2024, Vol. 13, Issue 1

Dr hab. prof. UKSW Łukasz Kułaga

Cardinal Stefan Wyszyński Univerity in Warsaw

ORCID 0000-0003-0784-8293

MAPPING THE POSITION OF STATES ON THE APPLICATION OF SOVEREIGNTY IN CYBERSPACE

Abstract: The article analyses views of states on application of sovereignty in cyberspace taking into account rising number of states' individual and collective positions in this respect. It identifies three major models of sovereignty: sovereignty as an international authority, sovereignty as only a principle and sovereignty as not only a principle. Against this background it aims at explaining the rule-principle dichotomy and consequences of its application. Finally, it distill converging components concerning the application of sovereignty in cyberspace. Such an exercise allows for delimiting the scope of application sovereignty as a rule in cyberspace vis-à-vis other norms of general international law.

Keywords: sovereignty, non-intervention, cyberspace, principle-rule distinction

1. Introduction

In the international order where under the influence of globalization the significance of international borders have started to blur, and the role of states themselves has diminished in favour of transnational entities, the importance of states' sovereignty has become somewhat hazy.[1] This context has also influenced initial considerations on the role of sovereignty in the cyber context.[2] As such cyberspace is often defined as an area without borders, a system of fast communications and transfer of data which is alien

1 Viñuales, *The UN Friendly Relations Declaration at 50. An Assessment of the Fundamental Principles of International Law*.

2 Tsagourias, "Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace".

to the difficulties of our off-line existence, including the problem of geography. As one of the processes closely related to globalization, the phenomenon of cyberspace appears to be conceptually and functionally distant from the traditional idea of state sovereignty.[3] The internet's pioneers stressed its qualitative difference from the classical sovereignty-based international order.[4]

Perhaps for these reasons in 1999 the United States Department of Defence assessed that it is too early to confirm that sovereignty applies to cyberspace in a similar way as it is applicable in other domains. 25 years later the bulk of state positions clearly lean towards acknowledging such an application. Still, such an approach is not acceptable by all and significant minority reports in this matter exist. Surprisingly, those views are on two ends of the spectrum: one advocates for absolute sovereignty in cyberspace while the other favours its complete non-application. The question has not been settled yet at the international level. The 2015 Group of Governmental Experts (GGE) consensus reports referred to the importance of sovereignty in cyberspace, however, without a precise explanation on how it should be understood both in theoretical as well as practical terms.[5]

There are a number of studies on the application of sovereignty in cyberspace. Undoubtedly, many of these analyses provide a valuable insight on the spectrum of problems related to the application of sovereignty in the sphere in question.[6] This article will concentrate on the views

3 If you want to achieve sovereignty in cyberspace, you cannot leave that system in place. You must either sever all digital connections with the outside world and be the supreme ruler of a digital island, or fight with other states to be the one sovereign over global cyberspace, Milton Mueller Hague Keynote: Sovereignty in Cyberspace, https://www.internetgovernance.org/2020/11/13/hague-keynote-sovereignty-in-cyberspace; see also Barlow, "A declaration of the independence of cyberspace".

4 Schmitt, Vihul, "Respect for Sovereignty in Cyberspace"; Schmitt, *Tallinn Manual 2.0*; Moynihan, "The Application of International Law to State Cyberattacks"; Kushwaha, Roguski, Watson, "Sovereignty and Non-intervention Up in the air: ensuring government data sovereignty in the cloud".

5 *State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory*, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, para 27; GGE Report 2021, A/76/135, para 71.

6 Corn, Taylor, "Sovereignty in the Age of Cyber", 207-212; Tsagourias, Buchan, *Research Handbook on International Law and Cyberspace*, 99-103; Broeders, *Digital Sovereignty: From Narrative to Policy?*; Chatinakrob, "Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty".

of states bearing in mind that, particularly in the last five years, the practice of formulating positions in this area has clearly intensified. 27 states individually and 55 African Union (AU) states jointly have articulated their position on sovereignty in cyberspace. Furthermore, the article demonstrates the two-dimensional character of the discussion around the applicability of international law, in particular sovereignty in cyberspace. On the one hand, it requires taking into account the specificity of conduct in cyberspace itself to confront it with the applicable general international law. On the other hand, however, it requires reflection on how states understand, also in the kinetic sphere, the fundamental norms of general international law.

2. Sovereignty, Sovereign Equality, Territorial Sovereignty – Concept, Principle and Rule of International Law

It is uncontroversial that sovereignty is a fundamental concept in international law. The international legal order is based on sovereignty, which is an essential, if not key element of its validity. Indeed, it is from sovereignty that stems the ability of states, the main subjects of international law, to create international law, and thus at the same time to be bound by it.[7] Such a perception of sovereignty leads to its description as a 'pivotal concept', 'principle about international law',[8] 'consequence of statehood, namely, the plenary competence that States prima facie possess',[9] 'fundamental term of international law',[10] a notion similar to freedom, equality or justice[11] and 'the term (...) descriptive in character, referring in a 'catch-all' sense to the collection of rights held by a state'.[12] Simultaneously, some authors who emphasize the descriptive meaning of sovereignty explicitly question the possibility of recognising its normative value.[13]

7 *SS Wimbledon (Government of his Britannic Majesty v German Empire)*, PCIJ Series A, No. 1, para 25.

8 Besson, "Sovereinty", para 3 and 86.

9 Crawford, *Creation of States*, 89.

10 Kwiecień, *Suwerenność państwa. Rekonstrukcja i znaczenie idei w prawie międzynarodowym* [Sovereingty of State, Reconsutruction and the Importance of the Idea in International Law], 95.

11 Kranz, *Pojęcie suwerenności we współczesnym prawie międzynarodowym [The Concept of Sovereingty in International Law]*, 50.

12 Crawford, *Browlnie's Principles of Public International Law*, 448; cf Crawford, *Chance, Order, Change: The Course of International Law. General Course on Public International Law (2013)*, 127; similarly Jennings, Watts, *Oppenheim's International Law: Peace*, 385-86.

13 Crawford, "Sovereignty as a Legal Value", 122.

In order to situate the normative meaning of sovereignty, it is important to refer to the distinction of norms of international law between rules and principles. According to Gerald Fitzmaurice, 'a rule answers the question 'what', a principle in effect answers the question 'why'.[14] For Matti Koskenniemi the difference between rules and principles denotes a lower or higher degree of abstraction.[15] In its draft conclusions on the identification of customary international law, the International Law Commission, following the judgement of International Court of Justice (ICJ) in Delimitation of the Maritime Boundary in the Gulf of Maine Area,[16] emphasized 'more general and more fundamental character' of principles as comparing to rules.[17]

Against this background, there is a fairly widespread acceptance that sovereignty, as a norm, is a principle of international law.[18] As Samantha Besson aptly notes 'most sovereignty rights and duties are usually derived from the principle of sovereign equality'.[19] Similarly Roman Kwiecień acknowledges that principle of sovereign equality of states is a source of an autonomous principle of international law.[20]

Furthermore, sovereignty was also applied as a rule by international courts and tribunals. In the *Corfu Channel case* the ICJ affirmed that:

> [b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations (...) to ensure respect for international law, of which it is the organ, the Court must declare that the action of the British Navy constituted a violation of Albanian sovereignty.[21]

14 Fitzmaurice, *The General Principles of International Law Considered from the Standpoint of the Rule of Law*, 7; Similarly: 'Rules are applicable in an all-or-nothing fashion ... the principle is one which [one] must take into account, if it is relevant, as a consideration inclining in one direction or another', Dworkin, *Taking Rights Seriously*, 42.

15 Fragmentation Of International Law: Difficulties Arising From The Diversification And Expansion Of International Law, Report of the Study Group of the International Law Commission Finalized by Martti Koskenniemi, A/CN.4/L.682 13 April 2006, p. 20.

16 *Delimitation of the Maritime Boundary in the Gulf of Maine Area*, Judgment of 12 October 1984, ICJ Reports 1984, para 79.

17 Commentary to conclusion 1 of the draft conclusion on identification of customary international law, A/73/10 para. (3).

18 Besson, ibidem, para 86.

19 Ibidem, para 115.

20 Kwiecień, ibidem, 56-57.

21 *Corfu Channel Case*, Judgment on Preliminary Objection, ICJ Reports 1948, p. 35.

The Court referred to possible violations of sovereignty also in the *Nicaragua case*[22] and certain activities carried out in the border area.[23] In all of these cases, the ICJ referred to sovereignty and territorial sovereignty as a rule that can be violated. This approach was also followed by some scholars.[24] According to Shaw:

> Territorial sovereignty has a positive and a negative aspect. The former relates to the exclusivity of the competence of the state regarding its territory, while the latter refers to the obligation to protect the rights of other states.[25]

To conclude there are a variety of approaches to sovereignty in academia. Still, there is an agreement that sovereignty is not only a fundamental term or concept for international law but also, at least in the form of sovereign equality of states, a principle of international law. Furthermore, international courts and tribunals[26] unequivocally applied sovereignty or territorial sovereignty as a legal rule.

3. Positions of States with respect to the Application of Sovereignty to Cyberspace

In the positions presented by states concerning the application of international law to cyberspace, three major models of sovereignty can be traced: sovereignty as an international authority, sovereignty as only a principle and sovereignty as not only a principle. When introducing these three models a caveat has to be made as some legal positions of states are not clear-cut in this respect.

22 *Military and Paramilitary Activities in and Against Nicaragua, Nicaragua v United States*, Merits, Judgment of 27 June 1986, ICJ Reports 1986, para 251.

23 *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua; Construction of a Road in Costa Rica along the San Juan River (Nicaragua v Costa Rica)*, Judgement of 16 December 2015, ICJ Reports 2015, para 66-69, 113 and 229.

24 Verdross, Sinma, Geiger, "Territoriale Souveranitdt und Gebietshoheit, Ósterreichisches Zeitschnft fur óffentliches Recht und Yólkerrecht"; Shaw, *International law*, 490; Anand, *Sovereign Equality of States in International Law*, 28.

25 Shaw, ibidem, 490.

26 'Both Parties are in agreement that the islands in dispute initially all fell under the territorial sovereignty of the Ottoman Empire', *Award of the Arbitral Tribunal in the first stage of the proceedings between Eritrea and Yemen (Territorial Sovereignty and Scope of the Dispute)*, Decision of 9 October 1998, Recueil des sentences arbitrales, vol. XXII, p. 209-332.

Notwithstanding the model, there exists an agreement that sovereignty is connected with several other norms of international law. In particular, states indicated the prohibition of intervention in internal affairs,[27] the right to self-determination,[28] the prohibition on the use of force[29] and the right to self-defence.[30] For China, the principle of sovereignty is also connected with the 'management and distribution of international Internet resources on equal footings',[31] whereas Austria considers that sovereignty protects also governmental data stored in data embassy situated in a third state.[32]

3.1. Sovereignty as an Internal Authority

Sovereignty as an internal authority model concentrates on the right to control the functioning of cyberspace and its use by private individuals.[33] The specificity of this model entails an emphasis on an understanding of sovereignty not only in the context of inter-state relations or international law in general but rather in the domestic context relation state versus the individual.[34] For example, China through a series of legal acts enacted

27 Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, p. 23-25 [Estonia 2021]; Government of Denmark, 'Denmark's Position Paper on the Application of International Law in Cyberspace' (4 July 2023) [Denmark 2023]; Government of the Kingdom of the Netherlands, Appendix: International law in cyberspace, 26 September 2019, [Netherlands 2019]; New Zeland, The Application of International Law to State Activity in Cyberspace, 1 December 2020 [New Zeland 2020]; Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, p. 67-68 [Norway 2021]; The Republic of Poland's position on the application of international law in cyberspace, Ministry of Foreign Affairs of Poland, 29 December 2022, 4., [Poland 2022]; Government Offices of Sweden, Position Paper on the Application of International Law in Cyberspace, July 2022 [Sweden 2022].

28 Italian position paper on 'International law and cyberspace', Italian Ministry for Foreign Affairs and International Cooperation. [Italy 2021], implicit Federal Government of Germany, 'On the Application of International Law in Cyberspace', Position Paper (March 2021) [Germany 2021].

29 Estonia 2021, Denmark 2023; New Zeland 2020, Norway 2021; Sweden 2022.

30 Denmark 2023; Netherlands 2019.

31 China's Positions on International Rules-making in Cyberspace, Ministry of Foreign Affairs of the People's Republic of China 2021.

32 Position Paper of the Republic of Austria: Cyber Activities and International Law, April 2024 [Austria 2024], p. 16.

33 Moynihan, "The vital role of international law in the framework for responsible state behaviour in cyberspace", 401.

34 Broeders, Adamson, Creemers, "Coalition of the unwilling? Chinese and Russian perspectives on cyberspace", 1-3.

in the last decade established the so-called Great Firewall in order to block citizens' access to or censor selected foreign websites.[35] In its statements China highlighted 'internal supremacy' and 'exclusive sovereign rights in cyberspace'.[36] Furthermore, the emphasis on entitlement 'to administer cyberspace in accordance with law'[37] seems to refer rather to domestic than international law. In 2019 Russia enacted 'Russia's sovereign internet' law in order to control Russian internet traffic and allow for cutting Russia off from the global internet in case of an emergency.[38] Furthermore, in 2023 Russia presented its updated concept of the UN convention on ensuring international information security. The document uses rather specific terminology such as 'social and economic stability of sovereign States' (para II.1) and

> sovereign right of each State to ensure security of national information space and to establish norms and mechanisms in order to manage its information and cultural space in accordance with national legislation (para III.1).[39]

Such an approach is based on the general vision of international law by China and Russia. Already in 1999, they criticized 'concepts of human rights are superior to sovereignty'.[40] The 2014 Declaration of the People's Republic of China and the Russian Federation on the Promotion of International Law does not mention human rights at all.[41] In 2022 both states indicated that:

> They oppose the abuse of democratic values and interference in the internal affairs of sovereign states under the pretext of protecting democracy and

35 Przychodniak, "China's Internet Policy"; Creemers, "China's Conception of Cyber Sovereignty – Rhetoric and Realization", 118-119.

36 China's Views on the Application of the Principle of Sovereignty in Cyberspace, Ministry of Foreign Affairs of the People's Republic of China, p. 3. [China 2021]

37 International Strategy of Cooperation on Cyberspace 2017, http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm.

38 Federal Law No. 90-FZ, dated May 01, 2019 On Amending the Federal Law 'About Communications' and the Federal law 'About Information, IT and Information Protection'; see also O'Hara, Kieron, "Policy Question: Is a Sovereign Internet Feasible?", Four Internets: Data, Geopolitics, and the Governance of Cyberspace (New York), 2021, p. 173-176.

39 https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf.

40 Sino-Russian Joint Statement (Dec 10, 1999).

41 https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/201608/t20160801_679466.html.

> human rights, and any attempts to incite divisions and confrontation in the world. The sides call on the international community to respect cultural and civilizational diversity and the rights of peoples of different countries to self-determination.[42]

To some extent, the described model resembles Bodin's doctrine of absolute sovereignty understanding as power above the law.[43] In a very limited way such an approach takes into account the need to exercise control over the Internet in accordance with international law. As a result, it is difficult to reconcile with basic parameters of international law. As it was mentioned in the *Wimbledon case* and later approved by the General Assembly resolution 'Declaration of rights and duties of states' from 1949:

> Every State has the duty to conduct its relations with other States in accordance with international law and with the principle that the sovereignty of each State is subject to the supremacy of international law.[44]

This position was also highlighted by several states in particular in the context of application of sovereignty to cyberspace.[45]

3.2. Sovereignty as only a Principle Model

The second model considers sovereignty as a principle, which cannot be violated *per se*, as it is not a rule of law. The most famous exemplification of this approach is the statement of the UK Attorney General in 2018 according to which:

42 Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development of 4 February 2022. Another passage of the statement that needs particular assessment indicates: 'as every nation has its own unique national features, history, culture, social system and level of social and economic development, universal nature of human rights should be seen through the prism of the real situation in every particular country, and human rights should be protected in accordance with the specific situation in each country and the needs of its population'.

43 Bodin, *On Sovereignty: Six Books Of The Commonwealth*.

44 https://legal.un.org/ilc/texts/instruments/english/commentaries/2_1_1949.pdf.

45 Estonia 2021; African Union Peace and Security Council, "Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace" (29 January 2024) [African Union 2024], para 12; Germany 2021, Irish Department of Foreign Affairs, Position Paper on the Application of International Law in Cyberspace (6 July 2023) [Ireland 2023] para 7, Italy 2021; Sweden 2022; Austria 2024, p. 4 and 13.

> Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.

A similar approach seems to be presented by Australia.[46] Israel indicated a lack of readiness at this moment to accept that territorial sovereignty as a rule is applicable to cyberspace.[47] Still, Israel differentiates between a sovereignty as a concept and territorial sovereignty as a rule.[48]

The United States opinion in this respect is less clear. One could have an impression that it somehow tries to bridge position 'sovereignty as only principle' with position 'sovereignty as not only a principle'. In 2020, the United States stated that

> States have sovereignty over the information and communications technology infrastructure within their territory. The implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law.[49]

Such an approach is certainly not as straightforward as the UK one. It can be interpreted that while the infringement of sovereignty in the kinetic world involves a violation of international law the situation is different in cyberspace. Such an approach would entail that the meaning of state sovereignty is significantly different in the cyberspace domain than in other domains. The other possible interpretations would have to concentrate on

46 2017 – Australia's Position On The Application Of International Law To State Conduct In Cyberspace, https://www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf.

47 'there are diverging views regarding whether sovereignty is merely a principle, from which legal rules are derived, or a binding rule of international law in itself'. 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/.

48 Ibidem.

49 Paul C. Ney, Jr., Dep't Def. Gen. Counsel, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://perma.cc/QY33-NEMY.

the meaning of the term 'infringement', which was used instead of 'breach' or 'violation'. Still, it can also be interpreted that there can exist infringements on sovereignty in cyberspace (even if only some and not all) that involve violations of international law. This would be in line with the US statement from 2021

> In certain circumstances, one State's non-consensual cyber operation in another State's territory, even if it falls below the threshold of a use of force or non-intervention, could also violate international law.[50]

Nevertheless, it was not explained what kind of rules of international law would be violated in such a situation.

What unites states sceptical on the applicability of sovereignty as a rule is a conviction that the non-intervention principle is the most well-suited international law norm to protect state sovereignty in cyberspace.[51]

3.3. Sovereignty as not only a Principle Model

Sovereignty as not only a principle model seems to be a predominant perspective. The position of states refers to territorial sovereignty[52] or state sovereignty.[53] Occasionally, however, these terms are used interchangeably.[54] Still, this approach does not necessarily exclude recognition of sovereignty as a principle. It rather considers that it can be both a principle and a rule.[55]

50 Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, 140.

51 See for example United Kingdom 2021.

52 African Union (2024), para 14-16.

53 Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, p. 18 [Brazil (2021)]; Finland 2020, France 2019; Iran 2020; Ireland 2023 para 5; Italy 2021; Japan 2021; Netherlands 2019; Poland 2022; Romania 2021; Singapore 2021; Switzerland 2021; Austria 2024; Documento De Posición De La República De Cuba Sobre La Aplicación Del Derecho Internacional A Las Tecnologías De La Información Y Comunicación En El Ciberespacio, La Habana, 28 de junio de 2024 [Cuba 2024], para 2 – but see para 3 and 27.

54 New Zealand 2020; Norway 2021.

55 Government of Canada, International Law applicable in cyberspace, April 2022 [Canada (2022)] ('principle of sovereignty applies in cyberspace', para 10; 'Territorial sovereignty is a rule under international law'; Ministry of Foreign Affairs of Costa Rica, 'Costa Rica's Position on the Application of International Law in Cyberspace' (21 July 2023), para 18-19 [Costa Rica 2023]; Ministry of Foreign Affairs of the Czech Republic, 'Czech Republic – Position paper on

Interestingly, China on the one hand underlines that sovereignty is a principle but on the other hand it implicitly seems to accept that it functions also as a rule.[56] Exceptionally, Canada indicated that as a rule it considers only territorial sovereignty and not sovereignty as such.[57] The approach of states toward the principle of sovereign equality of states in this context is less clear. Some emphasize the existence of two principles: sovereignty and sovereign equality of States[58] or independence and sovereign equality of States.[59] For others, sovereign equality of States constitute an aspect of external sovereignty[60] or an element of state sovereignty.[61] Exceptionally, Iran is of the view that the state's sovereignty is subject to the principle of equality.[62]

Furthermore, certain states acknowledge the distinction between internal and external dimensions or aspect of sovereignty.[63] Germany implicitly labels these dimensions as territorial sovereignty and political independence.[64]

All positions which refer to this issue indicate that sovereignty applies to inter-state relations. Simultaneously, there is an agreement that it can be violated also by conduct towards private individuals.[65]

4. Sovereignty in Cyberspace – Principle or Rule – Understanding the Genesis of the Positions and Consequences of its Application

Noting three perspectives on the application of sovereignty in cyberspace it is worth reminding ourslves that most states have not yet expressed their position in this respect. The first of the positions in fact disregards

---

the application of international law in cyberspace' (27 February 2024) [Czech Republic 2024], para 3; Government of Denmark, 'Denmark's Position Paper on the Application of International Law in Cyberspace' [Denmark 2023]; Finland 2020; New Zealand 2020; Norway 2021.

56 'A violation of the principle of sovereignty, which will constitute a wrongful act under international law' similarly Poland 2022; Romania 2021.

57 Canada 2022, para 10-11.

58 Czech Republic 2024, para 1.

59 AU 2024 para 17.

60 Denmark 2023.

61 Ireland 2023, para 4.

62 Iran 2020, para 5.

63 Netherlands 2019; Italy 2021; Norway 2021; Poland 2022; Romania 2021.

64 Germany 2021.

65 Iran 2020, para 3; Ireland 2023, para 6; Norway 2021; Poland 2022; Sweden 2022; Switzerland 2021.

an established understanding of the relationship between sovereignty and international law this part of the article will concentrate on the latter two.

The question is whether in cyberspace the sovereignty of states is protected by a rule of sovereignty or only by the principle of non-intervention in domestic affairs. The support for the latter is emphasized by states, which do not consider sovereignty as a rule. The growing prominence of the principle of non-intervention in the position of certain Western states is surprising since in the second half of the 20th century it was referred to primarily against the conduct of the Western states, particularly in situations when they promoted the observance of international human rights law. The first state which after 1945 broadly invoked this principle to protect its alleged rights was South Africa's apartheid regime. Up until today, the violation of the non-intervention principle is used as a shield and main argument of defence by states that do not respect the fundamental norms of international law and consequently are subjected to a variety of sanctions.

The protagonists of the sole non-intervention principle as an instrument of protection of states' sovereignty put forward the following arguments:

- Sovereignty as a rule is not a precise norm – in particular, it is not clear where to draw the minimum threshold for its violations.[66] In general, interacting with a computer system can always cause some manipulations.
- The potentially all-encompassing character of sovereignty could lead to an inflation of international law breaches through actions in cyberspace.[67] Such a situation could put governments in an uncomfortable position of the need to explain before public opinion what response will be taken and whether this response is adequate and could have a deterrent effect. It could lead to an escalation of international conflicts.
- From an offensive perspective context, catch-all sovereignty leads to a situation in which offensive or active defence actions can easily be identified as violations of the rule.[68] This can limit the range of available options which states would like to use.[69] A classic

66 Corn, Taylor, ibidem, 207-212.

67 Moynihan, "The vital role of international law in the framework for responsible state behaviour in cyberspace", 20; Heller, "In Defense of Pure Sovereignty in Cyberspace", 1486-1487.

68 Goldsmith, Loomis, "'Defend Forward' and Sovereignty", 10-15.

69 Schmitt, Durward, "Responding to Hostile Cyber Operations: The "In-Kind" Option", 100-101.

understanding of sovereignty in the cyber context does not leave states significant operational room for manoeuvre.

- Conversely, the principle of non-intervention enables one to conclude that only very specific, perhaps flagrant breaches of state sovereignty – below the use of force threshold – will constitute a violation of international law.[70] Certain states agreed that a breach of sovereignty would be easier to prove than a violation of the non-intervention principle.[71] When emphasizing the sole applicable rule, non-intervention gives states considering possible offensive/active defence actions, a significant margin of appreciation as there could be a broad scope of activities which would not regulated by international law, in particular not covered by a non-intervention norm.

Simultaneously, some substantial counterarguments to the above presented line of thinking can be advanced:

- States favouring the rule model seem to be aware of a certain lack of a precise scope of sovereignty in cyberspace. As stated by the Netherlands in this respect: 'precise boundaries of what is permissible have yet to fully crystalize'.[72] It is also for that reason States often use in their position a 'saving clause' that certain assessments are to be made on a case-by-case basis.[73] Still, both the growing practice of producing a national position as well as the discussion conducted within the GGE and the OEWG certainly solidify an understanding of sovereignty in this sphere.
- Below the use force threshold principle of non-intervention is similarly, if not even more difficult to apply than territorial sovereignty. This flows from the fact that their precise contours are unclear. Such a view was already confirmed by the academia in the context of its offline application. According to Vaughan

70 'The United Kingdom does not consider that the general concept of sovereignty by itself provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention referred to above', United Kingdom 2021.

71 Japan 2021; Poland 2022; Norway 2021.

72 Netherlands 2019; similarly New Zealand 2020 and Switzerland 2021 'defining what constitutes a violation of the principle of sovereignty in cyberspace is particularly challenging and has yet to be clarified conclusively'.

73 France 2019; Finland 2020; New Zealand 2020; Germany 2021; Italy 2021; Norway 2021; Switzerland 2021; Canada 2022, para 21; Sweden 2022; Denmark 2023; Ireland 2023, para 6; Czech Republic 2024, para 5.

Lowe it is 'One of the most potent and elusive of all international principles'[74] . Michal Wood and Maziar Jamnejad indicate that 'it is uncertain in scope'.[75] Such an approach can be a consequence of the fact that the Nicaraguan judgement of the ICJ – considered the most pertinent precedent– is still rather laconic and vague as regards the application of the principle. The term 'coercion' below the use force threshold was not defined by the Court at all. Following the *Nicaragua* interpretation would lead to a conclusion that the principle could find possible application in cyberspace only to a limited spectrum of activities, in particular to cyberattacks significantly and genuinely affecting elections or exercise of the most pertinent governmental competencies which can be considered as having an effect of subordination of the state concerned. Thus, besides the famous term 'dictatorial interference' in the functioning of the state, the scope of the principle is rather vague.[76] Attempts made to clarify its nature, in particular Marko Milanovic's concepts of extortion and control, although commendable, still need to find confirmation in international practice.[77]

- Sovereignty and non-intervention share two-dimensional normative character. They are both principles and simultaneously a rule of international law. As principles, they set the direction of interpretation. As rules, they can be directly applied to a particular situation. Both of these norms, have from the perspective of the theory of law the same quality. As a result, they both share the same difficulties regarding their interpretation and application whether online or offline. Still the practices of a national position, which is growing, despite different levels of their granularity, gradually set basic boundaries for their application in the context of cyberspace.
- Recognising that sovereignty as a rule does not apply to cyberspace and upholding the classical understanding of the non-intervention principles denotes that the scope of state's rights protected online would be limited compared to non-virtual reality.

74 Lowe, *International Law*, 104.
75 Jamnejad, Wood, "The Principle of Non-intervention", 380-381.
76 Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention".
77 Milanovic, "Revisiting Coercion as an Element of Prohibited Intervention in International Law".

- The consequences of the position that only the principle of non-intervention appplies to cyberspace without its redefinition can lead to a significant shift in a broader perspective. A number of the state's behaviours may no longer be classified as a breach of international legal obligations but only as malicious activities[78] or acts of international vandalism.[79] These terms, no matter how laudable they sound before public opinion, are to a large extent devoid of strict legal consequences.[80] If there is no breach, there is no responsibility – countermeasures and due diligence obligations are not applicable options[81] as well as mechanisms of dispute settlement.

5. Components of Sovereignty/Territorial Sovereignty

Analyses of the position of states enables distinguishing certain components concerning the application of sovereignty in cyberspace. Distilling these converging elements allows for delimiting the scope of application sovereignty as a rule in cyberspace vis-à-vis other norms of general international law. Moreover, it enables one also to identify potential differences in the positions presented.

5.1. Jurisdiction

There is an agreement between states that by virtue of territorial sovereignty, states are entitled to exercise all kinds of jurisdiction towards cyberspace

78 Statement by the North Atlantic Council concerning malicious cyber activities against Germany and Czech Republic. 03 May 2024, https://www.nato.int/cps/en/natohq/official_texts_225229.htm.

79 Similarly, the position of Finland: 'agreeing that a hostile cyber operation below the threshold of prohibited intervention cannot amount to an internationally wrongful act would leave such operations unregulated and deprive the target State of an important opportunity to claim its rights."'https://ccdcoe.org/uploads/2018/10/Finland_International-law-and-cyberspace_national-positions_ENG.pdf.

80 A good example of such an approach are the elucidations contained in the Advancing Cyberstability Final Report November 2019 such as 'the Commission merely affirms that election interference is intolerable whether it is considered to be a violation of international law or not', p. 33.

81 Similarly, Milanovic, Schmitt, "Attacks and Cyber (Mis)information Operations during a Pandemic", 281.

components that are located on their territory.[82] These prerogatives would also apply to aircrafts, ships flying the State's flag and space objects registered by the state.[83]

5.2. Unauthorized Access

In this respect, a significant divergence in the positions of states is discernible. Views are expressed that simple unauthorized access is a breach of international law.[84] Such an approach agrees also that sovereignty can be breached by causing harmful effects by cyberspace conduct.[85]

AU States are of the view that unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State is always unlawful.[86] A similar position is presented by Brazil according to which there exists no customary rules on the application of sovereignty to cyberspace that would envisage any particular exceptions or thresholds. Thus, as an example of a breach of international law it considers the interception of telecommunications.[87] For France 'Any cyberattack against French digital systems or any effects produced on French territory by digital means (...) constitutes a breach of sovereignty'.[88] Conversely, according to Austria, limited intrusion may constitute a violation in this respect only when it negatively affects the functioning of the state's ICT infrastructure.[89] Still, the opposite view is also expressed that:

> remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a *per se* violation of international law. In other words, there is no absolute prohibition on

82 African Union 2024, para 14; Austria 2024, p. 4; China's Positions on International Rules-making in Cyberspace, Ministry of Foreign Affairs of the People's Republic of China. Costa Rica 2023, para 18; Denmark 2023; Estonia 2021; Finland 2020; Germany 2021; France 2019; Iran 2020, para 2; Ireland 2023, para 4; Italy 2021; Netherlands 2019; Norway 2021; Poland 2022; Sweden 2022; P.C. Ney, Jr., Dep't Def. Gen. Counsel, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020).

83 African Union 2024, para 14.

84 China's Views on the Application of the Principle of Sovereignty in Cyberspace, Ministry of Foreign Affairs of the People's Republic of China, p. 3.. 2021.

85 African Union 2024, para 16. Brasil 2021.

86 African Union 2024, para 16.

87 Brasil 2021.

88 France 2019 similarly to Romania 2021.

89 Austria 2024, p. 4-5.

such operations as a matter of international law. This is perhaps most clear where such activities in another State's territory have no effects or *de minimis* effects.[90]

This position will be elaborated on in the next section.

5.3. Causing Harmful Effects

For some states causing harmful effects through cyber means is crucial in identifying violations of sovereignty. Canada, the Czech Republic and Denmark require proof of 'Cyber activities that rise above a level of negligible or *de minimis* effects, causing significant harmful effects'.[91] Such conduct could entail cyber activity that 'necessitates the repair or replacement of physical components of cyber infrastructure in the affected State'.[92] In particular conduct below the mentioned threshold is not a breach of international law even if it causes some loss of functionality and 'requires rebooting or the reinstallation of an operating system'.[93] Ireland however does not exclude that interference with data can be considered a violation of the state's sovereignty.[94]

According to Costa Rica, a breach of sovereignty would not only exist in a situation of physical damage but also 'loss of functionality of cyber infrastructure located in the victim State, regardless of ownership'. The latter

90 United States 2016 and 2021; Similarly New Zealand 2020 and Canada 2022, para 15 ('territorial sovereignty is not violated by virtue merely of remote activities having been carried out on or through the cyber infrastructure located within the territory of another State').

91 Government of Canada, International Law applicable in cyberspace, April 2022 [Canada 2022], para 15-16; Czech Republic 2024, para 5; Denmark 2023.

92 Canada 2022, para 16.

93 Canada 2022, para 17; similarly, 'physical effects and harm in the territory of another State constitute a violation of that State's territorial sovereignty (...) negligible physical effects and functional impairments below a certain impact threshold cannot – taken by themselves – be deemed to constitute a violation of territorial sovereignty', Germany 2021; Requiring 'significant harmful effects manifesting on the territory of another state'. Conversely, 'territorial sovereignty as applied in the cyber context does not prohibit states from taking necessary measures, with minimally destructive effects', New Zealand 2020. 'Causing serious adverse effects within the territory of a state, such actions should be considered a violation of the principle of sovereignty, irrespective of whether such effects are of kinetic nature or are limited to cyberspace', Poland 2022 para 2. 'The principle in question prohibits a State from conducting cyber operations, which produce harmful effects on the territory of another State', Italy 2021.

94 Ireland 2023, para 6.

could relate to operating system or database.[95] Similarly, Norway considers the violation of sovereignty in situation of 'use of crypto viruses to encrypt data and thus render them unusable for a substantial period of time'[96] as well as Sweden.[97]

The Czech Republic sets a significantly higher threshold than only loss of functionality by indicating the need for 'significant impact on national security, economy, public health, public safety or environment'.[98] Exceptionally, for Iran the violation of sovereignty would happen in the situation of 'destabilization of national security'.[99]

5.4. Interferences with Governmental Function

The component, resembling the issues protected also by the principle of non-intervention, concentrates on the influence of cyber activities on the exercise of governmental functions.[100] As governmental functions can be considered amongst others 'health care services, law enforcement, administration of elections, tax collection, national defence and the conduct of international relations, and the services on which these depend.[101] It would appear that the violation of territorial sovereignty in the case of direct impacts on governmental functions could be easier to ascertain.[102] According to AU States, territorial sovereignty prohibits exercising of enforcement authority

95 Costa Rica 2023, para 20.

96 Norway 2021; Schmitt, "Foreign Cyber Interference in Elections", 752.

97 'Interfering with data without causing physical harm may also violate sovereignty', Sweden 2022.

98 Czech Republic 2024, para 6b.

99 Iran 2020, para 3.

100 Austria 2024, p. 4; China's Positions on International Rules-making in Cyberspace, Ministry of Foreign Affairs of the People's Republic of China; Czech Republic 2024, para 5; Denmark 2023; Netherlands 2019; Sweden 2022.

101 Canada 2022, para 18.

102 For example, Norway 2021 'what matters is not whether physical damage, injury, or loss of functionality has resulted, but whether the cyber operation has interfered with data or services that are necessary for the exercise of inherently governmental functions. Cases in point would include altering or deleting data or blocking digital communication between public bodies and citizens so as to interfere with the delivery of social services, the conduct of elections, the collection of taxes, or the performance of key national defence activities'; Canada is of the view that 'There can be a violation of territorial sovereignty by way of effects on governmental functions regardless of whether there is physical damage, injury, or loss of functionality', Canada 2022, para 18; similarly, Costa Rica 2023, para 20-21; Czech Republic, para 5 (however compare in para 6c a standard of 'significantly disrupting the exercise of those functions').

on the territory of a foreign state by applying ICTS in cyberspace, even if such conduct does not have harmful effects.[103] Interestingly, the AU States seem to also exclude the possibility of exercising such an authority by virtue of countermeasure.[104] Such a position seems to be difficult to reconcile with the law of state responsibility. According to Article 50 of ARSIWA obligations not affected by countermeasures do not include territorial sovereignty.

5.5. Due Dilligence

Although considered a self-standing norm of international law – due diligence is sometimes also framed by states as strictly connected to state sovereignty.[105] Such an approach flows from at least two considerations. First of all, sovereignty does not absolve states from international law obligations, including respect for the sovereignty of other states. In this line of thinking, due diligence would be an expression of observance of the sovereign rights of other states.[106] Second, the jurisdiction that flows from sovereignty does not entail only rights but also responsibilities. The competences of states to exercise powers on their territory give rise to a presumption of state responsibility for harmful acts that may originate from its territory.[107] Still, certain states explicitly indicated that they do not consider due diligence as binding, in general or in the cyber context.[108]

Furthermore, it is to be noted that due diligence in the context of cyberspace is considered not only from the perspective of hard law but also as a soft law norm. Indeed, the 2015 GGE report labelled it as one

103 African Union (2024), para 15.

104 'International law, as it applies to the use of ICTs in cyberspace, does not permit a State to exercise enforcement authority on the territory of a foreign State in response to unlawful cyber activities that emanate from the territory of that foreign State', African Union (2024), para 15.

105 Sweden 2022; Poland 2022; African Union 2024, para 21; Australia 2020; Costa Rica 2023, para 27; Czech Republic 2024, para 15; Denmark 2023; Estonia 2021; Germany 2021; Ireland 2023; Netherlands 2019; Norway 2021; Switzerland 2021.

106 Cf. '[t]erritorial sovereignty ... has as corollary a duty: the obligation to protect within the territory the rights of other States', *Island of Palmas case (Netherlands v USA)*, Permanent Court of Arbitration (PCA), Final Award of 4 April 1928.

107 'A State's authority and jurisdiction include a responsibility not to allow knowingly its territory to be used for acts contrary to the rights of other State', Sweden 2022.

108 '[w]hether this norm also reflects a binding legal obligation is not settled. ... New Zealand is not yet convinced that a cyber-specific 'due diligence' obligation has crystallized in international law.' New Zealand 2020.] A similar position was presented by the United Kingdom, Canada, Israel and Argentina – Moynihan, "Unpacking due diligence in cyberspace', 6-7.

of the voluntary, non-binding norms, rules or principles of the responsible behaviour of States.[109] Whether such a practice strengthens or rather weakens the applicable legal framework in this respect remains unclear. According to the United Kingdom:

> the fact that States have referred to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace.[110]

However, it seems that at least for some states, support for such a non-binding norm can be without prejudice to acknowledging that simultaneously due diligence remains also a hard law.[111]

5.6. Cyber Espionage

The issue in principle is not covered by the position of states and is a subject of controversy even when performed in the kinetic sphere.[112] Still, some states explicitly or implicitly referred to this issue. Thus, according to Canada, cyber espionage does not amount to a breach of territorial sovereignty but can be prohibited by domestic law.[113] A similar position is presented by New Zealand.[114] According to United States, intelligence collection, as it is practised by most states, is in principle not prohibited by international law.[115] Conversely, for Costa Rica cyber espionage can amount to a breach in this respect as it is difficult to differentiate between data gathering and interfering

109 'c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs', A/70/174, 22 July 2015, p. 8.

110 United Kingdom 2021; similarly Kenny, 'Cyber Operations And The Status Of Due Diligence Obligations In International Law'.

111 Multiple States' views on best practices relating to the implementation of norm 13(c), working paper submitted by Belgium, Czech Republic, Estonia, Finland, France, Germany, Ireland, Italy, Latvia, Portugal, Slovakia, Spain, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_paper_-_Best_practices_relating_to_the_implementation_of_norm_13(c).pdf.

112 Terry, "The Riddle Of The Sands' Peacetime Espionage And Public International Law"; Buchan, "The International Legal Regulation of State-Sponsored Cyber Espionage".

113 Canada 2022, para 19.

114 New Zealand 2020.

115 United States 2016.

with the system.[116] Similarly, Austria is of the view that 'cyber espionage activities, including industrial cyber espionage against corporations, within a state's territory may also violate the state's sovereignty'.[117]

6. Conclusions

The discussion on the application of sovereignty in cyberspace has forced a renewed reflection on the relevance of this fundamental concept, principle and rule for the theory of international law and the practice of states. In particular, the practice of states formulating positions on the application of international law in cyberspace has created a remarkable body of research regarding the practical understanding of sovereignty both in terms of typologies of norms as well as the scope of its application. The debate has also influenced the development of the understanding of the principle of non-intervention.[118]

It is clear that the predominant number of states recognize the possibility of the application of state sovereignty as a rule to cyberspace. Thus, the pure conduct of a state in cyberspace can lead to a breach of sovereignty and as a result be qualified as an internationally wrongful act. Still, despite this significant convergence, it is surprising that states do not refer to a breach of international law in their statements on the attribution of cyberattacks. One explanation of such a practice can be perhaps the need to find a consensus language when the collective declarations are issued. Nevertheless, it could be questioned whether the reference to 'malicious' instead of 'unlawful' conduct indeed strengthens the applicability of international law to cyberspace.

In principle, there exists a significant convergence of views on the components of state sovereignty. It covers jurisdictional rights, causing harmful effects and interference with governmental functions. However, significant divergence exists concerning the assessment of unauthorized access which does not cause harmful effects. The discussion in this respect seems to be connected also with the question of espionage which as a generic term and is difficult to conclusive qualification *in abstracto* under international law.

116 Costa Rica 2023, para 22.
117 Austria 2024, p. 4.
118 Milanovic, ibidem.

Furthermore, the debate of sovereignty and due diligence in cyberspace opens the field for the examination of two additional questions. First, the question arises to what extent the constant need for explaining how the norms of general international law apply to cyberspace moves as closer to a *de facto lex specialis* regime of international law. Second, whether the development of norms of responsible state behaviour in cyberspace truly strengthens the legal framework. The issue would in particular relate to a situation when rules of general international law are blended with soft law standards.[119] These questions deserve further reflection.

Bibliography

7. Prakash, Anand Ram. *Sovereign Equality of States in International Law*. RCADI 1986.
8. Perry, Barlow John. "A declaration of the independence of cyberspace", 1996, https://www.eff.org/cyberspaceindependence .
9. Besson, Samantha. "Sovereignty." In *Max Planck Encyclopedia of Public International Law* online.
10. Bodin, Jean. *On Sovereignty: Six Books Of The Commonwealth*. Cambridge, 1992.
11. Broeders, Dennis (eds.). *Digital Sovereignty: From Narrative to Policy?* EU Cyber Direct, 2022.
12. Broeders, Dennis. "Coalition of the unwilling? Chinese and Russian perspectives on cyberspace." *The Hague Program For Cyber Norms Policy Brief*, November, 2019.
13. Broeders. Dennis (eds.). *Governing Cyberspace: Behavior, Power, and Diplomacy. Digital Technologies and Global Politics*. Lanham: Rowman & Littlefield, 2020.
14. Buchan, Rusel. "The International Legal Regulation of State-Sponsored Cyber Espionage." In *International Cyber Norms: Legal, Policy & Industry Perspectives*, edited by Osula, Anna-Maria and Roigas, Henry. Tallin, 2016.
15. Chatinakrob, Thanapt. "Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty." *Chinese Journal of International Law*, Vol. 23, Issue 1, March 2024.
16. Corn, Garry and Taylor, Robert. "Sovereignty in the Age of Cyber." *American Journal of International Law, Unbound* 2017, Vol. 111.
17. Crawford, James. *Creation of States*. Cambridge, 2004.
18. Crawford, James. *Browlnie's Principles of Public International Law*. Oxford, 2012.
19. Crawford, James. *Chance, Order, Change: The Course of International Law. General Course on Public International Law*. RCADI, Vol. 365 (2014).

119 Kastelic, "Due diligence in cyberspace. Normative expectations of reciprocal protection of international legal rights".

20. Crawford, James and Koskenniemi, Matti (eds). *The Cambridge Companion to International Law*. Cambridge University Press, 2012.
21. Creemers, R. "China's Conception of Cyber Sovereignty – Rhetoric and Realization." In *Governing Cyberspace: Behavior, Power, and Diplomacy. Digital Technologies and Global Politics*, edited by Broeders, D. and Berg, B. van den (eds.). Lanham: Rowman & Littlefield, 2020.
22. Dworkin, Richard. *Taking Rights Seriously*. London, Bloomsbury, 2013.
23. Goldsmith, Jack and Loomis, Alexis. "Defend Forward' and Sovereignty." *Aegis Series Paper,* No. 2102.
24. Fitzmaurice, Gerard. *The General Principles of International Law Considered from the Standpoint of the Rule of Law*. RCADI, 1957.
25. Heller, Kevin. "In Defense of Pure Sovereignty in Cyberspace." *International Law Studies* 2021, Vol. 97.
26. Jamnejad, Maziar and Wood, Michael. "The Principle of Non-intervention." *Leiden Journal of International Law* 2009, Vol. 22.
27. Jančárková, Tatana (eds.). *12th International Conference on Cyber Conflict: 20/20 Vision: the Next Decade*. Tallinn, 2020.
28. Jennings, Robert and Watts, Arthur (eds.). *Oppenheim's International Law: Peace*. 9th ed. 1992.
29. Kastelic, Andrea. *Due diligence in cyberspace. Normative expectations of reciprocal protection of international legal rights*. UNIDIR, 2021.
30. Kenny, Jac. "Cyber Operations And The Status Of Due Diligence Obligations In International Law." *International and Comparative Law Quarterly* 2024, Vol. 73, no. 1.
31. Kranz, Jerzy. *Pojęcie suwerenności we współczesnym prawie międzynarodowym* [The concept of sovereingty in international law]. Warszawa, 2015.
32. Kushwaha, Neal, Roguski, Przemysław and Watson, Bruce. "Sovereignty and Non-intervention Up in the air: ensuring government data sovereignty in the cloud." In *12*th *International Conference on Cyber Conflict: 20/20 Vision: the Next Decade* edited by Jančárková, Tatiana, Lindström, Lauri and Signoretti, Massimiliano (eds.). Tallinn, 2020.
33. Kwiecień, Roman. *Suwerenność państwa. Rekonstrukcja i znaczenie idei w prawie międzynarodowym* [Sovereingty of state, Reconsutruction and the importance of the idea in international law]. Kraków, 2004.
34. Lowe, Vaugham. *International Law*. Oxford, 2007.
35. Milanovic, Marko. "Revisiting Coercion as an Element of Prohibited Intervention in International Law." *American Journal of International Law*, 2023, Vol. 117, no. 4.
36. Milanovic, Marko and Schmitt, Michael. "Attacks and Cyber (Mis)information Operations during a Pandemic." *Journal of National Security Law & Policy,* 2020, Vol. 11.
37. Moynihan, Harriet. "The Application of International Law to State Cyberattacks." *Chatham House Research Paper,* December 2019.
38. Moynihan, Harriet. "The vital role of international law in the framework for responsible state behaviour in cyberspace." *Journal of Cyber Policy,* 2021.
39. Moynihan, Harriet. "Unpacking due diligence in cyberspace." *Journal of Cyber Policy,* 2023, 8:1.

40. Mueller, Milton. "Hague Keynote: Sovereignty in Cyberspace", https://www.internetgovernance.org/2020/11/13/hague-keynote-sovereignty-in-cyberspace.
41. Osula, Anna-Maria and Roigas, Henry (eds.). *International Cyber Norms: Legal, Policy & Industry Perspectives*, 2016.
42. Przychodniak, Marcin. "China's Internet Policy." *Bulletin PISM*, 2017.
43. Schmitt, Michael and Vihul, Liz. "Respect for Sovereignty in Cyberspace." *Texas Law Review*, 2017.
44. Schmitt, Michael and Durward, John. "Responding to Hostile Cyber Operations: The 'In-Kind' Option." *International Legal Studies*, 2021, Vol. 97.
45. Schmitt, Michael (eds.). *Tallinn Manual 2.0*. Cambridge, 2017.
46. Schmitt, Michael. "Foreign Cyber Interference in Elections." *International Legal Studies*, Vol. 97, 2021.
47. Shaw, Malcolm. *International law*. Cambridge, 2008.
48. Terry, Patrick. "The Riddle Of The Sands' Peacetime Espionage And Public International Law." *Georgetown Journal of International Law*, 2020, Vol. 51, no. 2.
49. Tsagourias, Nicholas and Buchan, Russel (eds.). *Research Handbook on International Law and Cyberspace*. Elgar, 2021.
50. Tsagourias, Nicholas. "Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace." *ESIL Reflections*, 17 December 2020 Vol. 9, Issue 4.
51. Verdross, Alfred, Simma, Brunno and Geiger, Richard. "Territoriale Souveranitdt und Gebietshoheit." Ósterreichisches *Zeitschnft fur* óffentliches *Recht und Vólkerrecht*, 1980, no 31.
52. Viñuales, Jorge (ed.). *The UN Friendly Relations Declaration at 50. An Assessment of the Fundamental Principles of International Law*. Cambridge, 2020.
53. Watts, Sean. "Low-Intensity Cyber Operations and the Principle of Non-Intervention." In *Cyber War: Law and Ethics for Virtual Conflicts*, edited by Ohlin, Jens David, Govern, Kevin and Finkelstein, Claire (eds.). Oxford, 2015.