Metodi Hadji-Janev*

Filling the *opinio iuris* vacuum on sovereignty in cyberspace: A call for the South-Eastern European States to act

Abstract

There is more than one reason why South-East European States should clarify their public positions on the applicability of sovereignty as a principle or as the rule of international law while addressing the growing ambiguity in cyberspace. The article argues that strategically and legally it is in the SEE States' interest to step up and fill the vacuum in ever needed *opinio iuris* on the applicability of sovereignty in cyberspace, particularly after some leading NATO States took an opposing course on the issue. Explaining the evolution in cyberspace and how this affects the Westphalian concept of sovereignty under international law the article introduces the importance of the main thesis. It then provides the rationale for the argument and explains why it is in the SEE States interest to act and express their position on the applicability of sovereignty in cyberspace under international law.

Key words: International law, sovereignty, Cyberspace, NATO, South-East European States, Strategy

* Metodi Hadji-Janev, A Brigadier General, Associate professor of law Military Academy General Mihailo Apostolski, Skopje and Adjunct Faculty Member, Ira A. Fulton School of Engineering, Arizona State University, ASU, U.S., e-mail: Metodi.hadzi-janev@ugd.edu.mk.

Introduction

The rapid threat development in cyberspace has urged States to reconsider the applicability of sovereignty and international law. Strives to extend sovereign control into cyberspace is a direct result of nations' attempts to protect their citizens and interest. The UK's position on the applicability of sovereignty delivered in 2018 has instigated debate over the issue and revoke the importance of *opinio iuris* on the matter. Since then, the debate had been underway over whether sovereignty is a principle of international law or it is a rule. Several NATO States have expressed opposing views, thus putting the Alliance in an awkward situation but also the whole debate focusing on some substantive grounds such as determining the threshold of the breach, for example.

South-East European (SEE) States (NATO and PfP members) are silent observers on the issue for now. Their position on the issue is of paramount importance for NATO but also in a broader international context for two reasons. First, because there is a lack of sufficient State practice and *opinio iuris* regarding the recognition of sovereignty as a rule of international law. Second, because in the latest doctrine on cyber operations NATO took the position that sovereignty is an independent right. The difference in approach i.e. applying sovereignty as a principle vs. as a rule is important because it determines how the State may respond to likely violation of sovereignty.

The article opens with the evolution of cyberspace and the traditional Westphalian sovereignty. Consequently, it provides a brief overview of the ongoing debate over the applicability of sovereignty to cyberspace indirectly pointing to the importance of SEE States' position on the issue. The main thesis is that there is strategic and legal importance for SEE States to express their position on the applicability of sovereignty. The article explains them accordingly.

The evolution of cyberspace and the traditional Westphalian sovereignty

The days of ultra-libertarian hopes for cyberspace are over[1]. While the Post-Cold War reality gave some hopes that we may have a globally interconnected

1 A.C. Madrigal, *The End of Cyberspace*, The Atlantic, May 1, 2019, https://www.theatlantic.com/technology/archive/2019/05/the-end-of-cyberspace/588340/ [dostęp: 20.08.2021].

society free of regulation, or the interference of bureaucrats, the dynamics in this sector in the last two decades seem to defy these views[2]. This is understandable giving that cyberspace evolved as the political concepts that underpin it also changed and are still changing.

The internet in general and consequently cyberspace was a Western liberal (predominantly American) creation[3]. The original idea was to develop a network that will support communication[4]. Soon the exchanges of ideas to support innovation, science, and general wellbeing also were nested under the idea of developing cyberspace. In no time this free space grew in a globally distributed network comprising many voluntarily interconnected autonomous networks. Arguably, Western liberal values of openness and free speech (shared by many, but not all countries) to a certain degree shaped the internet's technology and governance. Initially, this worked against sovereign control and strict application of shared principles, norms, rules, decision-making procedures, and programs that shape cyberspace evolution and use.

Free of regulation-heavy ideology and based on the *laissez-faire* approach the „new space" – cyberspace was developed on horizontal set-up structure as opposed to the physical space based on conventional hierarchical-vertical structures. Though the ongoing inevitable convergence between the two provided many positive aspects it raised some governing concerns.

It soon became evident that Westphalian-based sovereignty could easily be challenged and undermined in cyberspace[5]. Unlike the conventional trade-off between people's freedom and security provided by the State the concept on which Westphalian sovereignty (and with that modern Statehood and international order) was born, cyberspace stimulated trading on different grounds[6]. In cyberspace, the end-users, more or less, trade their freedom for

2 A. Greenberg, *It's Been 20 Years Since This Man Declared Cyberspace Independence*, August 2, 2016, Wired, https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/ [dostęp: 20.08.2021].

3 A. Barrinha, T. Renard, *Power and diplomacy in the post-liberal cyberspace*, „International Affairs" 2020, vol. 96, no. 3, p. 749–766.

4 M.B. Leiner i in., *Brief History of the Internet*, Internet Society, 1997, September 13, 2017, https://www.internetsociety.org/resources/doc/2017/brief-history-internet/ [dostęp: 20.08.2021].

5 Ch. Demchak, P. Dombrowski, *Cyber Westphalia: Asserting State Prerogatives in Cyberspace*, „Journal of International Affairs" 2013, p. 29–38, http://www.jstor.org/stable/43134320 [dostęp: 20.08.2021].

6 See more in: Sh. Leader, *Statehood, Power, and the New Face of Consent*, „Indiana Journal of Global Legal Studies" 2016, vol. 23, no. 1, p. 127–142.

services. This and other diverging futures that shape architectures of the two converging worlds (cyber and physical) produce weaknesses among others in protecting users' privacy and security and contradict the same liberal ideas on which the concept was developed[7].

Giving that sovereignty defines how policy, laws, regulations, conventions and treaties are built to ensure the continuation of proper and secure governance some States have started to revoke sovereignty in cyberspace. This is important because based on the concept of sovereignty Western democracies are built, develop their policy and strategy, actions and reactions. Moreover, serious debates on different levels try to address traditional ideas of security, stability, and sovereignty in the context of cyberspace, cybersecurity and cyber defense. One of the most prominent among these debates on the official level and in the legal community is the legal application of sovereignty in cyberspace.

Applicability of sovereignty in cyberspace and the South-Eastern States' position on the issue

The strives to extend sovereign control into cyberspace is a direct result of nations' attempts to protect their citizens and interest. Sovereignty had long been recognized as a rule of international law[8]. Put in the context of intrusive cyber activities it allows States to consider any aggressive cyber operations as unlawful. Under these circumstances, States may reserve the right to respond and strike back[9]. This, in the cyber context, means that hack-backs can sometimes be justified as countermeasures[10]. Nevertheless, what seems to be absolved in these regards changed after the United Kingdom (UK) Attorney

7 S. Herpig, J. Schuetze, J. Jones, *Securing Democracy in Cyberspace*, Stiftung Neue Verantworting, October 2018, https://www.stiftung-nv.de/sites/default/files/securing_democracy_in_cyberspace.pdf [dostęp: 20.08.2021].

8 S. Besson, *Sovereignty*, Max Planck Encyclopedias of International Law, 2011, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472 [dostęp: 20.08.2021].

9 M.C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)*, „Yale Journal of International Law" 2011, vol. 36, p. 421–459.

10 A.H. Perina, *Proceedings of the Annual Meeting, American Society of International Law*, *The Effectiveness of International Law*, vol. 108, Cambridge 2014, p. 77–80.

General Jeremy Wright's announcement that the UK view sovereignty as a principle, not as a rule that can be violated[11].

The UK's position on the applicability of sovereignty instigated confusion and concern among States even among traditional NATO allies[12]. The complexity of the issue, become evident during the second session of the UN's General Assembly Open-Ended Working Group established to address the developments in the field of information and communications technologies (ICT) in the context of international security[13]. Hence, different views expressed earlier on the applicability of sovereignty emerged again.

The difference in approach i.e. applying sovereignty as a principle vs. as a rule is important because it determines how a State may respond to likely violation of sovereignty. Precisely, if the approach that sovereignty is a principle that would mean that State (such as the UK, and to a certain degree the US) position would be that sovereignty is the base from which other rules of law, like intervention, for example, derived. This, however, would mean that sovereignty is not a rule capable of being violated in its own right[14]. If the State considers sovereignty as a rule of international law, this will mean that State would be obligated to respect sovereignty in cyberspace and any form of meddling attributed to other State would constitute an internationally wrongful act. The sovereignty-as-a-rule position thus would enable a target State of a cyberattack to seek reparation under the law of State responsibility and/or respond with proportionate countermeasures.

Following the UK's Statement and change of course – the position on the applicability of sovereignty, several NATO States have expressed opposing views, putting the Alliance in an awkward situation but also the whole debate focusing on some substantive grounds such as determining the threshold of

11 J. Wright, *Cyber and International Law in the 21st Century*, The UK's position on applying international law to cyberspace, Gov. UK, May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [dostęp: 20.08.2021].

12 D. Efrony, Y. Shany., *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, „American Journal of International Law" 2018, vol. 112, p. 583–657.

13 *Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG)*, Chair's working paper in view of the Second substantive session (10–14 February, 2020), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-working-paper-second--substantive-session.pdf [dostęp: 20.08.2021].

14 See in J. Wright, op. cit.

breach for example. France led the response and took an opposing position[15]. The Netherlands followed with the same course as France[16], but also other NATO (Estonia[17], Czech Republic[18], Germany[19]) and non-NATO (Austria[20], Finland[21] and Switzerland PfP States) countries that express their view on the issue expressed their support to the existence of the rule of sovereignty[22]. The United States[23] and Israel[24] have expressed their view but avoided a direct

15 M. Schmitt, *France's Major Statement on International Law and Cyber: An Assessment*, just security, September 16, 2019, https://www.justsecurity.org/66194/frances-major-Statement-on-international-law-and-cyber-an-assessment/ [dostęp: 20.08.2021].

16 *Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace*, a translation of a document sent by the Government, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [dostęp: 20.08.2021].

17 *President of the Republic at the opening of CyCon 2019*, Speeches, May 29, 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html [dostęp: 20.08.2021].

18 R. Kadlčák, *2nd Substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations*, New York, 11 February 2020, https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20--%20International%20Law%2011.02.2020.pdf [dostęp: 20.08.2021].

19 *On the Application of International Law in Cyberspace*, The position paper has been prepared by the German Federal Foreign Office and the German Federal Ministry of Defence in cooperation with the German Federal Ministry of the Interior, Building and Community, Position Paper, March 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf [dostęp: 20.08.2021].

20 *Austria welcomes the „Pre-Draft" Report of the Open Ended Working Group on developments in the field of Information and Telecommunication in the context of international security (OEWG ICT)*, Comments by Austria, March 31, 2020, https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf [dostęp: 20.08.2021].

21 *Finland published its positions on public international law in cyberspace*, Ministry for Foreign Affairs of Finland, October 15, 2020 (published in english October 19, 2020), https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace [dostęp: 20.08.2021].

22 e.g., Austria, Bolivia, China, Czech Republic, Finland, Guatemala, Guyana, Iran, New Zealand, Republic of Korea, and Switzerland.

23 *Remarks By Hon. Paul C. Ney, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, March 2, 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ [dostęp: 20.08.2021].

24 R. Schondorf, *Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, ranscript of the keynote speech delivered by Israeli Deputy Attorney General (International Law), Dr. Roy Schöndorf, on 8 December, 2020 at the US Naval War College's event on „Disruptive Technologies and International Law", EJIL: Talk, https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/ [dostęp: 20.08.2021].

response on the issue directly. Unlike these States, South-East European (SEE) States are silent observers on the issue.

The SEE States position on the issue is of paramount importance for NATO but also in a broader international context for two reasons. First, the U.S. has rightfully maintained that there is a lack of sufficient State practice and *opinio iuris* regarding the recognition of sovereignty as a rule of international law. Second, although the UK put a reserve on the issue, in its cyber doctrine NATO took the position that sovereignty is an independent right and as such, a State-sponsored cyberattack may violate a targeted State's sovereignty under certain conditions[25].

Strategic and legal importance for the SEE States' position on the applicability of sovereignty

There is more than one reason why the SEE States should express their position on the applicability of sovereignty. Along with the strategic importance (as NATO and PfP members) of the SEE States' position on the issue, there are legal reasons why SEE States should do so. Both strategic and legal importance stems from the governing, national defense requirements and a wider international responsibility and contribution.

Strategic importance for the South-East European States to express the position on sovereignty

Acceleration of scientific and technological advancement, ubiquity and access to dual-use systems, the emergence of powerful multinational corporations, private security companies and non-governmental movements will continue to erode SEE States' monopoly over strategic effects[26]. Abusing these developments and unintended governing loopholes that immerged in the

25 *Allied Joint Doctrine For Cyberspace Operations*, *Allied Joint Publication-3.20 (AJP-3.20)*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf [dostęp: 20.08.2021].

26 See more about this in D.J Davidson., L.W. Rees-Mogg, *The Sovereign Individual: Mastering the Transition to the Information Age*, New York 1999.

ongoing convergence between cyber and physical space allow State and non-State actors to exploit the disruptive nature of modern technologies and strategically challenge SEE States from community to national levels and *vice-versa*. Employing conventional and non-conventional methods acting across multiple domains through proxies or directly emerging peer competitors of the democratic world will continue to corrupt SEE States' cyberspace for control and power projection and posing asymmetric and hybrid threats[27].

As NATO and PfP members, it is crucial for both civilian and military SEE leaders to have an official position on the issue of applicability of sovereignty in cyberspace. With that, the SEE leaders need to understand how this affects national and international aspects of sovereignty issues in cyberspace. The belonging to the Alliance means that intentionally or not SEE may be on a retaliation map of a potential attacker who does not necessarily have any direct confrontation. Furthermore, retaliation breach of sovereignty could also be expected due to the recent solidarity practice in the diplomatic field, i.e. to expel Russian diplomats[28].

Initially, the determination of what constitutes cyber sovereignty will greatly influence the SEE threat assessment matrixes. Consequently, it will affect the development of the strategic concepts – strategies that will reflect new reality not in an isolated manner but in the regional and Alliance context manner. Based on this SEE State should operationalize strategic frameworks. This should help to define the role of relevant stakeholders and the overall societal role in responding to the threat vectors streaming from cyberspace. SEE should then project the development of proper capabilities (resources and manpower), structures and predict organizational frameworks capable to meet and successfully address the threats. This will also determine and provide background for mobilization, allocation and management of resources. With such an approach they will not just help NATO in achieving the ever-needed resilience but will also mitigate potential enemies and malicious

27 *NATO's response to hybrid threats*, March 16, 2021, https://www.nato.int/cps/en/natohq/topics_156338.htm [dostęp: 20.08.2021].

28 See for example *Czech Republic asks EU, NATO allies to expel Russian diplomats*, April 20, 2021, https://www.dw.com/en/czech-republic-asks-eu-nato-allies-to-expel-russian-diplomats/a-57266399 [dostęp: 20.08.2021]; Also see *Spy poisoning: NATO expels Russian diplomats*, March 27, 2018, https://www.bbc.com/news/world-asia-43550938 [dostęp: 20.08.2021].

actors' ambitions to define the boundaries of cyber sovereignty and the rules of cyberspace engagement, thus undermining proper response[29].

From the policy perspective, the SEE leaders should divorce from the more than three decades of „copy-paste mode" of strategic documents and aligning themselves in policy development on the fundamental issues. Moreover, despite numerous reports, think-tank events/projects, political Statements and initiatives (most on the „because we were told so" basis) for intervention in the legislation and administration sectors, the cyber policy discourse across the SEE has not advanced from the national security realm stuck in the 90s.

Giving the interdependence and interconnections that cyberspace introduces, the applicability of sovereignty to cyberspace is important in the economic and foreign investment context. Attacks to private enterprises either as policy retaliation[30] or as a strategy to erode peer enemy power by eroding its financial capabilities and thus preventing proper response are on large[31]. Giving that numerous foreign enterprises do business in SEE, it is very likely to expect that SEE citizens and with that critical infrastructures can be a target of foreign intrusive cyber-attacks. What is also concerning are the potential implications that the victim's response could cause. Some CEO's have already recognized that „In addition to spending money to prevent attacks, companies must have the mindset that breaches are inevitable, and they've got to be able to identify breaches quickly after they have occurred and then launch a proportionate response"[32].

Namely, a rightful pursue to protect the business by the private investor's IT cyber security response team, among others, may include striking back, either in the initial phases of a larger and orchestrated cyberattack as deterrence signal to prevent further implication or as the tactic to impose redundancy during the consequence management. This is especially important because

29 *Resilience and Article 3*, Jun 11, 2021, https://www.nato.int/cps/en/natohq/topics_132722.htm [dostęp: 20.08.2021].

30 A. Campbell, *The Legal Implications of Sony's Cyberhack*, „Oklahoma Journal of Law and Technology" 2015, vol. 11, no. 1.

31 *Remarks By Tom Donilon, National Security Advisor to the President: „The United States and the Asia-Pacific in 2013"*, March 11, 2013, https://obamawhitehouse.archives.gov/the--press-office/2013/03/11/remarks-tom-donilon-national-security-advisor-president-united-States-an [dostęp: 20.08.2021]. Also see X. Wang, L. Qiao, *Unrestricted Warfare*, Los Angeles, CA 2002.

32 H. Richardson, *Companies 'Must See Cyber Attacks as Inevitable'*, „Newsweek", February 16, 2015, http://www. newsweek.com/companies-must-see-cyber-attacksinevitable-307111 [dostęp: 20.08.2021].

in this case, the applicability of sovereignty in cyberspace as a principle or as a rule of law would have different implications. Moreover, if the foreign investor resident State has a different approach than the host SEE State where the incident has occurred urges, even more, SEE States to consider taking the position on the issue.

Finally, there are practical policy-based reasons why SEE States should express their position on the applicability of sovereignty to cyberspace. As with the recent strategic concepts that followed the new trends in the security and governing realm if not addressed as a need to be addressed, meaning by the SEE States leadership themselves, the issue on sovereignty will eventually be addressed as the bilateral push. In the past thirty years, we have already witnessed similar practices in the crisis management sector[33], or in the countering violent extremism (CVE) concepts (approach to rehabilitation and reintegration efforts as a part of the larger CVE national efforts[34], etc. The point here just to be clear is that there is nothing wrong with these concepts, strategies, or approaches. The problem is that most of them are done in a hurry (after some funds have been dedicated by the friendly partner western nations, or institutions) and that they are usually not tailored to fit the reality on the ground nor are adjusted with administrative regulations and above all are usually in discourse with the local cultural wisdom and traditions.

A clear example could be the crisis management sector across the SEE. After being extracted from the defense sector this sector was developed without proper strategic framework adjustments. This means that although the introduced crisis management concept follows the democratic framework of operation across the SEE it either emulate the US or the EU conceptual frameworks because as we mentioned before the concept was just copy-paste (again with good intentions). In North Macedonia, and this is the case for several other SEE States, for example, the Government has proudly announced that we have applied the Kyoto framework in disaster risk reduction strategic framework. At the same time, the two key players in the crisis management system law enforcement and defense sector follow the EU and NATO strategic framework conceptualization accordingly. While all are relevant and important

33 *Enhancing civil emergency response in the Western Balkans*, 26 Nov. 2016, https://www.nato.int/cps/en/natohq/news_138304.htm?selectedLocale=en [dostęp: 20.08.2021].

34 *Regional Strategy for Investment in the Western Balkans*, BM.12/DOC.09/Annex 1, 2019, https://www.gcerf.org/wp-content/uploads/2015/12/GCERF-Strategy-for-Investment-in-the-Western-Balkans.pdf [dostęp: 20.08.2021].

these three strategic frameworks have differences in how they assess risks, what they consider as a risk, how they respond, how they allocate resources communicate etc. While these strategic framework differences may not be that problematic when one tries to operationalize them the discrepancies on the ground are large. Hence, the institutions that need to cooperate and react/act does not have the same threat assessment, risk assessment, mission Statement, not to speak about the same standardized equipment, operating procedures, etc. On top of this are the different legal traditions with the sponsor nations when the concept was implemented.

International legal reasons for South-East European States' position on the applicability of sovereignty in cyberspace

What a potential SEE victim State of a cyber intrusion or aggressive operation either against its citizens, corporate or institutions can do in relation to other States' malicious cyber acts in accordance with the law is a matter of what that nation, as a sovereign, agrees to in relation to other States and institutions. Based on the position on sovereignty States can exercise jurisdictional rights over the physical cyberinfrastructure and can proscribe the conduct of individuals, corporates and other stakeholders in cyberspace that resides within their territorial boundaries. Hence, the outcome, i.e. States' reaction to the violation of sovereignty, would not in a legal term be the same if the State recognizes the sovereignty „as a rule" vs. if it does so „as a principle".

The question at hand is important because if the SEE States decide to consider sovereignty to be an underlying principle of international law, that means that the government will be ready to receive but also to practice operations and gaining access to a system in gray or red space. Put differently the SEE State in this context will reject the notion of a strict trespass rule of international law. In practice, this would mean that the unauthorized access of ICT or networks located in another country does not always violate territorial sovereignty and/or international law. To stay on the positive side of the spectrum under international law, however, the SEE State should provide proper justification for such actions[35]. Furthermore, there is a possibility that

35 See more on this in M. Schmitt, *Three International Law Rules for Responding Effectively to Hostile Cyber Operations*, Just Security, July 13, 2021, https://www.justsecurity.org/77402/

although a responding SEE State that accepts sovereignty as a principle might not see itself as operating in contravention of international law, the other NATO States that accept the rule (see sovereignty as a rule) might consider its response unlawful (barring a circumstance precluding wrongfulness).

The UK's position on sovereignty in cyberspace represents a discourse of the traditional UK position on sovereignty. Voices in the U.S. military are also advocating for this approach justifying it under the need for operational flexibility and more importantly ability to operationalize deterrence in cyberspace[36]. On the other hand, very few malicious cyber activities by authoritarian States (Russia, North Korea, China or KSA and UAE in the context of violating human rights) can unequivocally be characterized as violations of international law absent a rule of law protecting sovereignty. In addition to the fact that Article 2 (4), and 51 of the UN Charter (prohibited intervention or use of force) are both demanding and ill-defined, the 'sovereignty is not a rule' position affords other States the flexibility to act in an 'indiscriminate and reckless' manner while claiming to operate within the boundaries of international law[37]. Moreover, these strategic and operational requirements among the NATO democracies have increased the uncertainty over the exact meaning of sovereignty in international law and its applicability in cyberspace.

Although not in a larger number, as we have already pointed before, some NATO allies led by France, Netherlands, Germany, Czech Republic and followed by the PfP States Austria, Finland and Switzerland, have taken the position that sovereignty is a rule. This under international law means that the rule can be violated. Therefore, sovereignty, as a rule, limits operational flexibility, but it allows States to legally consider the majority of cyber operations occurring below the threshold of prohibited use of force, as an internationally wrongful act[38]. In practice, this would mean that if the SEE State without authorization access to computers or networks located in another State this activity will

three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/ [dostęp: 20.08.2021].

36 C.E. Ayers, *Rethinking sovereignty in the Context of Cyberspace*, *The cyber sovereignty workshop series*, Carlisle Barracks, PA, 2016, p. 82–94.

37 J. Biller, M Schmitt., *Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences*, EJIL: Talk, October 24, 2018, https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/#more-16574 [dostęp: 20.08.2021].

38 M. Schmitt, *Three International Law Rules for Responding Effectively to Hostile Cyber Operations*, Just Security 2021, July 13, 2021 https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/ [dostęp: 20.08.2021].

violate the territorial sovereignty of the penetrated State and/or international law. What is also interesting is that almost all of the countries that accepted this approach practice law under the civil law tradition and the former countries the UK and to a certain degree the US follow the common law tradition.

Regardless of which course SEE States will decide to proceed it is important to underline that in a situation like this, Statements on how sovereignty in cyberspace applies in international law may contribute to the formation of specific customary international law that may focus on or clarify the application of such rules. Furthermore, this is also an opportunity for SEE States to join smaller States such as Austria, Switzerland, or the Czech Republic and with that to strengthen the voices in the ongoing debate and show that small States can be important in expanding State practice and *opinio iuris* in international law.

Cyberspace is a domain where violations of sovereignty rule will continue to occur on a daily basis. While it is true that during the Nicaragua case the International Court of Justice found that frequent violations of a rule do not necessarily detract from its status as a rule of customary international law, the value of States recognizing such a rule without firm *opinion iuris* would surely be seriously undermined by these operations[39]. The lack of legal clarity so far has prevented States from taking legal action in response to cyberattacks[40]. Thus, State-conducted cyberattacks have been left formally unattributed and unchallenged by the law. Unless the leading States in cyberspace take a different more aggressive course the SEE States' decision and with that contribution in *opinion iuris*, regardless of the approach/position will bring hope to enhance international peace and security.

Conclusion

There are both strategic and legal reasons for SEE States to express their position on the applicability of sovereignty to cyberspace. The different approach on the issue among traditional Alliance members is another reason

39 *Military and Puramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986*, https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-BI.pdf [dostęp: 20.08.2021].

40 D. Broeders, E.D. Busser, P. Pawlak, *Three tales of attribution in cyberspace: Criminal law, international law and policy debates*, The Hague Program For Cyber Norms Policy Brief, April 2020, https://eucyberdirect.eu/wp-content/uploads/2020/04/three-tales-of-attribution-in-cyberspace.pdf [dostęp: 20.08.2021].

why its SEE members should take the position and provide clarity. On the other hand, expressing their position on the issue will enhance the threat assessment matrixes and strategic and operational response accordingly. Moreover, economic and practical policy reasons to address the issue extend the strategic importance beyond just security benefits.

Choosing between sovereignty „as a rule" vs. „as a principle" would provide SEE States different legal framework for response. Based on the position on sovereignty SEE States can exercise jurisdictional rights over the physical cyberinfrastructure and can proscribe the conduct of individuals, corporates and other stakeholders in cyberspace that resides within their territorial boundaries.

Indeed, SEE States' positions on disputed issues under international law are not legally binding. It is also true that just because of the SEE States' engagement the issue will not be crystallized, nor the SEE States' position on the applicability of sovereignty will set a legal precedent. Moreover, the SEE position will not confirm attribution or responsibility for malign behavior in cyberspace. However, voicing out the position is important to articulate strategy, propose policy, and conduct diplomacy. Ultimately, a Statement on the issue will broadcast SEE seriousness and will definitely send a message to their allies and adversaries.

Bibliography

Barrinha A., Renard T., *Power and diplomacy in the post-liberal cyberspace*, „International Affairs" 2020, vol. 96, no. 3.

Besson S., *Sovereignty*, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472 [dostęp: 20.08.2021].

Biller J., Schmitt M., *Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences*, https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/#more-16574 [dostęp: 20.08.2021].

Broeders D., Busser E.D., Pawlak P., *Three tales of attribution in cyberspace: Criminal law, international law and policy debates*, https://eucyberdirect.eu/wp-content/uploads/2020/04/three-tales-of-attribution-in-cyberspace.pdf [dostęp: 20.08.2021].

Campbell A., *The Legal Implications of Sony's Cyberhack*, „Oklahoma Journal of Law and Technology" 2015, vol. 11, no. 1.

Demchak C., Dombrowski P., *Cyber Westphalia: Asserting State Prerogatives in Cyberspace*, http://www.jstor.org/stable/43134320 [dostęp: 20.08.2021].

Efrony D., Shany Y., *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, „American Journal of International Law" 2018, vol. 112.

Greenberg A., *It's Been 20 Years Since This Man Declared Cyberspace Independence*, https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/ [dostęp: 20.08.2021].

Herpig S., Schuetze J., Jones J., *Securing Democracy in Cyberspace*, https://www.stiftung-nv.de/sites/default/files/securing_democracy_in_cyberspace.pdf [dostęp: 20.08.2021].
Kadlčák R., *2nd Substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations*, https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf [dostęp: 20.08.2021].
Leader S., *Statehood, Power, and the New Face of Consent*, „Indiana Journal of Global Legal Studies" 2016, vol. 23, no. 1.
Leiner B.M. i in., *Brief History of the Internet*, https://www.internetsociety.org/resources/doc/2017/brief-history-internet/ [dostęp: 20.08.2021].
Madrigal A.C., *The End of Cyberspace*, https://www.theatlantic.com/technology/archive/2019/05/the-end-of-cyberspace/588340/ [dostęp: 20.08.2021].
Perina A.H., *Proceedings of the Annual Meeting, American Society of International Law, The Effectiveness of International Law*, vol. 108, Cambridge 2014.
Richardson H., *Companies 'Must See Cyber Attacks as Inevitable'*, http://www. newsweek.com/companies-must-see-cyber-attacksinevitable-307111 [dostęp: 20.08.2021].
Schmitt M., *France's Major Statement on International Law and Cyber: An Assessment*, https://www.justsecurity.org/66194/frances-major-Statement-on-international-law-and-cyber-an-assessment/ [dostęp: 20.08.2021].
Schmitt M., *Three International Law Rules for Responding Effectively to Hostile Cyber Operations*, https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/ [dostęp: 20.08.2021].
Schondorf R., *Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/ [dostęp: 20.08.2021].
Waxman M.C., *Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)*, „The Yale Journal Of International Law" 2011, vol. 36.
Wright J., *Cyber and International Law in the 21st Century*, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [dostęp: 20.08.2021].

Wypełnienie luki w *opinio iuris* w kwestii suwerenności w cyberprzestrzeni. Wezwanie krajów Europy Południowo-Wschodniej do działania

Streszczenie

Istnieje wiele powodów, żeby kraje Europy Południowo-Wschodniej doprecyzowały swoje oficjalne stanowiska w kwestii możliwości zastosowania suwerenności jako zasady lub reguły prawa międzynarodowego podczas podejmowania próby rozstrzygnięcia problemu rosnącej niejednoznaczności w cyberprzestrzeni. W niniejszym artykule przytoczono argumenty, że ze strategicznego i prawnego punktu widzenia w interesie państw Europy Południowo-Wschodniej leży podjęcie działań i wypełnienie luki w *opinio iuris* (przekonaniu, że określona praktyka jest obowiązującym prawem) na temat możliwości zastosowania suwerenności w cyberprzestrzeni, zwłaszcza po tym, jak niektóre przodujące kraje członkowskie NATO zajęły odmienne stanowisko w tej kwestii. Opisując ewolucję w cyberprzestrzeni oraz to, jak wpływa ona na westfalską koncepcję suwerenności w prawie międzynarodowym, artykuł pokazuje znaczenie głównej tezy. Następnie przedstawia

jej uzasadnienie i wyjaśnia, dlaczego w interesie krajów Europy Południowo-Wschodniej leży podjęcie działań i zajęcie stanowiska w kwestii możliwości zastosowania suwerenności w cyberprzestrzeni na gruncie prawa międzynarodowego.

Słowa kluczowe: prawo międzynarodowe, suwerenność, cyberprzestrzeń, NATO, kraje Europy Południowo-Wschodniej, strategia