İSTANBUL UNIVERSITY PRESS

Annales de la Faculté de Droit d'Istanbul, 73: 327–325

DOI: 10.26650/annales.2023.73.0010
http://annales.istanbul.edu.tr/

Submitted: 27.07.2023
Accepted: 21.09.2023

Annales de la Faculté de Droit d'Istanbul

RESEARCH ARTICLE

International Law in Cyberspace: An Evaluation of the *Tallinn Manuals*

Ebru Oğurlu *

Abstract

While cyber technologies have been advancing since the late 1980s and early 1990s, cyberspace became one of the platforms in which interstate relations occur, ranging from politics and economics to war and conflicts as a result of the mainstreaming of broadband Internet access in the early 2000s. Previously imagined as a platform for free and open communication among people without any state controls or regulations, cyberspace has become one of the main topics of international politics over the last decade. However, laws and policies managing cyberspace have fallen behind the technological developments. Thus, the issue only started to gain the global attention it deserves when modest progress was observed in international law concerning the legal status of cyberspace and the relevant valid principles in the 2000s. State-led cyber operations against Estonia in 2008, Georgia in 2009, and Iran in 2010 supposedly played a significant role in transforming cyberspace into an area of national and international concern. Subsequently, various initiatives have emerged at the international level for adopting internationally recognized cyber rules and principles. Within the framework of Janssens and Wouters' (2022) study *Informal International Law-Making: A Way Around the Deadlock of International Humanitarian Law?*, this work aims to discuss how and to what extent international law can be developed for application in cyberspace by focusing on the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt [Ed.], 2013) and the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Schmitt [Ed.], 2017), the most comprehensive, albeit non-binding, works published to date on the applicability of existing international law in cyberspace. Using a literature review as its method, the study presents the results of the main legal texts and academic studies and argues that even though the issue has only recently come to the fore as one of the newest areas of international legal systems, the specific rights and duties of states flowing from the age-old principles of international law (i.e., sovereignty, territoriality, and non-intervention) have not become obsolete in this domain.

Keywords

International Law, Cyberspace, Sovereignty, Territoriality, Non-Intervention, Tallinn Manual 2.0, Informal International Law-Making

* **Corresponding Author:** Ebru Oğurlu (Prof. Dr.), European University of Lefke, Faculty of Economics and Administrative Sciences, Department of International Relations, Lefke-Northern Cyprus. Email: eogurlu@eul.edu.tr ORCID: 0000-0003-0538-5985
To cite this article: Ogurlu E, "International Law in Cyberspace: An Evaluation of the Tallinn Manuals", (2023) 73 Annales de la Faculté de Droit d'Istanbul 327. https://doi.org/10.26650/annales.2023.73.0010

This work is licensed under Creative Commons Attribution-NonCommercial 4.0 International License

I. Introduction

Cyber activities have been a key global concern due to the increasing number and size of hostile cyber operations since the early 2000s. Large-scale cyber operations against Estonia in 2007, Georgia in its war with Russia in 2008, and cyber-attacks targeting Iran's nuclear facilities in 2010 have drawn the attention of states to this issue due to the destabilizing impacts these have over the whole international system. Consequently, cyberspace and its peaceful management have become an integral dimension of both international relations and international law. The increase in the number of cyber operations coupled with the need to identify the responsible actors (whether states or non-state actors) have forced international society and its members to focus on establishing an international mechanism with the involvement of all stakeholders (e.g., states, academia, and private-sector organizations), along with the participation of the United Nations, to maintain international stability by also covering cyber activities.

International law is a legal system with the objective of regulating relations among states as well as their creators (including international organizations) and plays a crucial role in managing interstate relations on various issues. Global governance of cyberspace (i.e., the technical architecture that allows the global Internet to function) and global governance in cyberspace (i.e., how states, industry, and users may use this technology) have emerged as two prominent issues, as states' attention on this domain has been increasing and cyber operations have become more frequent in the international setting. In that sense, the question of whether international law and its established principles apply to cyberspace is not new. However, the issue has only recently started to gain the global attention it deserves.

Cyberspace offers new opportunities and challenges for states in the foreign policy domain. International lawyers recognize it as a cutting-edge issue of international law, considering its legal dimension not just about rules but also about order and strategic competition. In addition, due to cyberspace not being confined to states and their activities, its governance requires multi-actor cooperation, as non-state actors have expressed concern about the implementation of international law in cyberspace. However, the absence of definitive guidance and the normative ambiguity on the issue prevents the adoption of universally binding and approved rules regarding the use of cyberspace by actors in the international system. The objective of this study is to reduce this ambiguity and reveal the basic applicable rules and principles of international law in the context of cyberspace. Recognizing the fact that the responsibility of a state to secure its own network is supported by the internationally recognized concepts of sovereignty, territoriality, and non-intervention, this study accepts the established principles of international law to apply to state activities in cyberspace. Based on this assumption, the first part of the study defines cyberspace,

while later sections examine how the above-mentioned principles are applicable in the context of cyberspace.

II. Cyberspace: Definitional Framework

The term "cyberspace" is widely agreed to have first been coined by William Gibson in his 1984 novel *Neuromancer*. He defined the concept in unthinkable complexity as the "consensual hallucination of data or as a graphic representation of data abstracted from banks of every computer in the human system."[1] As commonly agreed by theorists, academicians, governments, and non-governmental organizations, however, the concept has lacked a definitional consensus.[2] Instead, numerous definitions have been presented in the literature with different focal points. The common aspect of all the definitions is their recognition of cyberspace as a virtual environment that surrounds the whole world,[3] where access to information is provided through different systems including electronic and computer-based technologies. Based on those commonalities, a comparatively more technical definition by the Pentagon states cyberspace to refer to "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communication technologies."[4] The technical definition describes the physical dimension of cyberspace as "an environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web."[5]

As a result of the significant developments in technology, information, and communication networks, cyberspace as an unnatural non-territorial setting constructed by humans for human purposes has emerged as the fifth field (i.e., operational space at the national level) where people and/or governments can use the necessary technologies to take action. From this perspective, cyberspace represents a sharp contrast to the four physical and natural spheres of states (i.e., land, sea, air,

1 W. Gibson, *Neuromancer* (Ace Publishing, 1984) p. 54.

2 E. Waltz, *Information Warfare: Principles and Operations* (Artech House Publishing, 1998); D. T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security* (National Defense University Press, 2009); T. Maurer, "Cyber Norm Emergence at the United Nations - An Analysis of the UN's Activities Regarding Cyber-security" in *Belfer Center for Science and International Affairs Discussion Paper* (2011-11). Retrieved from: https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf

3 V. Güntay, "21. Yüzyıl Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk" (2019) in *Novus Orbis Journal of Politics and International Relations*, *1*(2), 183.

4 Kuehl (n 2) 28

5 W. H. von Heinegg, "Legal Implications of Territorial Sovereignty in Cyberspace" in *Proceedings from 2012 4th International Conference on Cyber Conflict* (NATO CCD COE Publications, 2012) p. 8. Retrieved from: https://www.ccdcoe.org/uploads/2012/01/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf

and space)[6] and integrates cyberspace into all these spheres. Thus, one can argue cyberspace to be firmly embedded in the elements of power, one where the national community is involved at a more global level in an anarchic environment connecting millions of networks without any top authority or geographical boundary.[7] In this sense, cyberspace has emerged as a challenge to the established political, social, and economic settings of the international community and has drastically changed the system of "how states govern, how companies deliver services and public goods, how individuals interact with online social networks, and how citizens participate in civil society."[8] Under these conditions, the most complicated task for the whole international system is to determine the legal order of such a complex area, as this has critical significance for state sovereignty and national security.

III. Applicability of International Law in Cyberspace

States form part of an anarchic order in the international system. In this environment, they exist as sovereign equals not subject to any universally accepted legitimate political order and/or central authority. Interstate relations are regulated by international law as a fundamental pillar of a rules-based global system. States obey international law as a result of their habits and concerns about the chaos that may arise in the absence of such rules.[9] Among many other issues, international law is binding regarding states' use and regulation of information and communication technologies (ICTs) and defense against all kinds of malicious operations in an international context.[10] Over time, however, the law may become inadequate due to the technological developments in information and communication networks and their impacts on interstate relations. The emergence of cyberspace as the fifth domain has necessitated the clarification of the legal system in order for an open, safe, and reliable cyber environment to be achieved.

Despite the assumptions regarding the inadequacy of the current form of international law, cyberspace does not operate in a legal vacuum. It does not present a lawless zone where hostile and aggressive activities can be conducted without any

6 A. Liarapoulos, "Power and Security in Cyberspace: Implications for the Westphalian State System" in *Panorama of Global Security Environment* (Bratislava: Centre for European and North American Affairs, 2011), p. 115; S. K. Gourley, "Cyber Sovereignty," in P. A. Yannakogeorgos & A. B. Lowther (Eds.), *Conflict and Cooperation in Cyberspace: The Challenge to National Security* (Taylor & Francis, 2014), p. 278.

7 Şerife Karadağ, "Siber Uzayda Uluslararası Hukuk Mümkün Mü?" (2019) in *International Social Sciences Studies Journal*, *5*(36), 2828; M. C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009). Retrieved from https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

8 H. K. Ecemiş Yılmaz, "Siber Uzay, Siber Güvenlik, Dijital Egemenlik Kavramlarının Uluslararası Hukuk Bağlamında Değerlendirilmesi" (2021) in *ULİSA- Mühendislik, Hukuk, İletişim ve İktisat Perspektifinden Siber Güvenlik ve Sosyal Medya*, *12*(9), 21; D. J. Betz & T. Stevens, *Cyberspace and the State: Toward a Strategy for Cyber Power* (Routledge, 2011).

9 F. Sönmezoğlu, *Uluslararası Politika ve Dış Politika Analizi* (Filiz Kitabevi, 2000), p. 644.

10 S. Haataja, "Cyber Operations against Critical Infrastructure Under Norms of Responsible State Behaviour and International Law" (2022) in *International Journal of Law and Information Technology*, *30*(4), 425–429.

restraint. Rather, a general consensus exists among all actors in the international system about the validity of the established rules and principles of international law regarding states' activities in cyberspace, as is the case in non-cyber areas. The legal framework in this domain sets the principles and rules determining what is legal and illegal so as to guide states on how to legally and acceptably behave. These actors assume that "state sovereignty and international norms and principles that flow from sovereignty apply to state conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory."[11] Regarding their use of ICTs, states additionally have bound themselves to the principles of "sovereign equality, dispute settlement by peaceful means, and non-intervention in the internal affairs of other states."[12] Based on these assumptions, the subject of ongoing discussions is not whether international law applies to state activities in cyberspace but rather how it applies, mostly due to the ambiguity of states in invoking the law or in how they characterize it.[13] The issue is agreeing on the "relevant legal principles that bear on the person, place, object, or type of activity in question."[14]

Cyberspace's lack of a universally binding and well-functioning system of international law, has led to legal uncertainty due to disagreements and interpretative differences, even in the case of agreement regarding the letter and spirit of the law. In addition, the diversity and complexity of actors in cyberspace also makes determining the jurisdiction of international law in cyberspace difficult. With the development of the concept of cyberspace and the increase in its use by different actors in the international community, their interactions have become much more frequent and comprehensive, with vertical and diagonal connections through political, economic, social, and cultural networks.[15] This fact highlights the significance of international "multi-stakeholder governance,"[16] which includes both civil society and private companies in cyberspace management.

Other challenges for cyber governance include uncertainty about the target group for whom the legitimacy of the principles of international law will be valid and the necessity to attribute unlawful behavior to a state if it is blamed for the conduct

11 N. Tsagourias, "The Legal Status of Cyberspace: Sovereignty Redux?" in N. Tsagourias & R. Buchan (Eds.), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2021), p. 9; H. Moynihan, *The Application of International Law to State Cyberattacks Sovereignty and Non-intervention* (Chatham House, December 2019). Retrieved from: https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks

12 *Ibid*, p. 8

13 *Ibid*, p. 3

14 M. N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" (2013), in *Harvard International Law Journal Online*, *54*(5), 14. Retrieved from: https://harvardilj.org/2012/12/online-articles-online_54_schmitt/

15 K. Ziolkowski, "Confidence Building Measures for Cyberspace" in K. Ziolkowski (Ed.), *Peacetime Regime for State Activities in Cyberspace - International Law, International Relations and Diplomacy* (NATO CCD COE Publication, 2013), p. 156.

16 D. B. Hollis, *A Brief Primer on International Law and Cyberspace* (Carneige Endowment for International Peace, June 2021). Retrieved from: https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763

of unlawful behavior.[17] Because international law only regulates its subjects, such attribution is necessary but equally difficult, considering the existing complications in technical attribution. However, without the identification of who is responsible, deciding whether the issue falls within the framework of international law becomes impossible.[18] Such challenges are becoming more complicated due to the competing claims among states, as well as their substantial interpretative differences, even in the case of common assumptions.

Under these aforementioned difficulties, efforts to solve the problem involve evaluating the specific content of the individual rules to determine whether they are relevant to cyberspace, and if so, how they will be applied through cooperation among states. However, states have largely preferred to remain silent on the clarification of the relevant rules and principles, as well as on how to identify acceptable state behaviors as the basis of customary international law, despite the increased use of cyberspace and the need for regulatory mechanisms. On the other hand, states have individually attempted to strengthen their legal capacity regarding cyber issues and have collectively made efforts to contribute to common laws on cyberspace. In this regard, the 2017 publication, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, constitutes a significant achievement. Although it does not answer all questions and conflictual topics still remain, *Tallinn Manual 2.0* is presented in the next section as "the beginning of a longer and more significant discussion about the formulation of international law concerning cyberspace and its implementation."[19]

IV. The Tallinn Manuals[20]

Tallinn Manual on the International Law Applicable to Cyber Warfare as published in 2013 and the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* as published in 2017 have been prepared as the most comprehensive academic, albeit non-binding, document on the applicability of international law in cyberspace and cyber conflicts. They can be accepted as an attempt at "informal international law-making" and have been proposed by Janssens and Wouters as a "new form of law-making that does not fit into the traditional toolbox of public international law."[21] Informal international law-making emerged as an alternative method of overcoming the deadlock that has been led by states' unwillingness to work on and conclude a formal way of law-making. Through its flexibility, three

17 E. Yılmaz (n 8) pp. 22–23.

18 Hollis (n 16) pp. 3–5.

19 Moynihan (n 11), p. 5.

20 *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (*Tallinn Manual 1.0*) and its successor, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (*Tallinn Manual 2.0*).

21 P. C. Janssens & J. Wouters, "Informal International Law-Making: A Way Around the Deadlock of International Humanitarian Law?" (2022) pp. 104, 920–921. *International Review of the Red Cross*, 2114.

forms of informality distinguish informal international law making from formal and conventional ways: 1) output informality, where the final instrument, whether in the form of memoranda of understanding or as guidelines or declarations, are not recognized as a traditional source of international law; 2) process informality, where cooperation at the global level would take place in a flexibly organized forum or network rather than happening at a conventional diplomatic conference or in a traditional international organization; and 3) actor informality, which in addition to the traditional state actors, would welcome all other actors during and at the end of the negotiations, and states would be represented by those without diplomatic or representative power.[22]

Fitting these characteristics, the Tallinn Manuals were written by experts invited by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) and represent two of the most typical examples of informal international law making. They are not official documents but rather the output of two different interrelated initiatives taken by a group of professionals acting on their own behalf. They do not reflect the formal opinions of any international organization or any state involved in the process. However, the documents have become invaluable sources for legal advisors to governments and for scholars since their publication.

The original document, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (hereafter called *Tallinn Manual 1.0*), was published in 2013. The focus of *Tallinn Manual 1.0* is on cyber operations that involve force and that take place in the context of armed conflict. Due to the criticisms directed toward *Tallinn Manual 1.0*, mostly because of limited participation from the West and its limited coverage, a follow-up initiative was launched to extend the manual's coverage by also including cyber operations during peacetime. Its revised and expanded version, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (hereafter called *Tallinn Manual 2.0*) was prepared by a more comprehensive international group of experts and published in 2017. With additional rules and modifications, as well as a complete renumbering, *Tallinn Manual 2.0* supersedes the first. One should importantly note that both *Tallinn Manuals* present current international law and its application within the framework of the cyberspace context. Even if the manuals themselves are not binding, "the legal obligations they incorporate are."[23]

Tallinn Manual 2.0 is composed of four parts and is a revolutionary achievement that makes a significant contribution to the theoretical and practical clarification of international law with its focus on cyberspace. Part I is titled "General International

22 J. Pauwelyn, "Informal International Lawmaking: Framing the Concept and Research Questions," in J. Pauwelyn, R. A. Wessel, & J. Wouters (Eds.), *Informal International Law-Making* (Oxford University Press, 2014), pp. 15–20.

23 Janssens & Wouters (n 21) p. 2129.

Law and Cyberspace" and covers sovereignty, due diligence, jurisdiction, law of international responsibility, and cyber operations. Part II presents "Specialized Regimes of International Law and Cyberspace" and covers international human rights law, diplomatic and consular law, law of the sea, air law, space law, and international communication law. Part III deals with "International Peace and Security and Cyber Activities" and is taken mostly from *Tallinn Manual 1.0*. This part covers peaceful settlement, prohibition of intervention, the use of force, and collective security. Part IV presents "The Law of Cyber Armed Conflict" in the general framework of the law of armed conflict, and more specifically through the conduct of hostilities; certain persons, objects, and activities; occupation; and neutrality.[24] Overall, the whole document assumes that states' responsibility to secure the networks within their territories is supported by the principles of internationally recognized sovereignty and non-intervention. Accepting sovereignty as the foundation of international law and non-intervention as its corollary principle, the following part focuses on these two principles and evaluates how it has become possible to apply sovereignty and non-intervention in the cyberspace context by referring to the relevant rules of *Tallinn Manual 2.0*.

A. The Principle of Sovereignty in Cyberspace

While sovereignty signifies the power and supremacy of a state in its traditional definition, sovereignty also emphasizes the territoriality of a state in the framework of international law. However, the fact that "territory is not just a geographical or physical construct but a legal and political construct [referring to the] organization of sovereign power for political and legal purposes"[25] has to be underlined. Due to its nature and the actors involved in it, cyberspace as the fifth field after land, sea, air, and space has challenged the current state-centered system and forced actors in the system to reevaluate key concepts, including sovereignty,[26] security,[27] power,[28]

24 M N. Schmitt (Ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), pp. v–xi.

25 Tsagourias (n 11), p. 13.

26 D. Hassan, "The Rise of the Territorial State and the Treaty of Westphalia" in G. Morgan (Ed.) *Yearbook of New Zealand Jurisprudence* (University of Waikato School of Law, 2006), pp. 64–67; P. W. Singer & A. Friedman, "Cult of the Cyber Offensive" (2014), in *Foreign Policy*, p. 182. Retrieved from http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/

27 H. Tiirmaa-Klaar, "Botnets, Cybercrime and National Security" in H. Tiirmaa-Klaar, J. Gassen, E. Gerhards-Padilla, & P. Martini (Eds.) *Springer Briefs in Cyber Security – Botnets* (Springer, 2013), pp. 11–13; Lucas Kello, "The Meaning of the Cyber Revolution" (2013) in *International Security*, *38*(2), 31–32; J. S. Nye, *The Regime Complex for Managing Global Cyber Activities* (The Global Commission on Internet Governance and Chatham House, May 2014), p. 6. Retrieved from: https://www.cigionline.org/static/documents/gcig_paper_no1.pdf ; R. J. Deibert & R. Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security" (2010) in *International Political Sociology*, *4*(1).

28 J. S. Nye, *Cyber Power* (Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010). Retrieved from: https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf ; J. S. Nye, *The Future of Power* (PublicAffairs, 2011); R. O. Keohane & J. S. Nye, "Power and Interdependence in the Information Age" (1998), *Foreign Affairs*, 77(5).

and actor[29] in terms of the "cybered Westphalian age."[30] Thus, questioning many assumptions that have hitherto been taken for granted has become normal.

Despite its meaning being transformed in the digital and technological age, the principle of sovereignty remains the top priority for all states and frames current international relations.[31] The first rule in *Tallinn Manual 2.0* states, "The principle of State sovereignty applies in cyberspace."[32] If sovereignty symbolizes authority and power, according to *Tallin Manual 2.0*'s first rule, states are supposed to implement their sovereignty over persons, objects, and actions in their cyberspace as they do in their non-cyberspace. The implementation of sovereignty in cyberspace can be interpreted from two perspectives (i.e., rights-based and obligation-/duty-based). As a fundamental principle of statehood, state sovereignty first implies the ultimate authority of any state in terms of its "territorial integrity and political independence."[33] Due to much of what cyberspace consists of existing in the sovereign territories of states and being possessed by governments or companies within state borders,[34] states have authority over the ICT infrastructure that is located within their national territories and openly declare their commitment to protect their national cyber-borders. Thus, the cyber infrastructure is under the jurisdiction of the flag state and its sovereign prerogatives. Specifically, the physical infrastructure needed for cyberspace to function is terrestrial and therefore not exempt from state sovereignty.[35]

Because damage in cyberspace is a real possibility, states cannot afford to leave it uncontrolled, despite the difficulty in imposing their sovereignty over this borderless area. Instead, what cyberspace and cyber-management need is state regulations and governmental rules.[36] In this sense, states have the right to manage their cyberspace and to provide a secure environment for its healthy functioning. Accordingly, the sovereignty principle is applied to states' cyber activities as an

29 T. Lan & Z. Xin, "Can Cyber Deterrence Work?" in A. Nagorski (Ed.), *Global Cyber Deterrence: Views From China, The U.S., Russia, India, and Norway* (East-West Institute, 2010), p. 1; K. F. Rauscher, *First Joint Russian-U.S. Report on Cyber Conflict* (EastWest Institute, 2011). Retrieved from: https://www.eastwest.ngo/idea/towards-rules-governing-cyber-conflict-0 ; C. C. Demchak & P. Dombrowski, "Rise of a Cybered Westphalian Age" (2011) in *Strategic Studies Quarterly*, *5*(1), 54–57; N. Kshetri, "Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations" (2013) in *Electronic Commerce Research*, *13*(1).

30 Demchak & Dombrowski (n 29), p. 35.

31 P. W. Franzese, "Sovereignty in Cyberspace: Can It Exist?" (2009), *Air Force Law Review*ö *64*.

32 Schmitt (n 24), p. 11.

33 von Heinegg (n 5), p. 8; S. Couture & S. Toupin, 'What Does the Notion 'Sovereignty' Mean When Referring to the Digital?" (2019), in *New Media & Society, 21*(10), 4–6.

34 Liarapoulos (n 6), p. 37; Betz & Stevens (n 8).

35 Gourley (n 6), pp. 279–286; von Heinegg (n 5), p. 8; M. N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" (2013), in *Harvard International Law Journal Online*, *54*(5). Retrieved from: https://harvardilj.org/2012/12/online-articles-online_54_schmitt/ ; G. L. Herrera, "Cyberspace and Sovereignty: Thoughts of Physical Space and Digital Space," in M. Dunn-Cavelty, V. Maurer, & S. F. Krishna-Hensel (Eds), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (Ashgate, 2007), p. 68.

36 M. Carr, *US Power and the Internet in International Relations: The Irony of the Information Age* (Palgrave Macmillan, 2016); T. H. Wu, "Cyberspace Sovereignty? The Internet and the International System" (1997), in *Harvard Journal of Law & Technology*, *10*(3), 649–656.

outcome of their abilities "to regulate such matters within territorial borders and to exercise power."[37] In light of disagreements and uncertainties, a blurring of borders appears to exist among "sovereignty over cyberspace, sovereignty in cyberspace, and no cyber sovereignty,"[38] despite the concept of sovereignty in itself being well-understood. Accordingly, each state is given the right to determine the relevant rules and principles for governing cyberspace within its borders. Thus, "cyberspace is not immune to state sovereignty."[39] On the contrary, any state can declare "its sovereignty by exercising its jurisdiction over the cyber infrastructure located on its territory, over its nationals within its territory as well as over non-nationals, including legal persons such as companies within its territory."[40] This statement implicitly refers to different dimensions of cyberspace, technically called the layers of cyberspace. The physical layer of cyberspace consists of "the physical network components, i.e., computers, integrated circuits, cables and communications infrastructure." The logical layer comprises "connections which exist between network devices and allow the exchange of data across the physical layer." The social layer includes "human beings engaged in cyber activities."[41] Sovereignty can be asserted over each of these.

On the other hand, the principle of sovereignty also imposes obligations on states "to protect within the territory the rights of other states, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in a foreign territory."[42] From this perspective, sovereignty clearly prohibits specific types of cyber activities that may range from unauthorized conduct of cyber activities by a state present in another state's territory or remote cyber operations leading to the physical damage in the territory of another state in order to interfere with the use of governmental functions by the territorial state. *Tallinn Manual 2.0* clarifies this with the following statement: "A state must not conduct cyber operations that violate the sovereignty of another State." It is also clearly states, "States have sovereignty over cyber infrastructures in their own countries, and attacks on these infrastructures are unlawful."

Three core rights are embodied in the sovereignty principle. These include "the right to territorial integrity" (i.e., territorial/internal sovereignty as discussed in Rule 2), "the right to independence of state powers" (i.e., political independence), and "the equality of states in the international system" (i.e., external sovereignty as discussed in Rule 3). States' rights in relation to their land, air space, and all maritime zones

37 Russell Buchan, *Cyber Espionage and International Law* (Hart Publishing, 2019 [2018]), p. 50.

38 Gourley (n 6), p. 288.

39 *Ibid* pp. 286–287.

40 Tsagourinas (n 11), p. 14.

41 N. Tsagourias, "Law, Borders and the Territorialisation of Cyberspace," (2018), in *Indonesian Journal of International Law*, *15*(4), 539.

42 von Heinegg (n 5), pp. 8–9.

are covered by the sovereignty principle. These rights include the rights of states regarding their political independence and jurisdiction with the condition that they act within the confines of international law. This condition forces each and every state to recognize the independence and authority of other states while enjoying the privileges intrinsic to their sovereignty. Such a statement shows the wholeness of the three dimensions of sovereignty (i.e., internal sovereignty, political independence, and external sovereignty).

Because treaty provisions and customary law safeguard states' sovereignty and territorial integrity, they also provide the basis for states' claims prohibiting the use of force against their sovereignties.[43] According to these statements, cyberspace is thus "not immune from state sovereignty and from the exercise of jurisdiction."[44] Applying the sovereignty principle to cyberspace, the debate revolves around how and the extent to which sovereignty applies to cyberspace.[45] As indicated below, Rules 2, 3, and 4 in *Tallinn Manual 2.0* are clear about the applicability of sovereignty to cyberspace. In accordance to what Rule 2 states, a "state enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."[46] As Rule 3 provides, a "state is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding to it"[47] As Rule 4 indicates, "a state must not conduct cyber operations that violate the sovereignty of another state."[48]

The debate here is how a state, being a territorial entity, can exercise its traditionally structured sovereignty in a non-regional borderless area.[49] Considering the activities contravening the non-intervention principle as a violation of the sovereignty principle in itself, the principle of non-intervention and its implementation can be recognized as the answer to this question.

B. State Jurisdiction and Territoriality of International Law

Jurisdiction as a principle of international law refers to "the competence of a state to govern matters on its territory and provides the link between the sovereign government and its territory, and ultimately its people… [Which directly relates to] making, adjudicating, interpreting, and enforcing the law as well as rule making"[50] and

43 Moynihan (n 11), pp. 11–12.

44 Von Heinegg (n 5), p. 9.

45 Nicholas Tsagourias (n 11), pp. 19–24.

46 Schmitt (n 24), pp. 13–16.

47 *Ibid*, pp. 16–17.

48 *Ibid*, pp. 17–27

49 E. Yılmaz (n 8), p. 24.

50 C. Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2019 [2008]), p. 5; J. Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th ed., 2012), p. 448.

derives from the principle of sovereignty. As discussed above, because sovereignty is predominantly territorial under international law, the traditional approach regarding the basis of jurisdiction is also reinforced by the principles of territoriality, non-intervention, and state consent, which represent a clear manifestation of sovereign authority.[51] Overall, these principles restrict the power of a state to its own territories and prevents states from enforcing their jurisdiction within the territory of other states without the latter's consent.[52]

The exercise of power by any state violating any other state's sovereignty will most likely result in conflicts. Because jurisdiction under international law aims at preventing these kinds of conflicts, public international law has developed principles to be used as the justification for state jurisdiction regarding issues in their territories. States mostly link the matter to their territory "by means of connecting factors."[53] Thus in principle and under international law, as written in Rule 9 in *Tallinn Manual 2.0* "Every state is entitled to exercise three forms of jurisdictional competence (prescriptive, enforcement, and judicial) over persons and objects located on its territory, as well as conduct occurring there." According to the same rule and referring to the scope of this study, "A sovereign state may exercise territorial jurisdiction over cyber infrastructure and persons engaged in cyber activities on its territory; cyber activities originating or being completed in its territory, or cyber activities having a substantial effect on its territory."

In recent times, however, the territorial model of jurisdiction has become inadequate for managing the challenges caused by ever-increasing cross-border transnational cyber activities (e.g., cloud computing as the leading one among others). Cloud computing means "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself."[54] This leads to the possibility that significant portions of personal data could be stored in remote data-centers and has become the favored way of data storage in the age of contemporary computing practices. In this sense, cloud computing provides an opportunity to explore the idea of a "new spatiality"[55] and presents an interesting case challenging the current state-centric global order and traditional understanding of a number of legislative issues involving the territoriality of jurisdiction. Technological developments related to cloud computing have had at least two main impacts relevant to scope of this paper. First, service providers may store their data on networks where their servers are

51 Crawford (n 50), pp. 456, 479.

52 S. Allen, "Enforcing Criminal Jurisdiction in the Clouds and International Law's Enduring Commitment to Territoriality" in S. Allen, D. Costelloe, M. Fitzmaurice, P. Gragl, & E. Guntrip (Eds.), *The Oxford Handbook of Jurisdiction in International Law* (Oxford University Press, 2019), p. 4.

53 J. Hörnle, *Internet Jurisdiction - Law and Practice* (Oxford University Press, 1st ed., 2019), p. 5.

54 Allen (n 52), p. 6.

55 G. Dannat, *How Cloud Computing Complicates the Jurisdiction of State Law* (E-International Relations, 14 September 2012). Retrieved from https://www.e-ir.info/2012/09/14/how-cloud-computing-complicates-the-jurisdiction-of-state-law/

located in a different jurisdiction than that of the relevant data owner. Secondly, cloud computing systems makes setting up the national setting difficult for any particular datum stored in the cloud of any given service provider.[56]

Significance is had in acknowledging that, despite its considerable advantages for users and service providers, cloud computing creates uncertainties about states' jurisdiction powers. The nature of cloud computing and data storage involving cross-border data transfers or data in transit through many jurisdictions has blurred national boundaries and posed several challenges for the practice of territorial jurisdiction. On the contrary, the appearance of cloud services in different jurisdictions gives rise to the emergence of a number of states attempting to claim different forms of jurisdiction over particularly specified cyber activities. Thus, applying territoriality on a strictly conventional basis has also become difficult. Under these conditions, problems related to online activities and remote data storage, as well as the complex nature of cyber activities, have necessitated global cooperation to evaluate the viability of maintaining a territorial conception of jurisdiction in "digital settings and, especially, cloud environments."[57] The results of these efforts will show how flexible and successful international law is in adapting itself to changing conditions.

As stated in the above sections, another principle underpinning the traditional territorial approach to jurisdiction is non-intervention and is discussed in the following section.

C. The Principle of Non-Intervention in Cyber-Space

The non-intervention principle as a reflection of sovereignty signifies each state's claim to its territorial integrity and political independence. As a corollary to sovereignty and sovereign equality, the prohibition of intervention has long been recognized in political and legal circles, despite its definitional ambiguity and conceptual uncertainty. In compliance with the 1970 Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the UN, "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of another State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law."[58] In addition, the Court of International Justice recognizes this as part of customary international law.

56 Allen (n 52), pp. 9–10.

57 *Ibid*, pp. 5–6.

58 For the full text, see: https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/348/90/pdf/NR034890.pdf?OpenElement

The above statements show the principle of non-intervention to exist and to prohibit "action attributable to a state involving 'methods of coercion' regarding the internal or external affairs of a state."[59] This state of affairs has been carried over into the cyber context by *Tallinn Manual 2.0.* The manual discusses the prohibition of intervention regarding two separate rules: Rule 66 (i.e., Intervention by States) and Rule 67 (i.e., Intervention by the UN). Rule 66 states that "a state may not intervene, including by cyber means, in the internal or external affairs of another State."[60]

According to the conventional understanding, a violation of the territorial sovereignty of any state is naturally linked to the physical intrusion into the territory of a state, irrespective of whether this occurs by land, sea, or air. Although cyberspace interactions are often de-territorialized, cyberspace and its three intertwined layers (as mentioned in the previous sections) are encapsulated in the principles of sovereignty and non-intervention. Furthermore, the principle of non-intervention clearly codified in international legal documents as well as agreements prohibits a state from intervening within another state's sovereign territories and causing damages to their activities, including those in and from cyberspace.

V. Conclusion

The increasing use of technology since the 1990s has made cyberspace a new area of operation for members of the international community. Thus, cyberspace has become increasingly subjected to complicated, large-scale, state-led operations. Just as cyberspace has made very important contributions to the history of human development, many harmful incidents have also originated from this arena. Critical national infrastructure has become vulnerable to cyber-attacks. International stability may be endangered by cyber wars or cyber conflicts. International economics may be threatened by cybercrime and cyber espionage, and individuals are being terrorized by hackers. In order to overcome those challenges, an open, safe, stable, accessible, and peaceful cyberspace is needed for all. Consequently, the international community has been taking steps in various multi-lateral and multi-stakeholder platforms.

Cyberspace opens up a host of new legal questions, and states, legal experts, and business actors have been discussing and focusing on the issue of how to regulate cyberspace through international law since the mid-1990s. The starting point of these debates places state sovereignty as the basis of international law giving jurisdiction to states. However, due to the relatively new nature of cyber actions and activities, a binding and universal legal order and system has so far not been established. The

59 D. B. Hollies, "From Corollaries to Contents? Elaborating the Principle of Non-intervention in Cyberspace," in F. Delerue & A. Géry (Eds.) *International Law and Cybersecurity Governance* (European Union Institute for Security Studies, 2022), p. 52.

60 Schmitt (n 24), pp. 312–325.

complex structure of the issue prevents the establishment of binding rules in the international arena. Due to the voluntariness of current rules and non-existence of a binding mechanism to supervise them, their application and implementation are mostly subject to the political will of each state.

The view is that states should have an active role in the creation of international legal rules in accordance with the concepts of cyberspace. Development in this field is only possible through interstate cooperation, and this is a burgeoning area of law. Although a need exists for new approaches to existing problem, *Tallinn Manuals 1.0* and *2.0* appear to provide the basis and starting point for further laws and regulations regarding cyberspace. As the manuals show, a sovereignty redux definitely occurs in cyberspace, along with the continuing disputes about its scope and content. Because these are the states of the international society that make international law and are responsible for this uncertainty, they again have the power and capacity to reduce this uncertainty and clarify the legal understanding. The successful implementation of international law in cyberspace will depend on minimizing the disagreements among members of the international community.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Financial Disclosure: The author declared that this study has received no financial support.

Bibliography

Allen S, 'Enforcing Criminal Jurisdiction in the Clouds and International Law's

Enduring Commitment to Territoriality' in S Allen, D Costelloe, M Fitzmaurice, P Gragl, and E Guntrip (eds) *The Oxford Handbook of Jurisdiction in International Law* (Oxford University Press, 2019) 1-35.

Betz D J and Stevens T, *Cyberspace and the State: Toward a Strategy for Cyber Power* (first published, Routledge, 2011).

Buchan R, *Cyber Espionage and International Law* (first published 2018, Hart Publishing, 2019).

Carr M, *US Power and the Internet in International Relations: The Irony of the Information Age* (first published, Palgrave Macmillan 2016).

Couture S and Toupin S, 'What Does the Notion "Sovereignty" Mean When Referring to the Digital' (2019) 21(10) *New Media & Society* 1-18.

Crawford J, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th edition, 2012).

Dannat G, 'How Cloud Computing Complicates the Jurisdiction of State Law' (*E-International Relations*, 14 September 2012) < https://www.e-ir.info/2012/09/14/how-cloud-computing-complicates-the-jurisdiction-of-state-law/> accessed 8 September 2023.

Deibert R J and Rohozinski R, 'Risking Security: Policies and Paradoxes of Cyberspace Security' (2010) 4(1), *International Political Sociology* 15-32.

Demchak C C and Dombrowski P, 'Rise of a Cybered Westphalian Age' (2011) 5(1) *Strategic Studies Quarterly* 32-61.

Ecemiş Yılmaz H K, 'Siber Uzay, Siber Güvenlik, Dijital Egemenlik Kavramlarının Uluslararası Hukuk Bağlamında Değerlendirilmesi' (2021) 12(9) *ULİSA- Mühendislik, Hukuk, İletişim ve İktisat Perspektifinden Siber Güvenlik ve Sosyal Medya* 21-26.

Franzese P W, 'Sovereignty in Cyberspace: Can It Exist?' (2009) 64 *Air Force Law Review* 1-42.

Gibson W, *Neuromancer* (first published, Ace 1984).

Gourley S K, 'Cyber Sovereignty' in P A Yannakogeorgos and A B Lowther (eds) *Conflict and Cooperation in Cyberspace: The Challenge to National Security* (Taylor & Francis, 2014) 277-290.

Güntay V, '21. Yüzyıl Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk' (2019) 1(2) *Novus Orbis Journal of Politics and International Relations* 87-109.

Haataja S, 'Cyber Operations against Critical Infrastructure Under Norms of Responsible State Behaviour and International Law' (2022) 30(4) *International Journal of Law and Information Technology* 423-443.

Hassan D, 'The Rise of the Territorial State and the Treaty of Westphalia' in G M (ed) *Yearbook of New Zealand Jurisprudence* (University of Waikato School of Law, 2006) 62-70.

Herrera G L, 'Cyberspace and Sovereignty: Thoughts of Physical Space and Digital Space', in M D Cavelty, V Maurer and S F Krishna-Hensel (eds) *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (Ashgate, 2007) 67-93.

Hollis D B, 'A Brief Primer on International Law and Cyberspace' (*Carneige Endowment for International Peace*, June 2021) <https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763> accessed 26 June 2023.

Hollis D B, 'From Corollaries to Contents? Elaborating the Principle of Non-intervention in Cyberspace' in F Delerue and A Géry (eds) *International Law and Cybersecurity Governance* (European Union Institute for Security Studies, 2022) 51-58.

Hörnle J, *Internet Jurisdiction - Law and Practice* (Oxford University Press, 1st edn, 2019).

Janssens P C and Wouters J, 'Informal International Law-Making: A Way Around the Deadlock of International Humanitarian Law?' (2022) 104(920-921) *International Review of the Red Cross*, 2111-2130.

Karadağ Ş, 'Siber Uzayda Uluslararası Hukuk Mümkün Mü?' (2019) 5(36) *International Social Sciences Studies Journal* 2827-2833.

Kello L, 'The Meaning of the Cyber Revolution' (2013) 38(2) *International Security* 7-40.

Keohane R O and Nye J S, 'Power and Interdependence in the Information Age' (1998) 77(5), *Foreign Affairs* 81–94.

Kshetri N, 'Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations' (2013) 13(1) *Electronic Commerce Research* 41-69.

Kuehl D T, 'From Cyberspace to Cyberpower: Defining the Problem' in F D Kramer, S H Starr and L K Wentz (eds), *Cyberpower and National Security* (National Defense University Press, 2009) 24-42.

Lan T and Xin Z, 'Can Cyber Deterrence Work?' in A Nagorski (ed), *Global Cyber Deterrence: Views From China, The U.S., Russia, India, and Norway* (East-West Institute, 2010) 1-2.

Liarapoulos A, 'Power and Security in Cyberspace: Implications for the Westphalian State System' Panorama of Global Security Environment (*Bratislava: Centre for European and North American Affairs*, 2011) 541-549.

Libicki M C, *Cyberdeterrence and Cyberwar* (*RAND Corporation*, 2009) <https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf> accessed 30 April 2023.

Maurer T, 'Cyber Norm Emergence at the United Nations - An Analysis of the UN's Activities Regarding Cyber-security' (*Belfer Center for Science and International Affairs Discussion Paper*, 2011-11) <https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf> accessed 15 July 2023.

Moynihan H, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention' (*Chatham House*, December 2019) <https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks> accessed 1 July 2023.

Nye J S, 'Cyber Power' (*Harvard Kennedy School, Belfer Center for Science and International Affairs*, May 2010) <https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf> accessed 15 April 2023.

Nye J S, *The Future of Power* (first published, PublicAffairs, 2011).

Nye J S, 'The Regime Complex for Managing Global Cyber Activities' (*The Global Commission on Internet Governance and Chatham House*, May 2014) <https://www.cigionline.org/static/documents/gcig_paper_no1.pdf> accessed 15 April 2023

Pauwelyn J, "Informal International Lawmaking: Framing the Concept and Research Questions", in J Pauwelyn, R A Wessel and J Wouters (eds), *Informal International Law-Making (Oxford University Press,* 2014) 13-34

Rauscher K F, 'First Joint Russian-U.S. report on Cyber Conflict' (*EastWest Institute*, 2011) <https://www.eastwest.ngo/idea/towards-rules-governing-cyber-conflict-0> accessed 15 April 2023.

Ryngaert C, *Jurisdiction in International Law* (first published 2008, Oxford University Press, 2019) 5.

Schmitt M N, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed' (2013) 54(5) *Harvard International Law Journal Online* 13-37<https://harvardilj.org/2012/12/online-articles-online_54_schmitt/> 31 accessed 15 July 2023.

Schmitt M. N. (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (first published, Cambridge University Press, 2017).

Singer P W and Friedman A, 'Cult of the Cyber Offensive' (2014) *Foreign Policy* 182 <http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/> accessed 15 July 2023.

Sönmezoğlu F, *Uluslararası Politika ve Dış Politika Analizi* (first published, Filiz Kitabevi 2000).

Tiirmaa-Klaar H, 'Botnets, Cybercrime and National Security' in H Tiirmaa-Klaar, J Gassen, E Gerhards-Padilla and P Martini (eds) *Springer Briefs in Cyber Security – Botnets* (Springer, 2013) 1-40.

Tsagourias N, 'Law, Borders and the Territorialisation of Cyberspace', (2018) 15(4) *Indonesian Journal of International Law* 523-551.

Tsagourias N, The Legal Status of Cyberspace: Sovereignty Redux?,' in N Tsagourias and R

Buchan (eds) *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2021) 9-31.

von Heinegg W H, 'Legal Implications of Territorial Sovereignty in Cyberspace' (Proceedings of 2012 4th International Conference on Cyber Conflict - NATO CCD COE Publications, 2012) 7-19 <https://www.ccdcoe.org/uploads/2012/01/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf> accessed 4 May 2023.

Waltz E, *Information Warfare: Principles and Operations* (first published 1998, Artech House 1998).

Wu T H, 'Cyberspace Sovereignty? The Internet and the International System' (1997) 10(3) *Harvard Journal of Law & Technology* 647-666.

Ziolkowski K, 'Confidence Building Measures for Cyberspace' in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace - International Law, International Relations and Diplomacy* (NATO CCD COE Publication, 2013).