ROMANIAN
JOURNAL OF INTERNATIONAL LAW

ISSN 2559 – 3846

The Application of International Law to Cyber Operations:

Some Brief Remarks on Sovereignty, Use of Force and Attribution

Victor STOICA

RJIL No. 24/2020

Pages 41-53

The Application of International Law to Cyber Operations: Some Brief Remarks on Sovereignty, Use of Force and Attribution

Victor STOICA*

Abstract**:** *This paper reveals some concrete controversies related to the application of international law in cyberspace. The three main issues studied in this paper describe the manner in which the principle of state sovereignty interacts with cyberspace, potential problems related to the principle related to the prohibition of the use of force and the main hurdles that need to be surpassed for an act performed in cyberspace to be attributed to a state.*

Key-words: *Attribution; cyber operations; cyberspace; sovereignty; use of force*

Introduction

The exponential growth of cyber operations[1] and the implication of various actors performing in cyberspace, be it states, individuals, international organizations or corporations, are gradually affecting national security.[2] Several international organizations, heads of state, private entities or non-governmental organizations, confirm that we face a contemporary proliferation of illegal acts performed in cyberspace.[3] On the date of 29 June 2021, the United Nations High Representative for Disarmament Affairs, participating at the first open debate on maintaining peace and security in cyberspace before the Security Council, concluded that *"ICT threats are*

* *Victor Stoica is Assistant Lecturer in Public International Law and International Organizations and Relations at the Law Faculty of the University of Bucharest and Affiliated Lecturer in Public International Law, at the National University of Political Studies and Public Administration.* The opinions expressed in this paper are solely the author's and do not engage the institutions he belongs to.

[1] Julian Jang-Jaccard, Surya Nepa , *A survey of emerging threats in cybersecurity,* Journal of Computer and System Sciences, Volume 80, Issue 5, 2014.

[2] Herbert Lin, *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, *Columbia Journal of International Affairs,* Hoover Institution Aegis Paper Series on National Security, Technology, and Law, 2016, p. 21

[3] Scott Shackleford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, Berkeley Journal of International Law, Vol. 27, 2009, p. 209.

increasing, but efforts are also under way to address them".[1] Further, on the 23rd of June 2021, the European Commission concluded that there is a *"rising number of serious cyber incidents impacting public services, as well as the life of businesses and citizens across the European Union."*[2]

In this context, various discussions are currently held on the applicability of international law in cyberspace, including within the United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security[3] or within the Open-ended Working Group on Developments in the field of information and telecommunications in the context of international security.[4]

On the 12th of May 2021, the Presidential Administration of the United States of America issued the *"Executive Order on Improving the Nation's Cybersecurity",* which contains the following conclusion:

> *"The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."*[5]

Representatives of France,[6] Germany[7] or China[8] further confirm the need to properly address cyber threats. Illustratively, the Federal Government of Germany has published, in March 2021, a Position Paper on the Application of International Law in Cyberspace, through which it concluded that *"cyber activities have become an integral part of international relations",*[9] while the National Defense Strategy of Romania refers to cyber tactics in the following terms:

---

[1] Available at https://www.un.org/press/en/2021/sc14563.doc.htm

[2] Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088

[3] Available at https://www.un.org/disarmament/group-of-governmental-experts/

[4] Available at https://www.un.org/disarmament/open-ended-working-group/

[5] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[6] A white paper endorsed by the French Government concluded that *"Dans le même temps, les menaces identifiées en 2008 – terrorisme, cybermenace, prolifération nucléaire, pandémies… – se sont amplifiées. La nécessité d'une coordination internationale pour y répondre efficacement s'impose chaque jour davantage"*, p. 7, available at http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

[7] https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

[8] Cai Cuihong, *Cybersecurity in the Chinese Context: Changing Concepts, Vital Interests, and Prospects for Cooperation*, China Quarterly of International Strategic Studies, 2015, p. 472-473

[9] The Federal Government of Germany, Position Paper, On the Application of International Law in Cyberspace, March 2021, p. 1, available at: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

"Indications of security threats will be increasingly felt throughout the entire society as hostile actors multiply their combat tactics and interferes in states' domestic affairs, including by means of cyber and other hybrid tactics"[1]

There is little to no disagreement with respect to the recent proliferation of cyber-attacks, or regarding the need for international cooperation and multilateralism to address the threats posed within cyberspace, while few contest the role that international law has towards enhancing global cybersecurity.[2] In this context, the relevance of international law for enhancing cybersecurity has been labeled as being of *"critical importance"*[3] in addressing information and technology, internationally. However, more and more voices are currently advocating for the inadequacy of certain existing norms of contemporary international law[4] or, more drastically, their failure to maintain peace within the cyber realm.[5] Calls for specific regulations, prescribing certain vital areas of cyberspace are on the rise.[6]

The scope of this paper is to identify some relevant issues regarding the application of international law in cyberspace with respect to sovereignty, the use of force and attribution. This paper is the first part of wider endeavor, which intends to pinpoint the relevance of interpreting and applying certain concepts, traditional for international law, in cyberspace. Illustratively, the first section addresses sovereignty and the potential convolution of the concepts of "digital sovereignty" and "tech sovereignty". The second section addresses the manner in which the concept of "force" performed in cyberspace might (or might not) have the same meaning as "force" performed in the real world. Finally, the third section addressed attribution in cyberspace

---

[1] Presidential Administration of Romania, National Defence Strategy 2020-2024,Bucharest, 2020, p. 19, available at: https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf

[2] https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/

[3] The Federal Government of Germany, Position Paper, On the Application of International Law in Cyberspace, March 2021, p. 1, available at: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

[4] Michael Fischerkeller, *Current International Law Is Not an Adequate Regime for Cyberspace*, available at https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace ;

[5] Nori Katagiri, *Why international law and norms do little in preventing non-state cyber attacks*, Journal of Cybersecurity, Volume 7, Issue 1, 2021.

[6] Jurgen Feick, Raymund Werle, *Regulation of Cyberspace*, in Robert Baldwin, Martin Cave, Martin Lodge, "The Oxford Handbook of Regulation", 2010; Hassan Bashir, Mohammad Sadegh Nasrolahhi, *A Comparative Study for Regulating the Filtering in the US, the EU and China: Proposals for Policy Making in Iran*, Journal of Cyberspace Studie, Volume 2, Issue 1, 2018;

and some of the difficulties of applying the existing international lagal framework to cyber operations.

1. Sovereignty

The relationship between cyberspace and sovereignty has been developing ever since the Internet was born, as a medium.[1] On the face of it, the exponential digitalization of society might seem to push the concept of sovereignty to its limits.[2] Recently, the subject of sovereignty in cyberspace, linked with the proliferation of cyber threats, led to the conclusion that cyberattacks have become the number one global threat, *"listed within the 2013, 2014, 2015 and 2016 Worldwide Threat Assessments conveyed annually to Congress by the Director of National Intelligence."*[3] In this context, the manner in which states manifest their sovereignty in cyberspace and the terminology used by policy makers seem to need further clarification.

The principle of sovereignty is regulated through art. 2(1) of the Charter of the United Nations, which prescribes that the UN is *"based on the sovereign equality of all its Members".*[4] Among the essential prerogatives of sovereignty is the right to regulate in the public interest,[5] or, properly called, jurisdiction to prescribe. However, several debates exist regarding the manner in which the law operates in cyberspace.[6] In this sense, subjective[7] and objective[8] territorial jurisdiction pose certain limitations in cyberspace and, further, the application of extraterritoriality through traditional jurisdictional norms performed through the active or passive personality tests,[9] is not

[1] Milton Mueller, *Sovereign and Cyberspace, Institutions and Internet Governance*, Essay derived from the 5th Anual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana, October 3rd, 2018, p. 1, available at: https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10410/5th-Ostrom-lecture-DLC.pdf?sequence=1&isAllowed=y

[2] Julia Pohle, *Digital Sovereignty, Internet Policy Review*, Journal of Internet Regulation, Vol. 9., Issue 4, 2020, p. 2.

[3] Cynthia Ayers, *Rethinking Sovereignty in the Context of Cyberspace*, The Cyber Sovereignty Workshop Series, Center for Strategic Leadership, U.S. Army War College, 2016, p. 1.

[4] Available at https://www.un.org/en/about-us/un-charter/chapter-1

[5] Inga Martinkute, *Right to Regulate in the Public Interest: Treaty Practice*, JusMundi, 2021, available at: https://jusmundi.com/en/document/wiki/en-right-to-regulate-in-the-public-interest

[6] Timothy Wu, *Cyberspace Sovereignty? – The Internet and the International System*, Harvard Journal of Law and Technology, Vol. 10, no. 3, 1997, p. 648; Francois Delerue, "Cyber Operations and International Law", Cambridge University Press, 2020, p. 4.

[7] Jean-Baptiste Maillart, *The limits of subjective territorial jurisdiction in the context of a cybercrime*, Academy of European Law, Trier, 2018, p. 2.

[8] Darrel Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, Michigan Telecommunications and Technology Law Review, Volume 4, Issue, 1, p. 72.

[9] Ibid.

entirely suitable for the modern characteristics of cyberspace. Targeting,[1] universality,[2] or protective tests[3] share the same fate.

In order to address the issues related to the manifestations of sovereignty in cyberspace, unsurprinsgly, new terminology seems to emerge. For example, the German Presidency of the EU Council, addressing the Four Goals for the Digital Sector, refers to the concept of *"digital sovereignty",* in the following terms:

> *"1. Europe is to gain more digital sovereignty*
>
> *This presupposes a well-developed digital infrastructure which is at once resilient, sustainable and democratic. The idea is to put in place a digital economic area that meets these criteria."*[4]

The European Council on Foreign Relations seems to confirm this view, by concluding that, for the policy makers in Europe, digital sovereignty is part of "*a larger struggle that they face to maintain their capacity to act and to protect their citizens in a world of increased geopolitical competition."*[5] The quest for the digital sovereignty of the European Union is reflected in the EPRS Ideas Paper issued under the auspices of the European Parliament, which confirms that, in order to reach the goal of enhancing Europe's strategic autonomy in cyberspace, the Union should *"update and adapt a number of its current legal, regulatory and financial instruments".*[6] However, the same document seems to assimilate the notion of digital sovereignty with technological sovereignty.[7] Addressing the same issue, but from a different angle, Ursula von der Leyen, the President of the European Commission, in her op-ed entitled *"Shaping Europe's Digital Future"* concluded her piece, referring to the concept of *"tech sovereignty"*, in the following terms:

---

[1] Dan Jerker Svantesson, *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation*, International Data Privacy Law, Volume 5, Issue 4, 2015

[2] Darrel Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, Michigan Telecommunications and Technology Law Review, Volume 4, Issue, 1, p. 72.

[3] Elena Lazăr, Dragoș Costescu, Dreptul European al Internetului, Hamangiu, 2021, p. 168.

[4] Available at https://www.eu2020.de/eu2020-en/news/article/digitalziele-eu2020/2405548

[5] Available at https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/

[6] Available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[7] Ibid. The paper contains the following relevant distinction: *"The notion of 'technological' **or** 'digital sovereignty' has recently emerged as a means of promoting the notion of European leadership and strategic autonomy in the digital field."* (emphasis added)

"I sum up all of what I have set out with the term 'tech sovereignty'. This describes the capability that Europe must have to make its own choices, based on its own values, respecting its own rules."[1]

Even if these concepts (technological and digital) have certain common features, they are not identical, nor should they be construed as such. In this context, their interchangeable use might not an effective endeavor addressing the interaction between sovereignty and cyberspace. The Internet is not cyberspace.[2] Neither should the digital be confused with the technological, in the same manner in which the kitchen should not be confused with its appliances. In other words, the digital is an element of the toolkit through which states may optimize their use of technology, along with other elements, analogue material. From this perspective, the notion of tech sovereignty seems more appropriate, as it includes, to a certain degree, the notion of digital sovereignty. These terminological clarifications should be the first step in addressing the manner in which sovereignty manifests in cyberspace, with all its characteristics.

Briefly, digital sovereignty means that states should have the ability to control their own digital existence and experience, of their own cyber destinies.[3] Consequently, one expression of sovereignty is the ability to respond to cyber threats, including with force.

2. The prohibition of the use of force

The application of the norms regarding the prohibition of the use of force, as established through article 2(4) of the Charter of the United Nations, shares the same fate as attribution in cyberspace: it is surrounded by uncertainty. Perhaps one of the most pressing issues regarding the use of force in cyberspace relates to the terminology used, especially because its interpretation lacks uniformity.[4]

For example, several confusions exist regarding the meaning attributed to the concepts of cyber-attack, cyber-warfare, and cyber-crime.[5]

---

[1] Ursula Von der Leyen, *Shaping Europe's Digital Future*, Brussels, 19 February 2020, p. 3, available at: https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260

[2] Ananda Mitra, Rae Lynn Schwartz, *From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces*, Journal of Computer – Mediated Communication, Volume 7, Issue 1, 2001.

[3] Sean Fleming, *What is Digital Sovereignty and why is Europe so interested in it?*, World Economic Forum, 15 march 2021, available at: https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/

[4] Oona Hathaway, Rebecca Crootof, Philip Levitz, Nix Haley, Aileen Nowlan, William Perdue, Julia Spiegel, *The Law of Cyber-Attack*, California Law Review, 2012, p. 823.

[5] Ibid, 821.

Illustratively, some authors define the notion of cyber-attack as being *"efforts to alter, disrupt, degrade or destroy computer systems or networks or the information or programs on them."*[1] Others refer to the following definition:

> *"A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose"*[2]

Certain states have adopted guidelines or regulations through which they intend to clarify the conceptualization of the notion of cyber-attacks. For example, the Dictionary of Military and Associated Terms of the Department of Defense of the United States of America, as per January 2021, defines the notion of "cyberspace attack", as such:

> *"Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires"*[3]

While the above-mentioned quote considers that certain operations performed within cyberspace have a destructive potential and, in certain conditions, equate them to using fire, the French Government seems to undertake a slightly different path, which links the concepts of "cyber-attack" and "cybercrime". In this sense, the French Government mentions that the former may target individuals but also companies or administrations, with the purpose of obtaining personal information or in order to exploit it or resell it.[4] As such, it could be concluded, at least from this approach that a cyber-attack could, in fact, target an individual *and* a state. Nevertheless, the Strategy of France regarding the Defense of the Security of Systems and Information confirms the amplitude of the damage potentially caused through a cyber-attack, both to the lives of people and for the infrastructures of states,[5] leading to the conclusion that a cyber-attack is usually performed against a state, while a cybercrime is generally preformed against an individual.

Even if, in general, cyber operations to not reach the threshold of gravity to assimilate them to the use of firepower, the activities performed in

---

[1] Matthew Waxman, *Cyber Attacks as Force under UN Charter Article 2(4)*, Columbia Law School, Scholarship Archive, Faculty Publications, 2011, p. 43

[2] Oona Hathaway, Rebecca Crootof, Philip Levitz, Nix Haley, Aileen Nowlan, William Perdue, Julia Spiegel, *The Law of Cyber-Attack*, California Law Review, 2012, p. 826.

[3] DOD Dictionary of Military and Associated Terms, as of January 2021, p. 55, available at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

[4] Available at https://www.gouvernement.fr/risques/cybercriminalite

[5] https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02 15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

cyberspace can, at times, morph into cyberwarfare.[1] What is the threshold that should be applied in this respect is not clear-cut. A proper application of the concept of "force" is thus relevant, especially because a (cyber) armed attack may be linked with the use of (cyber) force. Article 2(4) of the UN Charter prescribes that all member of the UN shall:

> *" [...] refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."*[2]

However, there is no definition, provided under the Charter, to clarify the notion of force and its implications. In this respect, the International Court of Justice has issued several judgments through which it determined how the use of force is construed. The Court, in the Advisory Opinion related to the *Legality of the Threat or Use of Nuclear Weapons* concluded that the provisions of the UN Charter related to the prohibition of the use of force, i.e. article 2(4), article 51 and article 42, *"do not refer to specific weapons"*[3] and that the mentioned provisions apply to *"any use of force, regardless of the weapons employed"*.[4] Another relevant finding of the International Court of Justice regarding the use of force was issued in the Military and Paramilitary Activities in and against Nicaragua, in which the Court concluded that certain actions may not constitute an armed attack but may constitute use of force.[5] The Tallinn Manual 2.0, through Rule 69 attempts to clarify the application of the above mentioned interpretation in cyberspace by linking force with its external effects righter than its internal characteristics, in the following terms:

> *"a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of the use of force"*[6]

As such, when assessing the use of force in cyberspace, the effects and scale of the action are more relevant than the material (or the weapon) used. Even if the definition used by the Tallinn Manual 2.0. seems to reflect, to a

---

[1] Francois Delerue, "Cyber Operations and International Law", Cambridge University Press, 2020, p. 55.

[2] Available at https://www.un.org/en/about-us/un-charter/chapter-1

[3] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, para 39, p.

[4] Ibid.

[5] International Court of Justice, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, para. 210, p. 110.

[6] Michael Schmitt (ed.), "Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations", Cambridge University Press, 2017, p. 330.

certain degree, the conceptualization specific to general international law, some commentators suggest that it might be more appropriate to develop a set of new norms that would better address cyber operations.[1]

3. Attribution

One of the critical[2] and tedious[3] issues in international law today is the attribution of illegal acts in cyberspace. Attribution in cyberspace is, indeed, essential because *„most responses to cyber operations cannot be deployed without attribution".*[4] To further complicate the issue, potential answers to questions as to how to attribute an action, and to whom (or to what) are surrounded by uncertainty.[5]

Technical difficulties are, perhaps, most visible. The anonymity of cyberspace, enhanced by the ease with which a perpetrator can hide her IP address[6] or the identification of operations performed through multiple systems (or networks), located in different jurisdictions[7] are examples that entangle the possibility to pin point actions or perpetrators and, finally, to attribute the actions performed by said perpetrators to a state.

Legal difficulties are also present. Perhaps among the most complicated is the reconciliation of the traditional approaches regarding attribution, confirmed by international courts and tribunals or by international bodies involved in the codification and progressive development of international law with the ever-evolving complexity of certain operations performed in cyberspace. General public international confirms that for an act to be attributable to a state, the aggrieved party should perform the "effective control test", as adopted by the International Court of Justice in the Military and Paramilitary Activities in and against Nicaragua,[8] or the "overall control

---

[1] Jurgen Feick, Raymund Werle, *Regulation of Cyberspace*, in Robert Baldwin, Martin Cave, Martin Lodge, "The Oxford Handbook of Regulation", 2010.

[2] Nicholas Tsagourias, , *Cyber Attacks, Self-Defence and the Problem of Attribution*, Journal of Conflict and Security Law, Oxford University Press, 2012, p. 233.

[3] Florian Egloff, Max Smeets, *Publicly attributing cyber attacks: a Framework,* Journal of Strategic Studies, Routlege (2021), p 1.

[4] Francois Delerue, "Cyber Operations and International Law", Cambridge University Press, 2020, p. 51.

[5] Dan Efrony, Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, American Journal of International Law, 2018, p. 633

[6] Duncan Hollis, *An e-SOS for Cyberspace*, Harvard International Law Journal, Vol. 52, Nr. 2, 2011, p. 398

[7] Karin Bannelier, Theodore Christakis*, Cyber Attacks, Prevention – Reactions: The Role of States and Private Actors*, Les Cahiers de la Revue Défense Nationale, Paris, 2017, p.15.

[8] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14.

test", as adopted by the International Criminal Tribunal for the Former Yugoslavia in Prosecutor v. Tadic.[1] The International Law Commission, through its Articles on Responsibility of States for Internationally Wrongful Acts has codified, through articles 4 to 11 the manner in which conduct is generally attributed to states in international law.[2] However, the above-mentioned conceptual framework might prove difficult to apply *mutatis mutandis* to cyber operations.

Several opinions exist regarding the process of attributing acts performed within cyberspace. In this respect, Francois Delerue describes three main components, or three main steps, that should be undertaken in order to attribute the act: *'attribution to a machine, attribution to a human and attribution to a state'*.[3] Other authors describe the process in different terms and consider that machine attribution, specific perpetrator attribution and adversary attribution are the standards that should be met, when addressing the same issue.[4] Further, two-pronged classifications exist, classifying attribution as either technical or human.[5] Other views have been expressed in the sense that the first step in order to achieve attribution is to determine the cyber-weapon, i.e. to determine the instrument through which the illegal act has been committed, the state from which the act has been committed and, finally, the person.[6]

What is generally accepted today is that attribution for cyber operations implies the identification of the entity that is responsible for a cyberattack[7] or a cybercrime or any other malicious activities performed in cyberspace. Nevertheless, it is yet to be observed whether the current existing norms of international law are sufficient to address the various issues posed by the traditional framework of attribution.

---

[1] Tadić (IT-94-1), United Nations, International Criminal Tribunal for the former Yugoslavia

[2] https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

[3] Francois Delerue, "Cyber Operations and International Law", Cambridge University Press, 2020, p. 55.

[4] Florian Egloff, Max Smeets, *Publicly attributing cyber attacks: a Framework,* Journal of Strategic Studies, Routlege (2021), p. 3; Herbert Lin, *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, Columbia Journal of International Affairs*,* Hoover Institution Aegis Paper Series on National Security, Technology, and Law, 2016, p. 21

[5] Earl Boebert, *A survey of challenges in attribution*, National Academy of Sciences, Proceedings of a Work-shop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, 2010, pp. 41-54

[6] Jawwad Shamsi, Sherali Zaedally, Fareha Sheikh, and Angelyn Flowers, *Attribution in Cyberspace: Techniques and legal implications*, Security And Communications Networks, 2016, available at: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1485

[7] Abdulakir Bilen, Bedri Ozer Ahmet, *Cyber Attack Method and Perpetrator Prediction Using Machine Learning Algorithms*, Peer Journal of Computer Science, Volume 7, 2021.

Conclusion

The scope of this paper was not to clarify any of the pressing issues posed by the application of international law in cyberspace but, rather, to reveal them. This article pinpointed a series of controversies related to the manner in which certain concepts generally accepted under public international law interact with the specifics of cyberspace.

International law applies in cyberspace.[1] This conclusion is supported by the vast majority of stakeholders, be them states, policy makers, scholars, international lawyers or representatives of international organizations. Nevertheless, a contemporary trend seems to emerge, which concludes that certain key concepts prescribed through the existing norms of international are insufficient for addressing precise cyber operations. In this sense, the President of the European Commission concluded that the digital transition of Europe may require legislation "where appropriate".[2] This conclusion is relevant not only for Europe but for enhancing global cybersecurity, in line with the specific provisions of the United Nations Charter and the fundamental norms of international.

[1] Francois Delerue, "Cyber Operations and International Law", Cambridge University Press, 2020, p. 13

[2] Ursula Von der Leyen, *Shaping Europe's Digital Future*, Brussels, 19 February 2020, p. 3, available at: https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260

Bibliography

Books

Cynthia Ayers, *Rethinking Sovereignty in the Context of Cyberspace*, The Cyber Sovereignty Workshop Series, Center for Strategic Leadership, U.S. Army War College, 2016

Earl Boebert, *A survey of challenges in attribution*, National Academy of Sciences, Proceedings of a Work-shop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, 2010

Elena Lazăr, Dragoș Costescu, Dreptul European al Internetului, Hamangiu, 2021

Francois Delerue, "Cyber Operations and International Law", Cambridge University Press, 2020

Jurgen Feick, Raymund Werle, *Regulation of Cyberspace*, in Robert Baldwin, Martin Cave, Martin Lodge, "The Oxford Handbook of Regulation", 2010

Jean-Baptiste Maillart, *The limits of subjective territorial jurisdiction in the context of a cybercrime*, Academy of European Law, Trier, 2018

Michael Schmitt (ed.), "Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations", Cambridge University Press, 2017

Articles

Abdulakir Bilen, Ahmet Bedri Ozer, *Cyber Attack Method and Perpetrator Prediction Using Machine Learning Algorithms*, Peer Journal of Computer Science, Volume 7, 2021

Ananda Mitra, Rae Lynn Schwartz, *From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces*, Journal of Computer – Mediated Communication, Volume 7, Issue 1, 2001

Cai Cuihong, *Cybersecurity in the Chinese Context: Changing Concepts, Vital Interests, and Prospects for Cooperation*, China Quarterly of International Strategic Studies, 2015

Dan Efrony, Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, American Journal of International Law, 2018

Dan Jerker Svantesson, *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation*, International Data Privacy Law, Volume 5, Issue 4, 2015

Darrel Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, Michigan Telecommunications and Technology Law Review, Volume 4, Issue, 1, 1998

Duncan Hollis, *An e-SOS for Cyberspace*, Harvard International Law Journal, Vol. 52, Nr. 2, 2011

Florian Egloff, Max Smeets, *Publicly attributing cyber attacks: a Framework,* Journal of Strategic Studies, Routlege, 2021

Hassan Bashir, Mohammad Sadegh Nasrolahhi, *A Comparative Study for Regulating the Filtering in the US, the EU and China: Proposals for Policy Making in Iran*, Journal of Cyberspace Studie, Volume 2, Issue 1, 2018

Herbert Lin, *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, Columbia Jounral of International Affairs, Hoover Institution Aegis Paper Series on National Security, Technology, and Law, 2016

Julia Pohle, *Digital Sovereignty, Internet Policy Review*, Journal of Internet Regulation, Vol. 9., Issue 4, 2020

Julian Jang-Jaccard, Surya Nepa, *A survey of emerging threats in cybersecurity,* Journal of Computer and System Sciences, Volume 80, Issue 5, 2014

Karin Bannelier, Theodore Christakis*, Cyber Attacks, Prevention – Reactions: The Role of States and Private Actors*, Les Cahiers de la Revue Défense Nationale, Paris, 2017

Matthew Waxman, *Cyber Attacks as Force under UN Charter Article 2(4)*, Columbia Law School, Scholarship Archive, Faculty Publications, 2011

Milton Mueller, *Sovereign and Cyberspace, Institutions and Internet Governance*, Essay derived from the 5th Anual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana, October 3rd, 2018

Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, Journal of Conflict and Security Law, Oxford University Press, 2012

Nori Katagiri, *Why international law and norms do little in preventing non-state cyber attacks*, Journal of Cybersecurity, Volume 7, Issue 1, 2021

Oona Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, *The Law of Cyber-Attack*, California Law Review, 2012

Scott Shackleford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, Berkeley Journal of International Law, Vol. 27, 2009

Timothy Wu, *Cyberspace Sovereignty? – The Internet and the International System*, Harvard Journal of Law and Technology, Vol. 10, no. 3, 1997

Web sources

Inga Martinkute, *Right to Regulate in the Public Interest: Treaty Practice*, JusMundi, 2021, available at: https://jusmundi.com/en/document/wiki/en-right-to-regulate-in-the-public-interest

Jawwad Shamsi, Sherali Zaedally, Fareha Sheikh, Angelyn Flowers, *Attribution in Cyberspace: Techniques and legal implications*, Security And Communications Networks, 2016, available at: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1485

Michael Fischerkeller, *Current International Law Is Not an Adequate Regime for Cyberspace*, available at https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace

Sean Fleming, *What is Digital Sovereignty and why is Europe so interested in it?*, World Economic Forum, 15 march 2021, available at: https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/

Ursula Von der Leyen, *Shaping Europe's Digital Future*, Brussels, 19 February 2020, available at: https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260