neutral territory, is inconsistent with the characteristics of cyber activities. Others, on the other hand, argue that the law of neutrality may be applied in the cyber context *mutatis mutandis*.

OSLO MANUAL RULES AND COMMENTARY, *supra* note 22, at 25.

69. Eichensehr, *The Cyber-Law of Nations*, *supra* note 52, at 377. *See generally,* Michael N. Schmitt, *Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace*, 3 TEXAS NATIONAL SECURITY REVIEW 32, 36 (2020), https://tnsr.org/2020/07/taming-the-lawless-void-tracking-the-evolution-of-international-law-rules-for-cyberspace/.

70. The titles of Hague Convention V and XIII, respectively (emphasis added). Note, however, that each of these treaties contains provisions which affect the other domain as well. *See, e.g.*, HC-V, *supra* note 14, arts. 3, 7; HC-XIII, *supra* note 14, art. 5. *See also* Turns, *supra* note 7, at 391.

rule.[71] State practice is understood to mean sufficient, widespread, and consistent practice by States.[72] *Opinio juris* means that the State has undertaken the practice with a sense of legal right or obligation.[73]

Accordingly, the identification of customary neutrality rules relating to the cyber domain would require examining whether there is sufficient, widespread, and consistent State practice accompanied by *opinio juris* relating specifically to the applicability and substance of the law of neutrality to cyberspace.[74] Importantly, such identification of custom must be based on State practice that is closely related to the practice under examination in the cyber domain,[75] and the *opinio juris* regarding such rules must not be domain-specific.[76]

In respect of State practice, to the best of this author's knowledge, so far there have been no explicit cases in which States claimed their neutral status had been violated by belligerents as a result of cyber-attacks or cyber opera-

71. North Sea Continental Shelf (F.R.G v. Den.; F.R.G. v. Neth.), Judgment, 1969 I.C.J. Rep. 3, ¶ 77 (Feb. 20); Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 207 (June 27); Jurisdictional Immunities of the State (Ger. v. It.; Greece Intervening), Judgment, 2012 I.C.J. Rep. 99, ¶ 55 (Feb. 3). *See also* Int'l Law Comm'n, Rep. on the Work of Its Seventieth Session, U.N. Doc. A/73/10, at 125 (2018) [hereinafter ILC CIL Report].

72. Asylum (Colom. v. Peru), Judgment, 1950 I.C.J. Rep. 266, 277 (Nov. 20); *North Sea Continental Shelf*, 1969 I.C.J. Rep. 3 (Nov. 20).

73. S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 28 (Sept. 7); *North Sea Continental Shelf*, 1969 I.C.J. Rep. 3, ¶¶ 77–78.

74. *See, e.g.*, Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law* Opinio Juris *and the Law of Cyber Warfare*, 50 TEXAS INTERNATIONAL LAW JOURNAL 189, 231 (2015) (stressing that "State expressions of *opinio juris* take on added importance as cyber capabilities are developed and fielded" in light of the fact that existing IHL treaty and customary rules were not crafted or crystallized with cyber operations in mind"); Seger, *supra* note 7, at 252–53.

75. *See, e.g.*, *S.S. Lotus*, 1927 P.C.I.J. (ser. A) No. 10, at 21, 26–27; *North Sea Continental Shelf*, 1969 I.C.J. Rep. 3, ¶ 79.

76. *See, e.g.*, Frans G. von der Dunk, *Armed Conflicts in Outer Space: Which Law Applies?*, 97 INTERNATIONAL LAW STUDIES 188, 207 (2021) (while discussing the domain of outer-space, it seems that the author considers this approach to be generally applicable when discussing emerging domains of warfare). However, some object to the position whereby applicability of legal rules to cyberspace hinges on their domain-specificity. *See* Akande, Coco & de Souza Dias, *supra* note 39.

tions, or where belligerents claimed that a neutral State breached its obligations under the law of neutrality in the cyber domain.[77] Statements made by States regarding the routing of such attacks through their neutral territory seem to be even scarcer—despite the fact that due to the architecture of cyberspace, such attacks are most likely routed through servers in neutral territory.[78]

In terms of *opinio juris*, as noted above, States have generally expressed their openness towards the application of international law in the cyber domain.[79] However, the number of States that explicitly voiced their support for applying the law of neutrality to the cyber domain remains limited.[80] Even among those States who support this application, some have considered it to be narrow in scope, referring to particular rules and circumstances,[81] while others provided only limited guidance on how specific neutrality rules should be implemented.[82] Therefore, even among States that support the application of the law of neutrality to the cyber domain, what such application purportedly entails is murky, at best.

Consequently, there appears to be insufficient State practice and *opinio juris* to determine that the law of neutrality as a whole, or particular neutrality rules, necessarily apply to the cyber domain as a matter of custom.[83] For some, this conclusion may not be without difficulty, as it may appear to imply

---

77. DANISH MANUAL*, supra* note 7, at 60; Turns, *supra* note 7, at 382, 391–92. *See also* Dan Efrony & Yuval Shany, *A Rule Book on the Shelf?* Tallinn Manual 2.0 *on Cyberoperations and Subsequent State Practice*, 112 THE AMERICAN JOURNAL OF INTERNATIONAL LAW 583, 595 (2018); Hollis, *supra* note 67, ¶ 4.

78. It is worth noting that one possible reason for this lack of practice may be the limited instances where cyber-attacks or cyber operations were publicly acknowledged and attributed to a particular belligerent State. *See, e.g.,* Efroni & Shany, *supra* note 77, at 586; von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, *supra* note 39, at 139; Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA LAW REVIEW 520, 523–24 (2020); Hollis, *supra* note 67, ¶ 3; Schmitt, *Taming the Lawless Void*, *supra* note 69, at 36. *But see* HARRIET MOYNIHAN, CHATHAM HOUSE, THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS: SOVEREIGNTY AND NON-INTERVENTION ¶ 4 (2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks.

79. *See supra* note 64 and accompanying text.

80. *See supra* note 68.

81. U.S. DOD MANUAL, *supra* note 3, § 16.4.1.

82. *See, e.g.,* DANISH MANUAL*, supra* note 7, at 60; The Netherlands, International Law in Cyberspace, *supra* note 64.

83. The *Oslo Manual* reaches a similar conclusion, *See* OSLO MANUAL RULES AND COMMENTARY, *supra* note 22, at 25.

that there is a "legal void" in this respect. Indeed, certain States have expressed their aversion to such a result when it comes to international law more generally. The UK Attorney General, for instance, stated that: "Cyber space is not—and must never be—a lawless world. It is the UK's view that when states and individuals engage in hostile cyber operations, they are governed by law just like activities in any other domain."[84]

This concern may also rest on practical grounds, given that the formulation of new specific treaties concerning the cyber domain does not seem feasible (and at least for some, not necessarily desirable) in the near future in light of the current global political climate and the rapid and continuous technological developments in this field.[85]

These apprehensions may have been a catalyst for a prominent approach featured in current legal discourse, which takes the general willingness to apply international law to cyberspace a step further and assumes that the law of neutrality, or particular neutrality rules, can apply to cyberspace by analogy.[86] Such was the approach, for instance, taken by the experts in *Tallinn Manual 2.0*.[87] It is also reflective of the approach taken, to some extent, in

84. UK Attorney General, *supra* note 64. See, similarly, the position expressed by the Australian Foreign Minister: "[t]he activities of states in cyberspace have implications for us all. Cyberspace is not an ungoverned space. Just like in the physical domains, states have rights but they also have obligations." DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, COMMONWEALTH OF AUSTRALIA, AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY 6 (2017), https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf. *See also* Schmitt, *Taming the Lawless Void*, *supra* note 69; Harold Hongju Koh, *Keynote Address: The Emerging Law of 21st Century War,* 66 EMORY LAW JOURNAL 487, 489–90, 504 (2017); Dapo Akande, Duncan B. Hollis, Harold Hongju Koh & James C. O'Brien, *Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health-Care Sector*, OPINIO JURIS (May 21, 2020), https://opiniojuris.org/2020/05/21/oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-health-care-sector/.

85. *See* Higson, *supra* note 46, at 4, 25–26; Eichensehr, *The Cyber-Law of Nations*, *supra* note 52, at 320–21, 330–35; Duncan B. Hollis, Ben Vila & Daniela Rakhlina-Powsner, *Elaborating International Law for Cyberspace,* DIRECTIONS CYBER DIGITAL EUROPE (July 29, 2020), https://directionsblog.eu/elaborating-international-law-for-cyberspace/; Schmitt, *Taming the Lawless Void*, *supra* note 69, at 35. *See also* von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, *supra* note 39, at 123; McCosker, *supra* note 39, at 98. For an earlier reflection of this approach, based on these practical grounds, see George Walker, *Neutrality and Information Warfare*, 76 INTERNATIONAL LAW STUDIES 233, 247 (2002).

86. Biller & Schmitt*, supra* note 50, at 180–81; McCosker, *supra* note 39, at 93, 97–98.

87. TALLINN MANUAL 2.0, *supra* note 6, at 553–562.

the HPCR *Manual on International Law Applicable to Air and Missile Warfare*[88] and in several academic publications.[89]

While this approach is understandably appealing, it is important to bear in mind that the use of analogies in international law is not without its limitations.[90] Indeed, even its proponents recognize that its application requires a prudent case-by-case examination.[91] Nevertheless, the unique characteristics of the cyber domain, and the fact that the law of neutrality was developed based on situations arising in the physical world (where notions of borders and control are much more clear-cut), bring to the fore certain inherent tensions, and thus, fundamental constraints on the ability to draw analogies. Therefore, attempts to examine the application of neutrality rules by drawing analogies from other domains of warfare, *mutatis mutandis,* may prove to be not only a demanding task, but an unsatisfying one as well. The following Part will illustrate this by presenting several theoretical scenarios of cyber military operations, while attempting to apply specific neutrality rules to them.

V. EXPERIMENTS IN *MUTATIS MUTANDIS* APPLICATION

This Part will analyze three examples discussing various aspects relating to military cyber operations conducted during and as part of an international armed conflict. For each scenario, the possible application of certain neutrality rules, *mutatis mutandis*, will be explored. The following scenarios will be addressed: (a) a cyber-attack transmitted through servers located in a neutral

88. COMMENTARY TO THE HPCR MANUAL, *supra* note 16, at 309.

89. Biller & Schmitt, *supra* note 50, at 191–95; Higson, *supra* note 46, at 28–29; Turns, *supra* note 7, at 392, 396-399; Kelsey, *supra* note 3, at 1444; Walker, *supra* note 85, at 245–46. *See also* Eichensehr, *The Cyber-Law of Nations*, *supra* note 52, at 335-40.

90. This article will not dwell on the theoretical aspects of drawing analogies in international law. Suffice to say that the use of analogies is subject to various substantive and methodological limitations, and as such necessarily warrants a cautious approach. *See, e.g.*, Sandesh Sivakumaran, *Techniques in International Law-Making: Extrapolation, Analogy, Form and the Emergence of an International Law of Disaster,* 28 EUROPEAN JOURNAL OF INTERNATIONAL LAW 1097, 1117–1121, especially 1120–22 (2017); Fernando Lusa Bordin, *Analogy, in* CONCEPTS FOR INTERNATIONAL LAW: CONTRIBUTIONS TO DISCIPLINARY THOUGHT 25, 36–37 (Jean d'Aspermont & Sahib Singh eds., 2019). *See also* Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 I.C.J Rep. 174, 211 (April 11) (dissenting opinion by Pasha, J.).

91. TALLINN MANUAL 2.0, *supra* note 6, at 554; Biller & Schmitt, *supra* note 50, at 182; Turns, *supra* note 7, at 386; Jensen, *supra* note 48, at 816, 824; *See also* Eichensehr, *The Cyber-Law of Nations*, *supra* note 52, at 339–40.

State; (b) a neutral State relaying information regarding an impending cyber-attack as part of a computer emergency response team (CERT) network; and (c) the operation, by private corporations, of online services that block cyber-attacks from the territory of neutral States. Each analysis will attempt to apply neutrality rules that may be relevant to the scenario and discuss the possible implications and complexities that may arise. Scenario (a) will focus on the obligations incumbent on the belligerent States, scenarios (b) and (c) will focus on the obligations of the neutral State. Based on this analysis, the Part will then address challenges to the application of the law of neutrality to cyberspace by analogy that were identified as common to the various scenarios.

A. Possible Applications of the Law of Neutrality in Cyberspace

1. Cyber-attack via Servers in a Neutral State

States A and B are belligerent parties in an international armed conflict. During the course of hostilities, State A conducts a cyber-attack against State B by transmitting malware via servers located in the territory of neutral State C. The attack causes physical damage to cyber infrastructure in State B.[92]

This example appears relatively straightforward. As discussed above, under the law of neutrality, the inviolability of the territory of a neutral State must be upheld by belligerents.[93] Specifically, Articles 1 and 2 of HC-V addressing the land domain prohibit the belligerent State from moving "troops or convoys of either munitions of war or supplies" across that territory.[94] Under this scenario, one might equate the transmission of malware through computer servers with the "movement of troops or munitions of war,"[95] and

92. While the prevailing view is that cyber-attacks with results similar to those of kinetic attacks (i.e., causing death, injury, or physical damage or destruction to objects) trigger the LOAC rules of distinction, precautions, and proportionality, there is an ongoing debate whether cyber operations that do not directly involve physical damage, such as loss of functionality, trigger these rules. *See*, *e.g.*, U.S. DOD MANUAL, *supra* note 3, § 16.2.1; TALLINN MANUAL 2.0, *supra* note 6, at 415–20; Biller & Schmitt, *supra* note 50, at 203–4. Thus, and for the sake of simplifying the example, it is assumed that the attack involves physical harm or destruction.

93. HC-V, *supra* note 14, arts. 1–2.

94. *Id.* art. 2.

95. *See, e.g.*, Kelsey, *supra* note 3, at 1443–44. There is an ongoing debate whether malware or any other malicious code can be regarded as a "weapon" or as "munitions of war." In this context, some scholars have interpreted the term "munitions" broadly, so that it

thus argue that such transmission, when conducted as part of a cyber-attack through the territory of a neutral State, would violate State C's territory, and is therefore prohibited by the law of neutrality.

However, the examination of the relevant neutrality rules concerning the sea domain might lead to a different conclusion, since Article 10 of HC-XIII states that the "neutrality of a Power is not affected by the mere passage through its territorial waters of war-ships or prizes belonging to belligerents."[96] Applying this rule to our scenario by analogy may result in equating the malware used for the attack with warships (which can similarly be used for attacks).[97] Under this analysis, the transmission of malware that forms the basis of the cyber-attack may be considered as "mere passage" through the territorial waters of a neutral State, and therefore permissible.

Consequently, there seems to be a conflict between the different domain-based neutrality rules that pertain to what are, prima facie, similar issues.[98] This is understandable as the law of neutrality applicable to land was developed to protect the physical borders and territories of States,[99] whereas the law of neutrality applicable to the sea was developed distinctly for unique situations pertinent to that domain.[100]

---

might also apply to those contemporary "weapons" and "means" used in cyber operations. Some have also viewed the transmission of information in the neutral State's cyber infrastructure as something akin to physical transportation of those weapons, though this is not without controversy, as some consider that malware cannot be equated with either weapons or munitions. *See*, *e.g.*, TALLINN MANUAL 2.0, *supra* note 6, at 452, 557–78; Biller & Schmitt, *supra* note 50, at 192–95; U.S. DOD MANUAL, *supra* note 3, § 16.4.1 n.44; von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, *supra* note 39, at 148. These discussions, however, are outside the scope of the article.

96. HC-XIII, *supra* note 14, art. 10. *See also id.* art. 12 (generally prohibiting belligerent warships from "remain[ing] in the ports, roadsteads, or territorial waters of the said Power for more than twenty-four hours").

97. Although HC-XIII does not specifically address the possibility of transferring munitions, warships, by their nature, carry weapons systems.

98. 2 OPPENHEIM, *supra* note 4, ¶ 325. Note, however, that some commentators rely on the "silence" of the law in the sea domain and attempt to settle this inconsistency by assuming that the prohibition on land also extends to the sea. *See* Biller & Schmitt, *supra* note 50, at 192.

99. TALLINN MANUAL 2.0, *supra* note 6, at 554, ¶ 4. *See also* James Kraska, *The Law of Maritime Neutrality and Submarine Cables*, EJIL:TALK! (July 29, 2020), https://www.ejiltalk.org/the-law-of-maritime-neutrality-and-submarine-cables/.

100. Such as passage through neutral waters or docking at neutral ports. *See* Vagts, *supra* note 12, at 92–93; Seger, *supra* note 7, at 255.

Nevertheless, it remains unclear which set of rules would be more suitable to draw analogies from in the cyber context. If States adopt the rule pertaining to the land domain as the legal framework governing this scenario, belligerent States would arguably be required to verify that a certain cyber-attack, and the data packets it consists of, does not pass through servers located in the territory of a neutral State in order to avoid breaching the neutrality of other States. However, from a practical point of view, since data packets would most likely travel through neutral State servers on their way to the target State, adopting such an approach may result in the law of neutrality being regularly (and perhaps unwittingly) violated by belligerents. Accepting this conclusion may therefore undermine the continued relevance of this legal regime.[101]

Let us now consider the implications of adopting Article 10 HC-XIII, pertaining to the sea domain, to govern the scenario. Doing so raises a different set of compatibility questions. For warships, navigation routes are not limitless, and some territorial waters may even form part of "highways for international traffic," the passage through which cannot be prohibited.[102] In the cyber domain, as mentioned, data packets travel through multiple servers, and while they can be re-routed to pass through other servers, they will most likely have to pass through servers located in neutral States.[103]

Thus, on the one hand, a comparison between the transmission of data in cyberspace to navigation in the sea domain may be appealing given the relatively expansive freedom of passage available in the latter and the borderless nature of the former.[104] On the other hand, substantial differences between the two remain, such as the considerably greater ability to monitor navigation of vessels at sea, the speed at which such navigation takes place, and the significantly easier ability to attribute naval activity to particular States. Given the limitations arising from the application of both the land and sea domain rules, the uncertainty remains.

---

101. It may presumably also lead to the escalation of existing armed conflicts, since breaches of neutrality may lead to enforcement actions (taken either by belligerent or neutral States), thus drawing more States into the conflict. *See, e.g.,* Joshua Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 AIR FORCE LAW REVIEW 43, 56 (2009). However, it should be recalled that the law on the use of force imposes further obligations in this regard. *See* discussion *supra* Part II.

102. 2 OPPENHEIM, *supra* note 4, ¶ 325. *See also* 1 LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE: PEACE ¶ 188 (2d ed. 1912).

103. *See*, *e.g.*, Kraska, *supra* note 99.

104. *See*, *e.g.*, Higson, *supra* note 46, at 20–21, 29.

What complicates matters even further is that different possible analogies may be drawn even within the same domain of warfare. For example, with respect to the land domain, in addition to the possible application of Article 2 of HC-V to this scenario, it may likewise be possible to apply Article 8 of HC-V, according to which "the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals" is not prohibited.[105]

A *mutatis mutandis* application of Article 8 to our scenario could lead to the Internet being regarded as analogous to the aforementioned communication networks.[106] Accordingly, the use by belligerent State A of neutral State C's publicly accessible Internet servers to transmit data from its territory to State B—even if such data contains malware and is part of a cyber-attack that causes physical damage—would not be deemed a violation of State C's neutrality.[107]

This application of Article 8 may seem practical at first blush. However, such an approach has its limits, as it may be seen as carrying far-reaching consequences. Namely, if data passing through the cyber domain were viewed as a form of communication (as this term is understood under Article 8), irrespective of whether such data constitutes a cyber-attack, the transmissions would not be prohibited by the law of neutrality. Given the considerable support for the position that views the cyber domain as a separate theater of warfare,[108] it remains to be seen whether States will, in fact, support an approach that presumably may involve dispensing with the law of neutrality altogether in this regard.

2. Relaying Information via a "CERT" Network

State C has a governmental computer emergency response team (CERT) tasked with information sharing and cyber incident response, protecting

105. HC-V, *supra* note 14, art. 8.

106. See, for instance, COMMENTARY TO THE HPCR MANUAL, *supra* note 16, at 309; TALLINN MANUAL 2.0, *supra* note 6, at 556–57; von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, *supra* note 39, at 148–49; U.S. DOD MANUAL, *supra* note 3, § 16.4.1. However, applying Article 8, as suggested, to the cyber domain is not without difficulty. *See, e.g.*, Kraska, *supra* note 99; von Heinegg, *supra* note 39, at 149 (discussing lack of relevant State practice in support of such an interpretation).

107. U.S. DOD MANUAL, *supra* note 3, § 16.4.1.

108. *See supra* notes 38 and 39.

both public and private entities within the State.[109] This CERT is part of a network of national CERTs, from multiple States, that regularly shares real-time information about international cybersecurity risks. State A also has a national CERT that is part of the same network.

Following the outbreak of the armed conflict between States A and B, neutral State C's CERT receives information regarding a potential cyber-attack aimed at military cyberinfrastructure in State A. In accordance with its normal course of action within the inter-governmental network, State C relays the information it receives throughout the entire CERT network. Based on the information it shares, State A thwarts the cyber-attack, evidently carried out by State B as part of the armed conflict between them.

As explained above, the law of neutrality imposes a duty on the neutral State to refrain from participating in the conflict. This obligation is reflected, *inter alia*, in the prohibition to "supply, in any manner, directly or indirectly, by a neutral Power to a belligerent Power, of war-ships, ammunition, *or war material of any kind whatever*" as set forth in Article 6 of HC-XIII regarding the sea domain.[110] Thus, under this scenario, the provision of information by State C regarding State B's cyber-attack may perhaps be equated, *mutatis mutandis,* with the provision of "war material of any kind whatever,"[111] as this

109. CERTs (sometimes referred to as CSIRTs or CIRTs) monitor, collect, and analyze information regarding cyber-security incidents in order to identify and react to cyber-security threats. These teams can be governmental, public (such as academic), or privately-run, while one network can include actors from several sectors, which share information and best-practices. Several States have more than one CERT operating within their territory. *See generally* Peter Sullivan, *Computer Emergency Response Team (CERT)*, WHATIS.COM – TECHTARGET, https://whatis.techtarget.com/definition/CERT-Computer-Emergency-Readiness-Team (last visited Apr. 5, 2021); John Haller, Samuel Merrell, Matthew Butkovic & Bradford Willke, *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0*, SOFTWARE ENGINEERING INSTITUTE 1 (April 2011), https://resources.sei.cmu.edu/asset_files/TechnicalReport/2011_005_001_15401.pdf [hereinafter SOFTWARE ENGINEERING INSTITUTE]; *FIRST Members Around the World*, FIRST, https://www.first.org/members/map (last visited July 29, 2020); *CSIRTs by Country – Interactive Map*, EUROPEAN UNION AGENCY FOR CYBERSECURITY, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map (last visited Apr. 2, 2021).

110. HC-XIII, *supra* note 14, art. 6 (emphasis added). A similar prohibition can be found in Hague Rules of Air Warfare *supra* note 15, art. 44.

111. HC-XIII, *supra* note 14, art. 6. *See, e.g.*, 2 OPPENHEIM, *supra* note 4, ¶ 356. *See also* David A. Willson, *An Army View of Neutrality in Space: Legal Options for Space Negation*, 50 AIR FORCE LAW. REVIEW 175, 194, 199–200 (2001); Tess Bridgeman, *The Law of Neutrality and the Conflict with Al Qaeda*, 85 NEW YORK UNIVERSITY LAW REVIEW 1186, 1200 (2010).

information allowed State A to thwart an attack planned against it.[112] Under this analogy, State C would be in violation of its neutrality obligation under Article 6 of HC-XIII.

However, such a conclusion runs the risk of undermining the operation of inter-governmental CERT networks altogether, as these networks rely on a high degree of cooperation and transparency between their members, who work towards a common goal and rapidly respond to threats.[113] As dozens of States take part in such networks,[114] requiring them to either refrain from sharing information regarding a cyber threat or thoroughly investigate the source of every threat in order to make sure that relaying such information would not violate their neutrality obligations may be an onerous demand. As a result, there seems to be an inherent contradiction between taking an active part in a CERT network and the ability to remain neutral. Given the fact that CERTs have become commonplace in the international system, such an interpretation of the law of neutrality appears both undesirable and impractical.

The following example demonstrates some of the complexities that may arise even when the impugned actions are not those of the neutral State but rather of commercial service providers operating from a neutral State's territory.

3. A "Web Application Firewall" Service Operating from a Neutral Territory

State A protects its military website dedicated to recruiting reserve-duty soldiers through a privately-owned "web application firewall" (WAF) service, the servers of which are located in the territory of neutral State C. A WAF is "a firewall that monitors, filters and blocks data packets as they travel to and

112. *See, e.g.,* U.S. DOD MANUAL, *supra* note 3, § 15.3.2.1 (similarly holding that "[a] neutral State also has a duty to refrain from placing its various governmental agencies at the disposal of a belligerent in such a way as to aid it directly or indirectly in the prosecution of the war").

113. SOFTWARE ENGINEERING INSTITUTE, *supra* note 109, at 14, 18.

114. According to the ITU, as of March 2019, there were 109 National CIRTs. *See*, *National CIRT*, ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx (last visited Apr. 2, 2021). For further information regarding particular CERT networks*,* see, e.g., *CSIRTs Network*, ENISA, https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network (last visited Apr. 2, 2021) (for information on the European CSIRTS Network); *FIRST Teams*, FIRST, https://www.first.org/members/teams/ (last visited Apr. 2, 2021).

from a website or web application"[115] for the purpose of protecting that website from malicious activities, including distributed denial-of-service (DDOS) attacks.[116]

State B wishes to shutdown State A's website in order to prevent the recruitment of the additional troops needed to reinforce the frontlines in the international armed conflict. To do so, State B demands that State C disable the WAF provider's service, which originates from State C's territory.

As discussed, neutral States must prevent belligerents from pursuing various hostile acts from their territory. Thus, in the sea domain, Article 25 of HC-XIII provides that a neutral State "is bound to exercise such surveillance as the means at its disposal allow to prevent any violation of the provisions . . . occurring in its ports or roadsteads or in its waters,"[117] including "any act which would, if knowingly permitted by any Power, constitute a violation of neutrality."[118] Regarding the air domain, Article 47 of the Hague Rules of Air Warfare provides that a neutral State "is bound to take such steps as the means at its disposal permit to prevent within its jurisdiction aerial observation of the movements, operations or defenses of one belligerent, with the intention of informing the other belligerent."[119]

The use of WAF services, the servers of which are located in a neutral State's territory, can arguably be deemed a violation of neutrality under Article 25 of HC-XIII. More specifically, it may be equated with an observation of operations with the intention of benefiting one of the belligerents. These assumptions would presumably give rise to an obligation by State C to prevent the provision of WAF services from its territory as part of the armed conflict.

However, applying a different set of rules which appears in both HC-V and HC-XIII may lead to an opposite result, especially given that the service State B seeks to disable is provided by a private entity. Article 7 of HC-V

115. Ben Lutkevich, *Web Application Firewall (WAF)*, SEARCHSECURITY.TECHTARGET, https://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF (last visited Apr. 5, 2021).

116. This service is often provided by private companies, to clients from the private, governmental and public sector. *See id.*

117. HC-XIII, *supra* note 14, art. 25. Similarly, in the land domain, HC-V requires that neutral States "not allow any of the acts referred to in Articles 2 to 4 to occur on its territory," such as the movement of, *inter alia,* "munitions of war or supplies" across its territory. HC-V, *supra* note 14, art. 5.

118. HC-XIII, *supra* note 14, art. 1; *see also* SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA ¶ 15 (Louise Doswald-Beck ed., 1995).

119. Hague Rules of Air Warfare, *supra* note 15, art 47.

provides that "[a] neutral Power is not called upon to prevent the export or transport, on behalf of one or other of the belligerents, of arms, munitions of war, or, in general, of anything which can be of use to an army or a fleet."[120] Similarly, Article 7 of HC-XIII states that "[a] neutral Power is not bound to prevent the export or transit, for the use of either belligerent . . . of anything which could be of use to an army or fleet."[121] Both conventions require that if the neutral State does apply any such measure, such application must be carried out impartially towards all belligerents.[122]

Insofar as the WAF service can be equated to something "which can be of use to an army or a fleet" and the provision of such service to State A can be considered as "transport" or "transit" of the commercial service,[123] then State C would not be required to disable it or prevent its "transport" in any way, as long as it does not prevent State B from accessing that service as well.[124]

---

120. HC-V, *supra* note 14, art. 7.

121. HC-XIII, *supra* note 14, art. 7. *See also* Hague Rules of Air Warfare, *supra* note 15, art. 45, cmt. at 37.

122. HC-V, *supra* note 14, art. 9. While the wording of Article 9 of HC-XIII seems to be more limited, the preamble of the Convention nevertheless confirms that the principle of impartiality is applicable to measures undertaken pursuant to Article 7 of HC-XIII as well. *See also* 1 THE PROCEEDINGS OF THE HAGUE PEACE CONFERENCES, THE CONFERENCE OF 1907: PLENARY MEETINGS OF THE CONFERENCE 295 (James Brown Scott ed., 1920) [hereinafter 1 PROCEEDINGS OF THE HAGUE PEACE CONFERENCES]; Seger, *supra* note 7, at 256.

123. The *travaux préparatoires* of HC-V provide several indications that could be regarded as supporting the plausibility of drawing such an analogy. For instance, it is submitted that while Article 2 of the Convention is addressed to the belligerents themselves, Article 7 "refers only to commercial enterprises of individuals." Additionally, the *travaux* of Article 7 specifically state that the drafters deliberately chose wording broader than just the term "export," and that "the Commission adopted the more general text, embracing the transport as well as the export and making no mention of the nationality of the merchants interested . . . ." *See* 1 THE PROCEEDINGS OF THE HAGUE PEACE CONFERENCES, *supra* note 122, at 138, 141, respectively. *See also* U.S. DOD MANUAL, *supra* note 3, § 15.3.2.1; Willson, *supra* note 111, at 194. However, this possibility is put forth notwithstanding the intricate question of whether arms control regimes and the practice of legal inter-State arms trade, including when done through private corporations, have further modified the law of neutrality, which is outside the scope of this article. *See generally* Nasu, *supra* note 4, at 8–9, 13–14.

124. A similar conclusion may be reached when applying Article 8 of HC-V to this scenario. Under this Article a neutral State "is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals." As explained above, a *mutatis*

Consequently, if State C refrains from disabling the WAF service, the question of whether State C breached its neutrality obligation would seem to depend on the choice of analogy. Again, this results in a high degree of uncertainty as to what rules are—or should be—applicable to such scenarios.

In addition to the legal ambiguity, adopting the first possible application, whereby the neutral State is obligated to prevent the WAF service, may raise practical difficulties. WAF and similar services provided by private actors are commonly used by multiple clients, including governmental ones.[125] This would presumably require private corporations to constantly monitor their governmental clients' activities, as well as their international affairs, and, in turn, require neutral States to monitor these corporations' activities in this regard.[126]

Moreover, as a matter of policy, there is a question of whether neutrality rules should be applied in a manner that mandates States to interfere with Internet services provided from their territory, thus conceivably challenging the decentralized nature of the cyber domain on the one hand,[127] and perhaps contradicting one of the foundational notions of the law of neutrality—the preservation of free commerce despite ongoing armed conflicts—on the other.[128]

Adopting the second possible application—by using an analogy to Article 7 of HC-V and HC-XIII—again, may undermine the relevance of the

---

mutandis application of this Article may equate the Internet to these communication networks, and, since the WAF service is also provided by a private company, the neutral State would not be under any obligation to prevent the communications of WAF services from its territory.

125. Mordor Intelligence, *Web Application Firewall Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)*, RESEARCH AND MARKETS (Jan. 2021), https://www.researchandmarkets.com/reports/4534375/web-application-firewall-market-growth-trends?utm_source=BW&utm_medium=PressRelease&utm_code=5dtx2h&utm_campaign=1248702+-+Global+Web+Application+Firewall+Markets%2c+Forecast+to+2024:+Key+Players+are+Akamai+Technologies%2c+F5+Networks%2c+Barracuda+Networks%2c+and+Imperva&utm_exec=joca220prd. One WAF provider describes its services as delivered "from a physical presence in 200 cities across over 100 countries. This means threats are mitigated close to where they originate, not in your data center." *See Web Application Firewall*, CLOUDFLARE, https://www.cloudflare.com/waf/ (last visited Apr. 2, 2021). For an example of the diverse clientele of such services, see, e.g., *Case Studies*, IMPERVA, https://www.imperva.com/resources/customers/ (last visited Apr. 2, 2021).

126. *See, e.g.,* U.S. DOD MANUAL, *supra* note 3, § 16.4.1; OSLO MANUAL RULES AND COMMENTARY, *supra* note 22, r. 32 cmt., at 27.

127. In this regard, see von Heinegg, *Neutrality in Cyberspace*, *supra* note 5, at 43.

128. *See supra* notes 4, 123; *see also* Nasu, *supra* note 4, at 11.

law of neutrality, as described in the first scenario: belligerent States could regularly use private cyber services available in neutral States, while neutral States might rely on the fact that belligerent cyber activities in their territory are carried out through private corporations to justify their inaction.[129]

B. Challenges Arising from a Mutatis Mutandis *Application*

The scenarios described above are non-exhaustive illustrations of how the application of the law of neutrality, *mutatis mutandis,* in the cyber domain is fraught with interpretative difficulties and can lead in certain cases to counter-productive results. This Section will address some of the broader issues arising from these and similar scenarios by highlighting three challenges arising from attempts to draw analogies from neutrality rules in the physical domains to cyberspace: (1) the legal uncertainty created; (2) practical difficulties in applying the law of neutrality; and (3) policy questions relating to the desirability of such application.

1. Legal Uncertainty

The above scenarios have shown that applying traditional neutrality rules to cyberspace can lead to contradictory outcomes when relying on analogies—both between different domains and even within the same domain. This may be due, *inter alia,* to the fact that the intangible nature of the cyber domain presumably allows for several possible analogies between particular cyber activities to situations in the physical realm: data can flow like a ship through the high seas, it communicates messages as does wireless telegraphy, and requires physical infrastructure for its carriage. This is understandable in light of the fact that neutrality rules applicable to the physical domains were not designed with the cyber domain in mind.

Whatever the reason for these contradictions, their main consequence is that the suggestion that existing neutrality rules could apply *mutatis mutandis* to the cyber context still creates a great deal of legal uncertainty, and States are in no better position to ascertain which rules apply to which scenarios. In this sense, the *mutatis mutandis* approach has not advanced our understanding in any clear-cut manner.

129. Nasu, *supra* note 4, at 12.

2. Practical Difficulties

Even if the challenge of identifying the relevant legal rule is overcome, a *mutatis mutandis* application of neutrality rules to the cyber domain may further encounter significant practical difficulties. As discussed earlier, a certain reality already exists in cyberspace, both in terms of which stakeholders are involved in shaping the domain, and their behavior within it. Cyber infrastructure is scattered throughout the globe with almost no territorial limitations, and even the simplest cyber activities and services may frequently involve both State actors and private entities.

The scenarios above illustrate that in light of the ways in which data is transmitted, the fact that cyberspace is built with no regard to national borders (as they are understood in the physical world), and the question of what would be considered as under the responsibility or jurisdiction of the State is unclear, States confronted with similar scenarios would face a host of difficulties in implementing neutrality rules. The lack of control over both transmissions and their content, as well as over the private corporations who own and operate online services, is inherently at odds with the law of neutrality, which assumes that States have control over their respective jurisdictions.

Thus, application of the law of neutrality could potentially mean that either States risk being in breach of the law of neutrality at any given moment, or that the manner in which States and other stakeholders currently behave in, and use, cyberspace must undergo significant adaptations (for example, radically increasing State control over Internet traffic, changing routing protocols, unencrypting data packets, and the like). This raises the question of whether such demands would be practicable.

3. A Question of Policy

The scenarios described above, and the possible application of certain neutrality rules to them, also seem to raise several policy concerns. Some of the potential applications of the neutrality rules presented above resulted in consequences that run counter to certain underlying rationales of the law of neutrality, such as the prevention of escalation of conflicts and the preservation of free trade despite armed conflicts. Accepting some of the other suggestions resulted in a possible erosion of the law of neutrality due to the questionable practicality of applying particular provisions in the current cyberspace reality.

Similarly, as a matter of policy, there is a question of whether the application of certain neutrality rules would be compatible with the decentralized nature of cyberspace governance or with (at least certain) States' desire to keep it decentralized. Essentially, a more rigid application of some traditional neutrality rules requires that States exert more control over cyberspace, its architecture, and modes of domestic and international governance.

As these concerns exhibit, insofar as the notion that the law of neutrality applies in cyberspace is upheld, even *mutatis mutandis,* States may at times be in the precarious position whereby they need to decide, effectively, whether they prefer to conserve the cyber domain in its current form, risk the erosion of neutrality as a legal regime due to perceived impracticality and diminished compliance, or undermine its core rationales, as the case may be.

The tensions that arise from the scenarios described, relating both to the policy interests inherent to the law of neutrality and policy interests relating to the cyber domain as a whole, point to a broader question of whether such application is in fact desirable.

VI. NEUTRALITY AND CYBERSPACE: THE WAY FORWARD

The analysis in the previous Part highlighted the main obstacles on the legal, practical, and policy levels created when attempting to draw analogies in order to apply the law of neutrality to particular scenarios arising in the cyber domain. This Part will suggest where the discussion regarding the law of neutrality in cyberspace can focus going forward.

First, as a matter of principle, if the law of neutrality is to be applied to the cyber domain, then a careful consideration of the status of each and every norm must be undertaken. The experts who drafted the *Tallinn Manual 2.0* were also mindful of this need.[130] This careful consideration is warranted in light of the material differences between the cyber domain and the domains for which neutrality rules were originally formulated; the time that has elapsed since that formulation; and the fact that, as demonstrated above, acts in the cyber domain may be interpreted in different ways and thus equated with various neutrality rules, leading to different and possibly contradictory outcomes.

Such a careful, norm-specific assessment can be carried out, for instance, by focusing on concepts that do not inherently change from one domain to another. These concepts may have either physical or non-physical elements.

130. TALLINN MANUAL 2.0, *supra* note 6, at 554.

For example, neutrality rules in the land, sea, and air domain all require that the neutral State prevent belligerents physically present in its territory from conducting attacks. This rule can be applied in a straightforward manner in the cyber domain to hackers of a belligerent State operating from within the neutral State.[131] In this sense, a view according to which the cyber-attack can be equated with a kinetic attack carried out by any other military squadron that deploys an attack from neutral territory is plausible.

Other concepts that do not change from one domain to another may be behavioral ones, which do not necessarily rely on physical manifestation. For instance, the prohibition "to supply, in any manner . . . war material of any kind whatever"[132] could potentially be interpreted as encompassing the provision of money or loans to belligerent States.[133] Insofar as this interpretation is deemed acceptable, it would be reasonable to consider that the transfer of money is conduct that remains the same regardless of domain. Thus, such a prohibition would equally apply to the provision of cash as it would to digital transfers.

Concepts that do not inherently change in each and every domain might also be based on broader overarching principles that appear in the law of neutrality. A prominent candidate for such a concept is impartiality.[134] However, as the neutrality rules discussed above demonstrate, broader neutrality principles often have different manifestations in different domains. As a result, and bearing in mind the unique characteristics of the cyber domain, the possible application of these principles to cyberspace must be cautiously considered, taking into account only those that apply in a similar fashion in the other domains,[135] and only if the rationale behind such application is not altered by the unique characteristics of the contemporary practice in cyberspace. Thus, for example, it could be argued that to remain impartial, if a

131. This act presumably violates the obligation "to abstain, in neutral territory or neutral waters, from any act which would, if knowingly permitted by any Power, constitute a violation of neutrality." *See* HC-XIII, *supra* note 14, art. 1.

132. HC-XIII, *supra* note 14, art. 6.

133. U.S. DOD MANUAL, *supra* note 3, § 15.3.2.1. This *Manual* relies on a specific provision in the Havana Convention in this regard. *See also* HC-V, *supra* note 14, art. 18(a).

134. *See, e.g.,* HC-V, *supra* note 14, art. 9. See, in this regard, the U.S. *DoD Manual*'s discussion of impartiality. U.S. DOD MANUAL, *supra* note 3, § 15.3.2; *See also* von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, *supra* note 39, at 144.

135. For example, Article 7 of HC-V, *supra* note 14, Article 7 of HC-XIII, *supra* note 14, and Article 45 of the Hague Rules of Air Warfare, *supra* note 15, all state that a neutral Power is not bound to prevent the export or transit of arms and munitions on behalf of a belligerent.

neutral State imposes restrictions on privately-owned banks providing cryptocurrency loans to one belligerent State, it must do so towards the other belligerent as well.

Looking at the broader picture, a breakthrough in understanding the law of neutrality in the cyber domain can only be achieved by pointing the spotlight back to States. This would consist of discerning the legal significance of their actual practice in the cyber domain and examining their public expressions concerning military activities in cyberspace. While this is admittedly a long-term approach, it is critical to achieving a sound understanding of the law of neutrality in cyberspace.

As noted above, it is currently difficult to ascertain that there is sufficient State practice to identify customary neutrality rules that apply in the cyber domain. At the same time, States' activities within the cyber domain have also gradually evolved over the years, and, as the analysis in the previous Part makes plain, this practice is not fully compatible with neutrality rules.

Yet, States' current practice in the cyber domain must be considered when examining which rules are regarded as applicable, as this is perhaps the most significant indication of how States view the relationship between cyberspace and the law of neutrality. Moreover, while an examination of State practice may also be indicative of their *opinio juris*, it would not necessarily suffice for reaching a conclusive determination in this regard.[136] As mentioned above, so far, many States have voiced their position that international law applies in cyberspace. Still, only a few States have expressly indicated that they view the law of neutrality as applicable in the cyber domain. To determine whether States have a sense of obligation to apply and comply with specific neutrality rules in cyberspace, States must clearly voice their positions. This would be an essential first step in elucidating the current legal ambiguity and inconsistent practice.[137]

---

136. *See*, *e.g.*, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J Rep. 226, ¶¶ 64–72, 96 (July 8); ILC CIL Report, *supra* note 71, at 127, 141.

137. Hollis and his co-authors aptly highlighted this point:

> In the absence of a treaty, an accepted treatise or concrete applications in practice, states have begun to make individual "national statements" on the subject. Since 2018, several states have issued such statements. With the exceptions of Australia and the United States, most are European, and include Estonia, France, Germany, the Netherlands and the United Kingdom. The UN General Assembly has encouraged participants in the current UN Group of Governmental Experts to issue statements, and various contributions to the parallel UN Open Ended Working Group touch on the subject. Yet, the application of international law to cyberspace is neither an exclusive project of the UN nor one that should

While these may seem to be obvious steps, they are often overlooked in the discourse on the applicability of the law of neutrality to cyberspace. Yet, given the challenges discussed at length throughout this article, getting "back to basics" may actually provide the best course of action to bridge the gap between the law of neutrality on the one hand and the reality of how States operate in cyberspace, on the other.

VII. CONCLUSION

This article examined whether the law of neutrality applies to cyberspace and what such an application would entail. It found that it is difficult to ascertain that the *lex lata* supports the applicability of the law of neutrality to cyberspace, given that there are no relevant treaty provisions, and that there is insufficient State practice and *opinio juris* to conclude that customary rules of neutrality have crystallized in the cyber domain. The article then addressed the problems with relying on analogies for the purposes of the application of the law of neutrality to cyberspace. This analysis established that beyond general statements referring to the applicability of international law in the cyber domain, there must be a careful examination of the shape such applicability takes.

Therefore, the article pointed to possible directions in identifying aspects of the law of neutrality that are nevertheless relevant in cyberspace. These include a cautious norm-specific examination in each case and reaching conclusions regarding the *lex lata* based on the actual practice of States, as it manifests in cyberspace. The inquiry undertaken in this article has highlighted the need for States to further express their views: not only as to the applicability of international legal regimes in cyberspace but also on the actual implementation of their specific rules.

Of course, the analysis and conclusions presented in this article are not necessarily unique to the law of neutrality. As such, the proposed approach

---

rely primarily on European contributions (or contributions by those states with the greatest cyber capabilities). As the European Union itself has emphasised, *all* states should have the opportunity—and indeed be encouraged—to delineate and describe their respective positions on how international law operates in the digital environment. Simply put, states need additional opportunities and fora to develop and issue their understandings of the relevant international legal issues.

Hollis, Vila & Rakhlina-Powsner, *Elaborating International Law for Cyberspace, supra* note 85. *See also* Schmitt & Watts, *supra* note 74 (calling for more States to express their *opinio juris* regarding IHL/LOAC and cyber warfare related issues more broadly).

may very well be useful in assessing the applicability of other legal regimes to the cyber domain as well.