Cybersecurity and International Law: Are We Where We Should Be?

Jacques KABANO*

ABSTRACT

The Council of Europe in 2001 established the *Convention on Cybercrime*. Although this Convention received mixed criticism, it remains the only convention with an international dimension on cybersecurity. Due to the virtual nature of cyberspace, we often fail to link it to the outside world and pretend it always remains virtual. However, many cyberattacks proved to have reached the physical world and left warning signs.

The law is both a witness and an instrument of the relationship between individuals and their society. Therefore, the question of knowing what becomes of that relationship in a networked society is, in part, a question of what is the law in an environment like cyberspace. In cyberspace, the interactions between internet users are not limited to domestic laws. International law appears as an answer to the transnational nature of cybersecurity issues. If the risks raised by cybercrime on the economy had already been identified for a long time, the perception of a risk weighing more particularly on the security of states should also be identified and be resolved at once. Although incorporating the rules of International Humanitarian Law (IHL) into cyber warfare seems helpful, the existing IHL rules cannot cover all tricky aspects of cyber warfare. It is still not easy to arrive at an international consensus on cybersecurity matters such as cyber attributions, cyber sovereignty, the definition of cyber-attacks, and ways to respond to those attacks.

This paper examines why it is challenging to regulate cyberspace, existing ways to deal with cybersecurity issues, and analyzes whether a completely new convention on cybersecurity would resolve this matter.

Keywords: Cybersecurity, Cybercrime, Cyber Warfare, International Law, Cyber Sovereignty, Cyber-attack

I. INTRODUCTION

*Ankara University, Graduate School of Social Sciences, Department of Public Law, Ph.D. Candidate. E-mail: Kabano@ankara.edu.tr, jakatuholy18@gmail.com ORCID: https://orcid.org/0000-0002-0248-9204

From a remarkably humble beginning[1] to the current situation[2], nothing beats the internet when it comes to accessing information and easing communication. Internet users created a virtual world with no geographical delimitation which, in turn, created a challenge to domestic legislation. An adage says: '*where there is a society, there is a law'*[3] the internet should not be an exception since it became a crucial element in a global society. The internet is undoubtedly today one of the objects and one of the vectors of *internationalization*[4] *and globalization*[5]; therefore, the law, applicable to the internet, must or should necessarily have an international dimension. This is where appears, if not the novelty, at least the main difficulty. The current insufficiency and failures of international law, due to the voluntary commitment and participation of states, are replicated for international law in cyberspace. The main problem for international law comes when a cyber operation from one state affects another state's sovereignty[6]. In this situation, international law should offer solutions to stabilize this unstable environment. However, it is necessary to go through the interpretation and the concrete implementation of this legal corpus.[7] Critically analyzing the applicability of international law to cybersecurity issues, this paper focuses on two main points; the challenges facing the regulation of cyberspace and plausible mechanisms to deal with cyberconflicts, which includes establishing a new cybersecurity convention.

---

[1] Domenico Ferrari, 'Humble beginnings, uncertain end: getting the internet to provide performance guarantees' (2006) 36(4) ACM SIGCOMM Computer Communication Review1, 1-2

[2] In this paper, the "current "situation, … means existing internet technologies, see for example: internet technologies overview, at http://user.engineering.uiowa.edu/~ie181/Documents/Section1-Text.pdf accessed 25 January 2022.

[3] Aaron X. Fellmeth and Maurice Horwitz, *Guide to Latin in International Law* (Oxford University Press, 2011) 102.

[4] Shane Mathews &Marilyn Healy, '"From garage to global" The Internet's influence on international market growth An Australian SME perspective', International Council for Small Business, 51st World Conference – June 2006, p.2 https://eprints.qut.edu.au/7209/2/7209.pdf.

[5] Dody Budi Waluyo, 'Globalization and deglobalization: the Indonesian perspective', in BIS papers No 100, *Bank for International Settlements 2018, p. 177 https://www.bis.org/publ/bppdf/bispap100.pdf*

[6] The sovereignty, means independence of states, the ability not to have the will of other states imposed on them, and freedom of internal organization. (Kabano, J. "CONQUEST OVER CYBERSPACE: AN UNLIMITED SOVEREIGNTY?". Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 18 (2021): 117-139)

[7] John K. Gamble, 'International Law and the Information Age' (1996) 17(3) Michigan Journal of International Law, 748-751

II. CHALLENGES BEHIND REGULATING CYBERSPACE

Like any other field of Law, regulating cyberspace requires the normative condition of whether governing this field will result in a desirable outcome. It is crucial to understand the methods of emergence and application of the normativity[8] that prevails there.

a. A New Concept of Sovereignty

For an open space like the internet, it appears unlikely that the same rules would be operational throughout the network because every country has its own internet infrastructures and imposes its own rules. The notion of sovereignty in cyberspace brings new epistemological difficulties.[9] It is indeed difficult to conceive of state sovereignty in a dematerialized space, but state sovereignty serves as a superstructure for a vast set of human activities that take place at the local level.[10]

In cyberspace, it is still not clear who is the real sovereign entity. Some writers[11] claim that users, consumers, companies, and states share the governance of the internet. Others[12] suggest that there should be a straight distinction between the regulation of the internet and its political and legal aspects, and its management, which involves its technical side. Technical limitations always affect any legal or political decisions because they usually rely on the available technology to establish such decisions.[13] Therefore, the beginning of cyberspace translated into a shift in sovereignty[14]because a new space in which states and internet users

---

[8] Sylvie Delacroix, *Legal norms and normativity: an essay in genealogy* (Oxford: Hart Publishing, 2006) 9

[9] Cynthia E. Ayers, 'Rethinking Sovereignty in The Context of Cyberspace (U.S. Army War College-The Cyber Sovereignty Workshop Series, 2016) 12-14 https://csl.armywarcollege.edu/usacsl/Publications/Rethinking%20sovereignty.pdf accessed 2 February 2021

[10] Hao Yeli, 'A Three-Perspective Theory of Cyber Sovereignty' (2017) 7 (2) Prism109, 109-115 https://cco.ndu.edu/Portals/96/Documents/prism/prism_7-2/prism_7-2.pdf accessed 20 December 2020

[11] Henning Lahmann, Philipp Otto, Valie Djordjevic, and Ana Maire, *who governs the internet? Players and fields of action (*Abteilung Politische Akademie, 2017) 6-26.

[12] Antonio Seguro Serrano, 'Internet Regulation and The Role of International Law' (2006) 10 Max Plank Yearbook of United Nation Law, 197-199

[13] Farid GUEHAM, *Digital Sovereignty – Steps Towards A New System of Internet Governance (*The Fondation pour l'innovation politique, 2017)11-15. http://www.fondapol.org/en/etudes-en/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/ accessed 20 December 2020

[14] Samuel Woodhams, 'The Rise of Internet Sovereignty and the End of the World Wide Web?' (In Opinion, 23 April 2019) https://theglobepost.com/2019/04/23/internet-sovereignty/ accessed 27 December 2020

exercise their control appeared. The state[15] loses some parts of its sovereign power to the users and the networks that make this virtual space.[16]

b. New Forms of Standards

The decentralized organization of the internet makes it necessary to think of regulation according to paradigms, different from those commanded by the teachings prevalent in most legal communities. The difficulties that have arisen in applying the law to cyberspace call for the dilapidation of legal formalism and encourage a legal framework that seeks to support solutions rather than being confined solely to the laws considered dogmatic. The law has its rationality. The changes brought about by cyberspace are causing mutations in the rationality underlying several rules of law. Additionally, the debates around the rationality that should justify the law or the elimination of law crystallize around the search for appropriate metaphors to name new applications in cyberspace.[17]

Behind every corpus of rules are the principles, values, and interests that underpin their legitimacy.[18] Often, the law is the result of a decision that reconciles different interests and values. The legal framework of activity reflects values from which requests arise to frame certain aspects. This is what constitutes rationality of laws.[19] When it aims to contribute to the implementation of policies, the legal framework is dependent on the values, often contradictory, that societies try to reflect. Therefore, there is no analysis of any legal framework by ignoring these values. When values form the basis of law, the values are charged with meaning and legal consequences. Understanding the law dimensions of a phenomenon like cyberspace requires knowledge of the issues related to the rationality envisaged.[20] To know the law dimensions of a phenomenon requires

---

[15] In this paper, a State means an independent country, like Turkey, Germany, USA, Japan, Rwanda etc.

[16] Johnson, David R., and David Post. "Law and Borders: The Rise of Law in Cyberspace." *Stanford Law Review* 48, no. 5 (1996): 1370. Accessed May 26, 2021. doi:10.2307/1229390.

[17] Eneken Tikk-Ringas, 'International Cyber Norms Dialogue as an Exercise of Normative Power' (2016) 17(3) Georgetown Journal of International Affairs 47, 48

[18] Stryker Robin, 'Rules, Resources, and Legitimacy Processes: Some Implications for Social Conflict, Order, and Change' (1994) 99 (4) *American Journal of Sociology,* 847-49 https://www.jstor.org/stable/2781734 accessed 2 February 2021.

[19] Robert Hébert, 'C. Atias, *Savoir des juges et savoir des juristes. Mes premiers regards sur la culture juridique québécoise, Montréal, Centre de recherche en Droit privé et comparé du Québec,* 1990' (1992) 19 (1) Philosophiques, 123-129 https://www.erudit.org/fr/revues/philoso/1992-v19-n1-philoso1794/027176ar.pdf accessed 27 December 2020.

[20] Mark Leiser, 'The problem with 'dots': questioning the role of rationality in the online environment' (2016) 30(3) International Review of Law, Computers & Technology,191-

understanding the reasons for the adopting the law and making it rational.[21]Cyberspace offers a representation of media environments defying executives derived from national borders. Regulatory regimes for electronic media stand on the premise that a state can determine what is lawful to broadcast. However, the configuration of cyberspace locates the determination of what to or not communicate at the individual level; this capacity to configure cyberspace disqualifies, even illegitimates the state as a central player in the regulation, and supports a shared governance. Therefore, rationality attached to cybersecurity and the illustration of national creativity experience a crisis of legitimacy.

c. New Changes in the Expression of Rules

The activities of states and private actors online are the origin of emerging diversified available rules in cyberspace.[22] Several rules prevailing on the Internet are often part of regulatory processes aimed at producing coordination.[23] Coordination regulation[24] is one that facilitates an activity that without it would be almost impossible. In the Internet universe, regulating domain names aims at ensuring the necessary coordination to make communication possible.[25] The increase in the numbers of Internet users and diversification of activities that take place on the internet; helps to reduce the number of questions that are simple coordination questions. The challenges facing Internet users increasingly consist of subjects and issues of varying scopes and meanings within the cultural universes to which they belong.[26] That is why it is becoming increasingly difficult to expect the internet to respond to simple standards.

210, https://www.tandfonline.com/doi/full/10.1080/13600869.2016.1145952 accessed 15 January 2021.

[21] Phillipe Jestaz, Le *droit* (2nd Edition, Dalloz, Paris, 1992)267

[22] Developments in the Law: The Law of Cyberspace." *Harvard Law Review* 112, no. 7 (1999): 1574-704. Accessed May 27, 2021. doi:10.2307/1342414.

[23] Hofmann Jeanette, Christian Katzenbach, and Kirsten Gollatz, 'Between Coordination and Regulation: Finding the Governance in Internet Governance.' (2017) 19 (9) New Media & Society 1, 8-10.

[24] Ibid.

[25] OECD, 'Internet Domain Names: Allocation Policies' (OECD Digital Economy Papers, No. 30, OECD Publishing, Paris, 1997), http://dx.doi.org/10.1787/237020717074 accessed 15 January 2021.

[26] Scots in United Kingdom and Catalans in Spain, are good examples of people who want to own their own cultural and linguistic features without being collectively homogenized as one (UK and Spain), and constantly demand to be acknowledged within internet community as well as nations. (Combi M. (2016) Cultures and Technology: An Analysis of Some of the Changes in Progress—Digital, Global and Local Culture. In: Borowiecki K., Forbes N., Fresa A. (eds) Cultural Heritage in a Changing World. Springer, Cham. https://doi.org/10.1007/978-3-319-29544-2_1)

When there is a consensus on the subject matter, it is relatively easy to state the rules using terms with specific content. The usual principles of interpretation of legal texts require that we rely on the ordinary meaning of words.[27] It means the interpreters limit themselves to a written context. The text of the law or regulation makes it possible to discover the general object of legislative communications and controls the range of meanings that the interpreter can give to the text.[28] Electronic environments bring together players from diverse cultural backgrounds. The levels of consensus and the frames of reference used in their national cultural spaces are no longer necessarily operational in virtual space.[29]

d. **A New Distribution of Roles Between Sources of Normativity**

The characteristic features of cyberspace, mainly those which make state regulation appear less realistic, favor an increase in the relative weight of other sources of normativity.[30] Several authors have stressed the limits of state law in cyberspace.[31] Trotter Hardy noted that laws are just one possible answer to problems in cyberspace.[32] The adjudication on a case-by-case basis and the gradual construction of rules which result from it, the contracts, the customs that people may follow, the rules implemented by the networks, and even a certain degree of anarchy may prove more appropriate to govern behavior on the Internet.[33]

---

[27] Solan Lawrence M. and Gales Tammy, 'Finding Ordinary Meaning in Law: The Judge, the Dictionary or the Corpus?' (2016), The International Journal of Legal Discourse, Forthcoming, Brooklyn Law School, Legal Studies Paper No. 474, https://ssrn.com/abstract=2850703 accessed 29 December 2020.

[28] William N. Eskridge, Book Review: The New Textualism and Normative Canons Reading Law: The Interpretation of Legal Texts, Antonin Scalia and Bryan A. Garner. St. Paul: West, 2012, Columbia Law Review, [Vol. 113:531], p. 532-533.

[29] Jörg Roche and Leah P. Macfadyen and Sabine Doff, Communicating *across Cultures in Cyberspace: A Bibliographical Review of Intercultural Communication Online* (LIT Verlag, Annotated edition, 2004) 14-15.

[30] Dan Hunter, 'Cyberspace as Place and the Tragedy of the Digital Anticommons' (2003) 91 (2) California Law Review 439, 443.

[31] Johnson David R., and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review*1367, 1370–76. *JSTOR*, www.jstor.org/stable/1229390 Accessed 2 Feb. 2021; Jean-Baptiste Maillart, 'The limits of subjective territorial jurisdiction in the context of cybercrime' (2019) 19 *ERA Forum* 375–390 https://doi.org/10.1007/s12027-018-0527-2 accessed 25 January 2021.

[32] Trotter Hardy, 'The Proper Legal Regime for 'Cyberspace' (1994) 55 University of Pittsburgh Law Review 993,1025.

[33] Milton Mueller, *Sovereignty and Cyberspace: Institutions and Internet governance*, essay derived from the 5th Annual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana 3 October 2018.

Cyberspace is certainly not the only environment whose regulation results from the synergy of technical architecture, social standards, self-regulation, and the law.[34] Outer space generally responds to such a description. The comparative analysis of these two spaces appears both legitimate and particularly instructive in the context of a prospective approach. As with outer space, cyberspace will have to encompass, according to Anna Maria Balsano, distinct branches of law such as intellectual property law, criminal law, administrative law, and be inspired by experience gained in the development of legal standards for outer space activities.[35] However, the features cyberspace presents modify the distribution that prevails between these different sources of normativity.[36] Because regardless of the system of governance, a Cybernorm (a norm that governs behavior in cyberspace) is thought to be dangerous when enforcing restrictions, such as laws and policies, and equally vital when supporting informal restrictions inherent to a self-regulatory system.[37]

Technical architecture means all technical elements or artifacts, such as hardware, software, standards, and configurations that determine access to and rights to use cyberspace resources.[38] These rules governing the flow of information, imposed by communication networks and technology, play a significant role in regulating an increasing number of activities. Technical objects have a regulatory effect in various forms. First, architectural elements can be software, such as firewalls or proxy

---

[34] Monroe Price and Stefaan Verhulst, 'The Concept of Self-Regulation and the Internet' In J. Waltermann & M. Machill (Eds.), *Protecting our children on the internet: Towards a new culture of responsibility* (Bertelsmann Foundation Publishers, 2000) 133-198

[35] Anna Maria Balsano's article, " *An International Legal Instrument for Cyberspace? A Comparative Analysis with the Law of Outer Space (2000)* "is part of this logic. Recalling initially the legal nature of outer space, its genesis (in the 1950s), and its development through the five major treaties concluded within the framework of the United Nations, Anna Maria Balsano in recalls the different elements: right of use (but not of appropriation), obligation of use for peaceful purposes, State responsibility for private activities (and monitoring of its activities), registration of objects launched into space, conservation jurisdiction and control, liability for damage caused and, finally, application of international law.

[36] April Mara Major, *Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution*, 78 WASH. U. L. Q. 59 (2000). https://core.ac.uk/download/pdf/233173015.pdf Accessed 27 May 2021.

[37] Mara Major, 2000, p. 60.

[38] Jeremy Faircloth, *Enterprise Applications Administration* (Morgan Kaufmann, 2014) 1-26.

servers.[39] Some states[40] use such resources to control the circulation of content from abroad on their national Internet networks. Second, the masters of the networks implement the architecture.[41] The choice of its characteristics, of what it allows or prohibits, is an act of regulation, even law.[42] That is why, in various ways, architecture constitutes a component of the legal framework for activities taking place in cyberspace.[43]

Several works have highlighted the substantial role of technical architecture in controlling the activities taking place in cyberspace.[44] The political dimension of technical objects is one of the fields of study of sociologists of science, like Langdon Winner.[45] His work outlines the framework of a new approach to regulating technology that would take into account and take advantage of its technical architecture. The examination of the legal dimension of this technical architecture helps researchers to work on its normative difficulties.

The practice observed on the Internet reveals the main models of self-regulation prevailing there.[46] Thus, those who have control of a place (website) have the possibility of adopting policies relating to access to the site, accepted behavior, and prohibited acts on the site. Although these policies are similar in form and structure all over the internet, they are different from each other by their more or less restrictive nature. The expression 'Acceptable Use Policies'[47] constitutes standards that the user must follow to maintain access to a given network. There are different types of standards of conduct practiced in the various networks that make the Internet.

To understand the law in a place like cyberspace where physical borders no longer make sense requires situating the foundations of normativity on

---

[39] Solum Lawrence B. and Chung Minn, 'The Layers Principle: Internet Architecture and the Law' (SSRN, 2003), https://ssrn.com/abstract=416263 accessed 26 January 2021.

[40] Internet Society, 'The Internet and extra-territorial effects of laws' (Internet Society Concept Note, 2018) https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws-EN.pdf accessed 26 January 2021.

[41] Solum Lawrence B. and Chung Minn, 2003.
[42] Solum Lawrence B. and Chung Minn, 2003.

[43] Solum Lawrence B. and Chung Minn, 2003.
[44] Solum Lawrence B. and Chung Minn, 2003.
[45] Langdon Winner, 'Do Artifacts Have Politics?' (1980) 121 (1) *Daedalus* 109, 121-36. https://www.jstor.org/stable/20024652 accessed 29 December 2020.
[46] Price and Verhulst (n24) 137-8.
[47] Christensson Per, 'AUP Definition' TechTerms (January 16, 2014) https://techterms.com/definition/aup accessed 30 January 2021.

the internet.[48] Knowing how and where to situate these foundations helps to determine the state that will implement them. Normative foundations do not rest at the lines of the political borders but at the lines between the networks, which are the absolute constituent units of cyberspace.[49]

In cyberspace, the expression of the law uses techniques that transcend the national laws.[50] Far from being downgraded, state law is a component of a regulatory process resulting from synergies between various normative sources.[51] These sources come from the technical architecture, which makes cyberspace what it is, contractual practices, and self-regulation put in place by the players. It is through this kind of regulation that the law gives the ideal adjustments and protections. As it may be understood, dominating the normativity of the internet is a condition for its progress. It is about users who hold a portion of sovereign power on the internet. From this viewpoint, normativity challenges public and private approaches to self-regulation of cyberspace, and the test here is to promise normativity on the internet will reflect values predictable with human rights and social diversity.

III. ARE WE WHERE WE SHOULD BE IN DEALING WITH CYBERSECURITY ISSUES?

A cybernetic arms race is happening.[52] The deployment of cybernetic weapons is now an extension of state power.[53] The United States has set up a cyber command authority, equipped with defense tools and cyber-

[48] Von Matthias C. Kettemann, *The Normative Order of the Internet*, Normative Orders Working Paper 01/2020, https://www.hiig.de/wp-content/uploads/2020/06/Matthias-Kettemann_The_Normative_Order_of_the_Internet-1.pdf accessed 27 May 2021.

[49] Von Matthias C. Kettemann, 2020, p. 3-4.

[50] Johnson David R., and David Post (n22) 1378–81.

[51] George E. Glos, 'The Normative Theory of Law' (1969) 11(1) William & Mary Law Review, 173 https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=2772&context=wmlr accessed 27 January 2021.

[52] Arpagian Nicolas, *La cybersécurité (*Presses Universitaires de France, « Que sais-je ? », 2010) 23-27.

[53] Public-Private Analytic Exchange Program, Commodification of Cyber Capabilities: A Grand Cyber Arm Bazaar, 2019, p. 2 https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf accessed 20 January 2022.

attacks.[54] A similar escalation is taking place in China and Russia, as well as in many other countries.[55]

By strictly applying international law to relations between States in the context of cyber operations, a sovereign state is responsible for the cyberinfrastructures on its territory, which means that it can prosecute the authors before its courts.[56] It is necessary to clearly distinguish between agreements of good conduct, official speeches linked to political and diplomatic issues from what is currently binding in terms of international law. Recalling that treaties and international agreements become binding only once ratified. There are real fundamental differences regarding the vision of States in the search for their cybersecurity. However, each State develops its defense policy and its national strategies by referring to its legislation. States define their needs, expectations, the types of threats to which they are subject, and the means to protect themselves, repair, and prevent future attacks.

Before examining whether we are where we should be regarding these cybersecurity issues, it is important to first examine what has been achieved so far:

a. Tallinn Manual

About 20 international legal experts whose nationalities are representative of NATO member nations, attempted the first analysis of the interpretation of international law norms against cybernetic attacks.[57] By relying on pre-existing international law, particularly in international humanitarian law (for space, sea, and air), some rules were linked analogously to digital activities.[58] Their work[59], which is not official and not representative of the whole global community, appears to be the best interpretation of international law to cybersecurity issues.

The Tallinn Manual aims to provide legal standards applicable to cyberspace. Technologies are constantly developing at a breakneck pace, and the law must evolve simultaneously to avoid any future problems for states and their actions in cyberspace. The Tallin Manual stands on three

---

[54] Edward Hunt, US Government Computer Penetration Programs and the Implications for Cyberwar, IEEE Annals of the History of Computing, the IEEE Computer Society,2012, p.4 http://courses.isi.jhu.edu/malware/papers/HUNT.pdf.

[55] Acton, James M. "Cyber Warfare & Inadvertent Escalation." *Daedalus* 149, no. 2 (2020): 133-49. Accessed May 28, 2021. https://www.jstor.org/stable/48591317.

[56] *Infra* note 57.

[57] Michael N. Schmitt, *Tallinn Manual 2.0 On the International Law of Cyber Operation: What it is and isn't,* 9 February 2017, https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/ accessed 28 May 2021.

[58] Ibid.

[59] Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare (*Cambridge University Press, New York, 2013).

main objectives: interpreting existing standards by applying them to cyber-attacks because before its establishment, there was no common interpretation of treaties for cyber operations; reconnecting computer-based techniques and legal words in their reciprocal analyses and understandings, and gauge the capacity of states to seek consensus on ethical and legal limits in cyberspace (including the meaning of an 'armed attack' and the 'use of force').

The Tallin manual therefore examines the international law norms applicable to cyber conflicts, whether international or non-international, strictly limited to cyber operations. Only cybernetic operations reaching a certain threshold are analyzed in the manual. All operations that have not reached the "degree" of use of force under the United Nations Charter (jus ad bellum) such as cybercrime or cyber espionage are not studied except in the case where such an act is directly linked to an armed conflict.[60]

The 95 rules of the manual are written with the consensus of the group of experts working for the application and interpretation of the rules of international law (lex lata) and not the practice or the political choices of a particular nation (lex feranda). Each rule is supplemented with comments providing a detailed analysis of the legal interpretations adopted. The applicable law which was therefore used for the analysis encompasses the international regulations of jus ad bellum (use of force between States) and jus in bello (the law of the conduct of hostilities, including the law of armed conflict).

b. Prevention of Cyber Crimes

At the international level, the Budapest Convention against Cybercrime of 23 November 2001, the first and only treaty of an international character, aims to harmonize the laws of the 65 signatory states[61] through modernization and international cooperation in the area of extradition and mutual law enforcement assistance. The scope of the geographic impact of cybercrimes is generally extensive. Due to this vast geographic scope of cybercrime, many states find themselves in a position to claim subjective territorial jurisdiction over a single cybercrime.[62][63]

---

[60] The example to date is the conflict between Russia and Georgia, which has been termed an international armed conflict in which cyber operations have been carried out. They fell de facto under the regime of the law of armed conflict.

[61] Council of Europe, '65 Parties to the Budapest Convention' (T-CY Committee, 2020) https://www.coe.int/en/web/cybercrime/parties-observers accessed 31 January 2021.

[62] Maillart, JB, The limits of subjective territorial jurisdiction in the context of cybercrime, *ERA Forum* **19,** 375–390 (2019). https://doi.org/10.1007/s12027-018-0527-2.

[63] Some countries like Georgia, Japan, Norway, Sweden, etc., do not respect the principle of double criminality. See more: *T-CY assessment report: The mutual legal assistance*

States are trying to provide very different responses[64], and even if European and international cooperation is starting to develop, it is still insufficient. Legislative instruments are distinctive from state to state and do not evolve in the same way. Some states have laws that make it possible to criminalize unlawful acts related to internet more or less effectively. However, some states still find themselves confronted with terrible loopholes and cannot suppress this new form of crime.[65] However, faced with an offense that has become global,[66] states should find a coordinated international response.

c. Cyberspace and National Security

The security sector unites all the structures, institutions, and individuals responsible for providing, managing, and monitoring security at the national and local levels. In cyberspace, no entity has exclusive authority and control over the entire digital space. However, the governance of cyberspace lies in the hands of a multitude of diverse actors, whose different roles and responsibilities influence political decisions and regulatory decision-making methods.[67]

Currently, many cybersecurity services are provided by private commercial entities (e.g., Red Sift (United Kingdom), Deep Instinct (New York))[68], which poses challenges for the effective application of the practices of cybersecurity governance.[69] Because of the involvement of private commercial entities, transparency is one of the aspects of good

---

provisions of the Budapest Convention on Cybercrime, Adopted by the T-CY at its 12th Plenary (2-3 December 2014), https://rm.coe.int/16802e726c.

[64] Stefan Fafinski, 'Public Policy Responses to Cybercrime' (2011) 2(3) Policy & Internet, 1-5 https://onlinelibrary.wiley.com/doi/pdf/10.2202/1944-2866.1139 accessed 28 January 2021.

[65] Okoniewski, Elissa A. "Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet." American University International Law Review 18, no. 1 (2002): 295-339. Here, the case concerned the sale of memorabilia from the Nazi Germany. In France, it is an offence to use or spread anything related to Nazis, on the other side it was stated by Yahoo (a registered company in US) that it is not a crime in the US, it is only a matter of Freedom of Expression.

[66] For example, using online platforms to spread genocide ideology should be punishable globally since the crime of genocide itself, is an international crime under customary international law.

[67] Henning Lahmann, Philipp Otto, Valie Djordjevic, and Ana Maire, *who governs the internet? Players and fields of action (*Abteilung Politische Akademie, 2017) 11. http://library.fes.de/pdf-files/akademie/13910.pdf.

[68] The Software Report, The Top 25 Cybersecurity Companies Of 2020, (22 December, 2020), TSR 2020, https://www.thesoftwarereport.com/the-top-25-cybersecurity-companies-of-2020/ Accessed 31 May 2021.

[69] The Geneva Centre for Security Sector Governance is a good example in this context, https://dig.watch/actors/geneva-centre-security-sector-governance.

governance that is increasingly difficult to achieve. The first difficulty in responding to transparency challenge is that there is no clear definition of transparency from the effective regulation of the security sector's angle. Knowing when a breach of an information system has occurred and the degree of seriousness of the breach remains the challenge in providing transparency. The state can reinforce cybersecurity practices by encouraging or requiring actors who were breached to disclose cybersecurity breaches. This not only enhances transparency in cyberspace but also ensures steps to address gaps in current cybersecurity practices, which helps to combat the spread of cyber-attacks and improve cybersecurity.[70] Lack of transparency about cyberattacks undermines human security in cyberspace, as it can increase the number of victims affected by malicious cyber-attacks.

Numerous initiatives are being carried out at international and regional levels to promote more responsible behavior in cyberspace and develop regulatory frameworks and confidence-building measures applicable to cyberspace.[71] International and regional frameworks provide a set of standards for the development, adoption, and review of cybersecurity legislation.[72] State authorities are primarily responsible for ensuring good governance in cybersecurity. Strengthening of protection and defense of information systems should first be the subject of greater mobilization by the state. State authorities should develop and update national laws to respond to new technological challenges. To address current and emerging cybersecurity threats, states must continuously assess and adapt their national cybersecurity strategies according to the evolving threat environment. This should include a conventional method to identify the origin of cyber threats which to date, is the most challenging area of cybersecurity.[73]

d. Any Remedy to the Victim States?

The intensive use of cyberspace dominates most activities in the world today, from those activities performed by individuals to interactions between states. However, internet dependency is fragile because digital transactions can be easily attacked by those who have malicious intentions and make them vulnerable. Individuals, states, and state-supported groups

---

[70] Paul Smith, 'New mandatory data breach notifications laws to drag Australia into cyber age' (Financial Review, afr.com, 23 February 2018) https://www.afr.com/technology/new-mandatory-data-breach-notifications-laws-to-drag-australia-into-cyberage-20180222-h0whxa accessed 30 December 2020.

[71] Le Centre pour la gouvernance du secteur de la sécurité, *Guide pour la Bonne Gouvernace de la Cybersurité'*, (Geneva, 2019) 44-57.

[72] Le Centre pour la gouvernance du secteur de la sécurité (2019, p. 46).

[73] M. Lalou, H. Kheddouci and S. Hariri, "Identifying the Cyber Attack Origin with Partial Observation: A Linear Regression Based Approach," 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS*W), 2017, p.329.

can organize cyberattacks to harm digital systems. In international law, the attribution of cyber operations aims to determine whether the digital operations can be linked to a particular state.[74]

According to the *Articles on State Responsibility for Internationally Wrongful Acts* two situations should be distinguished.[75] First, an act or omission is attributable to a state if it is committed by one of its organs[76] (Article 4)[77], by persons or entities exercising public authority prerogatives (Article 5)[78], or by organs placed in the disposition of the state by another state (Article 6).[79] Second, the conduct of a non-state actor is attributable to a state if it is committed under the instructions, direction, or control of that state (Article 8).[80]

Several options are available to the victim state[81]. In particular, the victim state may decide to refer the matter to the UN Security Council or to submit the dispute to international jurisdiction, such as the International Court of Justice.[82] However, this solution is not always possible, as international law lacks a centralized judicial mechanism. For this reason, states that are victims of a cyber operation may adopt unilateral extrajudicial measures (the right of self-defense, countermeasures, and retorsion)[83] to coerce the offending state to fulfill its responsibilities, by putting an end to the attack and repairing the damage suffered under certain conditions.[84]

However, it ought to be noticed that, in specific conditions, measures are taken by a state which would not be justified as countermeasures or

---

[74] Clara Assumpção, The Problem of Cyber Attribution Between States, (E-International Relations, May 6, 2020), https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/ accessed 31 May 2021.

[75] Responsibility of States for Internationally Wrongful Acts 2001, General Assembly resolution 56/83 of 12 December 2001, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

[76] *Organ of State means any department of state or administration in the national, provincial or local sphere of government, performing a public duty in terms of constitution or any other legislation.*

[77] Responsibility of States for Internationally Wrongful Acts 2001.

[78] Responsibility of States for Internationally Wrongful Acts 2001.

[79] Responsibility of States for Internationally Wrongful Acts 2001.

[80] Responsibility of States for Internationally Wrongful Acts 2001.

[81] A state (Nation) which is a victim of a wrongful act.

[82] International Court of Justice, How the Court Works, https://www.icj-cij.org/en/how-the-court-works.

[83] Schachter Oscar, 'Dispute Settlement and Countermeasures in the International Law Commission' (1994) 88(3) *The American Journal of International Law*, 471-472 https://www.jstor.org/stable/2203714?seq=1 accessed 29 January 2021.

[84] Examples: Air services Agreement of 27 March 1946(United States V. France), United Nations report of International Arbitral Award, (1979) Vol. XVIII.; Nuclear test (Australia v. France) I.C.J., Report 1974.

measures of self-defense in reaction to a cyber operation, could have their illegality excluded or mitigated by some circumstances such as *force majeure*, distress, consent or necessity. The most probable scenario would be the state of necessity, the sole method for the state to secure its imperative interest against a severe and imminent danger.[85]

e. Do We Need a Cybersecurity Treaty?

There is currently no international cybersecurity treaty regulating cyberspace. Is this treaty even necessary? Some authors like Barat-Ginies [86] argued that there are real fundamental differences regarding the vision of states in the search for their cybersecurity. However, each state develops its defense policy and its national strategies by referring to its legislation. States define their needs, expectations, the types of threats to which they are subject, and the means to protect themselves, repair, and prevent future attacks.[87]Others like Ghernaouti-Hélie argued that bilateral cyber treaties are not enough, that an international cyber treaty would help to reduce vulnerabilities from various cyber threats to an acceptable level.[88]Such treaty would provide approaches on how to respond to a cyber threat and propose ways to repair damages caused by those threats.

Today, the cyberweapons situation is similar internationally to that of nuclear weapons before the *Non-Proliferation Treaty*. A few digital superpowers (USA, China, Russia, and Israel) have created and conveyed cybernetic weapons either protectively or hostile and have utilized them but not broadly.[89] Nations are scrambling to construct their digital abilities behind an excessive amount of mystery.[90] Moreover, similar to the improvement of atomic weapons, horror, and unpredictability about the effects of cyber warfare act as ground-breaking forces encouraging this cyber weapons contest. Nonetheless, the conceivably annihilating consequences of digital warfare are sufficiently severe to make it

---

[85] States like Tanzania (1995), Macedonia (1997), and Jordan (1998) closed their borders and refused entrance to people seeking refuge from violence in their home countries, on the basis of the state of necessity because their national security may have been violated under international law. Roman Boed, *State of Necessity as a Justification for Internationally Wrongful Conduct,* Yale Human Rights and Development Law Journal, Vol. 3 [2000], p.2-3.

[86] Barat-Ginies Oriane, 'Existe-T-Il Un Droit International Du Cyberespace?' (2014) 1-2 (153-154) Hérodot*e* 201, 219.

[87] Ibid 219.

[88] Solange Ghernaouti-Hélie, 'We need a Cyberspace Treaty' (2010) 3(38) Intermedia-IIC 4, 4-5.

[89] Arpagian Nicolas (n34) 24.

[90] Fred Schreier, 'On Cyberwarfare' (DCAF HORIZON 2015 Working Paper) 80 https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf accessed 2 February 2021.

conceivable to accomplish agreement around controlling the expansion of these weapons.

A realistic cyber treaty is a necessary step to be where we should be, which according to the author of this paper, implies; to be able to control cyber weapons proliferation, harmonization of rules regarding cybersecurity, having a competent authority (mostly a judicial organ) to manage disputes related to cybersecurity between nations, and a well-established inclusion of cyber warfare into the rules of international humanitarian law, if a separate treaty is not established. However, any cyber treaty that does not fill at least the following conditions[91], is not worthy any international attention:

- *Universality:* all parties should be included in the agreement without targeting only cyber superpowers. This is important because a cyber treaty that recognizes imbalance of cyber power among nations would encourage cooperation rather than a feeling of less cyber capabilities countries of being exploited by those with so much cyber powers.
- *A clear definition of the term cyber weapon:* a definition broad enough that it can cover anything about cybernetic weapons, is a prerequisite to effectively drafting a treaty, because failing on this, would make the term ambiguous and leaves gaps for the violation of the treaty.
- *A clear definition of the term cyber-attack*: cyber-attacks come in many forms, and their unfortunate consequences are not the same. The convention must restrict its extent to activities started, either directly or sponsored,[92]by states.
- *Verifiability*: any agreement aimed at limiting the proliferation of cybernetic weapons must contain a provision regarding its regular verifiability.
- *Integration into the United Nations Charter*: Cyber-attacks can lead to cyber warfare. Security Council activities covered by Chapters VI and VII should be interpreted to extend to cyber weapons and their use. Having a clear application of the UN Charter on cyber warfare would help the UN Security Council to keep international peace in the domain of cybersecurity.

---

[91] Edward M. Roche and Michael J. Blaine, '*Convention internationale sur l'utilisation pacifique du cyberespace*' (2013) 3-4 (27) Netcom 309, 314-17*)* https://journals.openedition.org/netcom/1449 accessed 25 January 2021.

[92] Catherine Lotrionte, 'Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law' (2018) 2(3) The Cyber Defense Review 73, 73-114.

- *Non-interference with Human Rights*: There is a fear that any treaty aimed at "controlling" the Net will turn it into a massive, state-manipulated force to control and support tyranny at the international level. Control of digital weaponry should not be a pretense to violate human rights.
- *Flexible and adaptable to technologies*: The fast expansion of IT technologies should not make the convention obsolete. It is crucial for a cyber treaty to keep track of the evolution of technology otherwise it would be outdated in a very short time.
- *Enforcement*: Enforcement is essential for any international convention to be effective. This provision should add some adjustments to measures available to the UN Security Council through Chapter VII to be adapted to specific cyberwarfare scenarios.

Edward M. Roche and Michael J. Blaine in their article, *Convention Internationale sur l'utilisation Pacifique du cyberespace*, drafted a whole treaty which we consider to be meaningful to the purpose of this article. Like the Tallinn Manual, the Roche and Blaine's article that can inspire decision-makers, including legislators, to establish a cybersecurity treaty that will reduce vulnerabilities in cyberspace and introduce a binding framework on the international level. The various legal discussions in this section contribute significantly to identifying the main principles of international cyberspace law, which remain in the draft stage. However, the militarization of cyberspace is a worrying phenomenon that slows down the development of international cyberspace law because different nations are now seeing cyberspace as an opportunity to extend their military capabilities by exploiting all it has to offer rather than worrying on what will be the applicability of international law to cyberspace. [93]

CONCLUSION

Cyberspace poses unprecedented problems for politics and law since it transcends concepts of territory and border, rendering the definitions of war and peace outdated. The political will of states towards cyber defense greatly influences how war and peace are understood in cyberspace. Today, efforts at the international level to deal with the threat of cyber warfare are much less numerous than national strategies, though the launches of initiatives have been multilateral. Attempts from bilateral initiatives are far from a comprehensive framework likely to improve cybersecurity and guarantee peace in cyberspace, given the involvement of a small number of the actors concerned in the cyber peace equation.

[93] Gomez, Miguel Alberto N, "Arming Cyberspace: The Militarization of a Virtual Domain," *Global Security and Intelligence Studies:* Vol.1, no.2, 2016, https://www.ibei.org/arming-cyberspace-the-militarization-of-a-virtual-domain_54871.pdf accessed 2 June 2021.

Hostilities like these can start from anywhere in the world and strike any state; these threats, therefore, have an international dimension by nature and require international cooperation, assistance in the investigation, and the adoption of general substantive and procedural arrangements to deal with them. Nowadays, the regulation of cyber conflicts or cyber peace is not on the agenda; instead, military leaders are thinking only of establishing cyber commands and their intention to develop their attacks, defense, or network exploitation capabilities. When countries found themselves confronted with nuclear weapons, they loudly called for the control and non-proliferation of nuclear weapons. Countries must harmonize their legal frameworks to manage cyber conflicts and promote dynamic and multifaceted international cooperation.