Carmen Moldovan*

Mirror, Mirror on the Wall, Who's the Most Authoritative of Them All? Cyber Sovereignty from a Critical Perspective

Abstract

The paper aims to highlight the conflict between the idea of state control over the Internet and the impact on freedom of expression and access to information and to challenge the state-driven regulatory model. The doctrine of cyber sovereignty, as advocated by China and Russia, is an example of such control in the absence of international legally binding regulation. First, the special features of cyberspace as a *sui generis* phenomenon are presented, as well as the attempts of the United Nations to create a legal framework for this special environment. Second, the digital perspective of the right to access information is analysed, followed by the meaning of the principle of state sovereignty and the impact on the digital space, especially its fragmentation. Addressing this conflict is crucial to safeguarding fundamental rights in the digital empire, divided between the doctrine of human rights, the idea of open space and the control of information supported by authoritative regimes.

Keywords: cyberspace, digital environment, access to information, state control

I Introduction

The development of the Internet has had a profound impact on technology and communications, influencing and advancing human activity at many levels and establishing cyberspace as a global ecosystem that would not be possible in its absence. The creation of a digital empire with special features generates multiple problems related to the identification of applicable rules, the extent of the protection of fundamental rights and the balance of power, including new dimensions for international law.[1]

* Dr Carmen Moldovan PhD, Associate Professor, Alexandru Ioan Cuza University of Iasi, Faculty of Law. ORCID iD: 0009-0002-7470-8557.

1 Philip Alston, Colin Gillespie, 'Global Human Rights Monitoring, New Technologies, and the Politics of Information' (2012) 23 (4) The European Journal of International Law 1089–1123

Cyberspace has been characterised as being chaotic, anarchic[2] and asymmetric with respect to resources and capabilities[3] in order to justify the notion of state cyber sovereignty that safeguards the latter's best interests as they relate to other states; establishing this principle does not resolve all of the subsequent difficulties such as state responsibility and repercussions concerning the interests and rights of private individuals and non-state actors.[4]

The concept of cyber sovereignty is referred to as the establishment and control of a 'national cyberspace'[5] subject to domestic laws, authoritarian in nature, with the goal of seizing complete control of cyberspace and the Internet and isolating them from the global network, which contradicts the very essence of their existence. Although such an idea is presented as an alternative to the intention of the United States to build a hegemonic order in global cyberspace[6] and as a means of ensuring the principle of equality between states, taking into consideration that there are significant differences in actual access to cyberspace due to unequal technological levels of development, the outcome is a fragmented environment that negatively affects fundamental rights, especially freedom of expression and access to information. Such a submission disregards the fact that, in practice, cyber sovereignty only widens the gap between technologically advanced nations and developing ones. On the contrary, a free and global cyberspace offers open accessibility to public information and the public sector to everyone. Thus, employing such arguments plainly shows that the issue of cyber standards continues to be a tool of geopolitical rivalry.[7]

DOI: https://doi.org/10.1093/ejil/chs073; Daniel Bethlehem, 'The End of Geography: The Changing Nature of the International System and the Challenge to International Law' (2014) 25 (1) The European Journal of International Law 9–24. DOI: https://doi.org/10.1093/ejil/chu003

2 Séverine Arsène, 'Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order?' (2016) (2) China Perspectives 28, DOI: https://doi.org/10.4000/chinaperspectives.6973; Jinghan Zeng, Tim Stevens, Yaru Chen, 'China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"' (2017) 45 (3) Politics & Policy 451, DOI: https://doi.org/10.1111/polp.12202

3 Yi Shen, 'Cyber Sovereignty and the Governance of Global Cyberspace' (2016) 1 Chinese Political Science Review 84, DOI: https://doi.org/10.1007/s41111-016-0002-6

4 Issues linked to the topic of cyber sovereignty have been analysed previously by the author: Carmen Moldovan, 'On the normative equivalence paradigm in cyberspace' 177 02002 (2023) SHS Web of Conferences Legal Perspectives on the Internet. COPEJI 6.0, DOI: https://doi.org/10.1051/shsconf/202317702002; Carmen Moldovan, 'Suveranitatea digitală – viitorul spațiului virtual? (2021) 67 (2) Analele Ştiinţifice ale Universităţii Alexandru Ioan Cuza din Iași Științe Juridice 271–284, DOI: https://doi.org/10.47743/jss-2021-67-4-19

5 Milton Mueller, *Sovereignty and Cyberspace: Institutions and Internet governance,* Essay presented at the 5th Annual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana October 3rd 2018 <http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10410/5th-Ostrom-lecture-DLC.pdf?sequence=1&isAllowed=y> accessed 15 October 2024.

6 Yi Shen (n 3) 82; Daniel Joyce, 'Internet Freedom and Human Rights' (2015) 26 (2) The European Journal of International Law 494–514, DOI: https://doi.org/10.1093/ejil/chv021

7 Harriet Moynihan, 'Power Politics Could Impede Progress on Responsible Regulation of Cyberspace' (2019) <https://www.chathamhouse.org/expert/comment/power-politics-could-impede-progress-responsible-regulation-cyberspace> accessed 15 October 2024.

Although relatively intriguing, the idea that various types of cyberspace or virtual frontiers may be established by governments according to their interests and supported by territorial sovereignty has ramifications for other regulations and rules. The term cyber sovereignty may be considered inaccurate or a misnomer simply because the principle of sovereignty, which is the cornerstone of international law, cannot be fully transferred to this environment. The notion of territorial sovereignty in cyberspace must be applied in a restrictive manner and only in relation to elements of Information and Communication Technology (ICT) infrastructure on state territory, as it results from the conclusions of special groups established with the purpose of identifying how international law applies in the digital empire and not impacting on freedom of expression.

II Cyberspace – From Matrix to a *Sui Generis* Phenomenon

States appear to be unable to reach a consensus on how to govern cyberspace or even how to comprehend how this intricate ecosystem works. Since the goal of international law is to regulate state behaviour within cyberspace rather than the environment itself, discussing its characteristics may be helpful in addressing the conflict between the legal concept of sovereignty and this environment, as well as the implications for free speech.

Terms used to refer to cyberspace[8] are inconsistent and synonymously include 'virtual space', 'digital space', and 'digital ecosystem'.[9] Instead of being utilised or defined as such under international law, the United Nations prefers to use the term 'Information and Communication Technology' (ICT) in various reports and documents. Cyberspace is one of the greatest of humanity's creations; it does not rely on natural elements; it is entirely human-made[10] and is a complex global network, a logical space which is unlimited, imperceptible, non-materialised, time-dependent[11] and constantly changing. It is an interconnected information system which has been developed by non-state actors and has

[8] The term was coined by William Gibson in his cyberpunk book *Neuromancer* (Ace Books 1984): 'Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts… A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.'

[9] Eileen Donahoe, 'The Need for a Paradigm Shift on Digital Security' in Fen Osler Hampson, Michael Sulmeyer, (eds), *Getting beyond Norms New Approaches to International Cyber Security Challenges* (Special Report, Centre for International Governance Innovation 2017) 31.

[10] Marie Baezner, Patrice Robin, *Trend Analysis: Cyber Sovereignty* (Risk and Resilience Team Center for Security Studies 2018, ETH Zürich) 8.

[11] Rain Ottis, Peeter Lorents, 'Cyberspace: Definition and Implications' in Leigh Armistead (ed), *Proceedings of the 5th International Conference on Information Warfare and Security* (Academic Conferences Limited 2010, Reading) 267.

no borders[12] corresponding to physical territory. This is entirely opposed to state territory, which has a material and physical dimension, yet cyberspace requires the physical support of material infrastructure.[13] Employing the expression 'Information Society'[14] is adequate with reference to the components of freedom of expression.

Currently, cyberspace is being used for a variety of activities and purposes, including military operations. Its special traits make it a *sui generis* phenomenon[15] that challenges rules and principles already established and widely recognised. Although it may not be the subject of exclusive state control, its features are no longer sufficient to qualify as *res communis omnium*,[16] excluding all forms of sovereignty[17] similar to the high seas or outer space.

III The Complicated Relationship between International Law and Cyberspace

1 From an Unregulated Environment to (Blurred) Normative Equivalence

The absence of a legal definition of cyberspace serves as the foundation for any form of activity by states and may impact their responsibility to protect fundamental rights. There are no legally enforceable mechanisms governing this environment, despite the fact that states and other stakeholders[18] (including employees, shareholders, marketers, mass media organisations, civil society groups, and, in general, platform users)[19] have expressed concern and even proposed regulations. The task of developing and clarifying cyber standards is

12 Katrin Nyman Metcalf, 'Legal View on Outer Space and Cyberspace: Similarities and Differences' Tallinn Paper 2018/10, 2.

13 Yi Shen (n 3) 83.

14 Daniel Joyce, 'Internet Freedom and Human Rights' (2015) 26 (2) The European Journal of International Law 493–514, DOI: https://doi.org/10.1093/ejil/chv021

15 Dennis Broeders, Liisi Adamson, Rogier Creemers, 'Coalition of the unwilling? Chinese and Russian perspectives on cyberspace' (2019) The Hague Program For Cyber Norms Policy Brief 2, <https://www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace> accessed 15 October 2024.

16 Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in C. Czosseck, R. Ottis, K. Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict* (NATO CCDCOE Publications 2012, Tallinn) 8.

17 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press 2012, Oxford) 203.

18 Anri van der Spuy, *What if we all governed the Internet? Advancing multistakeholder participation in Internet governance* (UNESCO Series on Internet Freedom 2017, Paris) 26.

19 Barrie Sander, 'Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law' (2021) 32 (1) European Journal of International Law 166, DOI: https://doi.org/10.1093/ejil/chab022

not just the responsibility of the United Nations. The contribution of regional bodies and organisations is equally essential.

In general, regional instruments are limited in scope, and they do not specify what it means by the 'responsible behaviour of states' in this regard. The Budapest Convention on Cybercrime[20] and its Additional Protocol[21] define a restricted scope for the criminal activity of individuals using information systems that does not address jurisdiction issues. The Shanghai Organisation (headed by Russia and China) in its International Information Security Agreement[22] defines cyber warfare but does not address other aspects of state action or applicable standards of international law.

In 2015, the Shanghai Organisation presented the International Code for Information,[23] which received little attention or reaction from other states. The International Code for Information Security is intriguing in terms of terminology;[24] at least in part, the goal of this code of conduct is similar to the suggestions created by the United Nations. It refers to the United Nations Charter, specifically to the principles of sovereignty, territorial integrity and political independence.[25] Overall, it refers to the general application of international law, which may apply to states' cyber conduct and, as opposed to other texts, the Code focuses on information society[26] rather than cybersecurity. However, it only serves a declaratory purpose.

The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations (The Tallinn Manual 2.0)[27] is widely regarded as the most comprehensive academic work on the

---

[20] *Convention on Cybercrime*, opened for signature 23 November, 2001 ETS 185 (entered into force on 1 July 2004).

[21] *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* opened for signature 28 January 2003, ETS 189.

[22] *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security*, Yekaterinburg, 16 June 2009 <https://eng.sectsco.org/documents/?year=2009> accessed 15 October 2024.

[23] Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, sixty-ninth session Agenda item 91 Developments in the field of information and telecommunications in the context of international security, UN Doc A/69/723 <https://ccdcoe.org/uploads/2018/11/UN-150113-CodeOfConduct.pdf> accessed 15 October 2024.

[24] It provides that its purpose is 'to identify the rights and responsibilities of States in the information space, promote constructive and responsible behaviour on their part and enhance their cooperation in addressing common threats and challenges in the information space, in order to establish an information environment that is peaceful, secure, open and founded on cooperation, and to ensure that the use of information and communications technologies and information and communications networks facilitates the comprehensive economic and social development and well-being of peoples, and does not run counter to the objective of ensuring international peace and security', International Code of Conduct, § 1.

[25] International Code of Conduct, § 2(1).

[26] Broeders, Adamson, Creemers (n 15) 2.

[27] Michael N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017, Cambridge) DOI: https://doi.org/10.1017/9781316822524

subject of cyber activities. It offers useful content about the concepts of sovereignty and non-intervention in cyberspace, but it does not provide answers to all questions and concentrates on themes such as the use of force in peacetime, preventative self-defence, cyber-attacks and determining the imminence of cyber-attacks. In chapter 2, the concept of state sovereignty in cyberspace is examined in relation to the physical aspects of state infrastructure[28] located on their territory. Although not legally binding, the Tallinn Manual had a significant impact on state cyber activity.[29] Version 3 is now awaited.[30] There are also various private initiatives aimed at establishing cyberspace rules.[31]

2 The Findings of the United Nations on Sovereignty in Cyberspace

Currently, it is commonly agreed that international law applies to cyber operations,[32] resolving previous disputes and refuting the claim that states should refrain from regulating this field as a means to protect Internet freedom. One legal implication of this acknowledgement is that states are required to abide by corresponding rights and obligations in their cyberspace activities,[33] including ensuring the safeguarding of fundamental freedoms.

Soft law tools, such as reports from specialised United Nations working groups like the UN Group of Government Experts (the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

---

[28] The terms are the following: '[a] State enjoys sovereign authority with regard to cyber infrastructure… located within its territory', Schmitt (n 27) 13.

[29] Michael N. Schmitt, Liis Vihul, 'The Nature of International Law Cyber Norms' Tallinn Paper 2014/5, 31.

[30] <https://ccdcoe.org/research/tallinn-manual/> accessed 15 October 2024.

[31] The Paris Call for Trust and Security in Cyberspace was launched in 2018 as a multistakeholder initiative and formulated nine principles (<https://pariscall.international/en/> accessed 15 October 2024). Principle number 9 refers to international norms, and it aims to promote the widespread acceptance and implementation of international norms of responsible behaviour as well as confidence-building measures in cyberspace. A Digital Geneva Convention was proposed by Microsoft in 2017, and it underlines the importance of international humanitarian law in cyberspace without giving details on how this is applicable and to what extent. It is at the same time appreciated [Joseph Guay, Lisa Rudnick, 'What the Digital Geneva Convention means for the future of humanitarian action' (25 June, 2017) The Policy Lab <https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/> accessed 15 October 2024] and criticised [Valentin Jeutner, 'The Digital Geneva Convention. A Critical Appraisal of Microsoft's Proposal', (2019) 10 (1) Journal of International Humanitarian Legal Studies 158–170, DOI: https://doi.org/10.1163/18781527-01001009].

[32] Maria Tolppa, 'Overview of the UN OEWG developments: continuation of discussions on how International Law applies in cyberspace' (2020) <https://ccdcoe.org/library/publications/overview-of-un-oewg-developments-continuation-of-discussions-on-how-international-law-applies-in-cyberspace/> accessed 15 October 2024.

[33] Antonio Coco, Talita de Souza Dias '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32 (3) The European Journal of International Law 771–805, DOI: https://doi.org/10.1093/ejil/chab056; Sean Kanuck, 'Sovereign Discourse on Cyber Conflict' (2010) 88 Texas Law Review 1575.

– UNGGE) and the Open-ended Working Group (OEWG),[34] emphasise the voluntary nature of non-binding norms, rules and principles governing responsible state behaviour in cyberspace. These reports support the use of international law in cyberspace and call for confidence-building measures to increase trust between states and strengthen global cybersecurity. Despite being among the first UN endeavours on the subject,[35] these reports fall short of providing clear direction for implementing these ideas or developing customary international law.

The common thread across all legal frameworks concerning state activities in cyberspace is the acknowledgement that existing international law provides the foundation for regulating states' conduct.[36] However, none of these reports delineate specific implementation strategies, nor do they constitute elements of international customary law. State practice remains varied or involves silence, notwithstanding the latter's authority to formally adopt rules governing conduct in cyberspace. To advance clarity on the application of international law to cyber sovereignty, a strategic shift may be necessary, separating discussions on this specific issue from broader political deliberations on behavioural norms and confidence-building measures.[37]

The UN GGE, established in 2004,[38] represents a significant step towards identifying cyber norms and addressing responsible state behaviour in cyberspace. Critical to its work are the 2013[39] and 2015 reports that assert that UN Charter principles extend to states' conduct and operations in cyberspace. Notably, both Russia and China participated in this group.

---

[34] United Nations Office for Disarmament Affairs, Fact Sheet – Developments in the field of information and telecommunications in the context of International Security (July 2019) <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf> accessed 15 October 2024.

[35] Tolppa (n 32).

[36] Moynihan (n 7).

[37] François Delerue 'The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?' (2018) 7 (4) European Society of International Law Reflections 2.

[38] United Nations Office for Disarmament Affairs 2019. Initially, it was established as an exclusive body, with 15 members (Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, Russia, South Africa, South Korea, United Kingdom, United States of America). The numbers expanded to 25 for the period 2004–2005 (Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, and Uruguay).

[39] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Developments in the field of information and telecommunications in the context of international security-Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' Sixty-eighth session Agenda item 94, U.N. Doc. A/68/98 (24 June 2013) § 19.

The 2013 report emphasises the application of state sovereignty to ICT-related activities and jurisdiction over ICT infrastructure within state territories,[40] albeit with some ambiguity regarding an open ICT environment versus state sovereignty in ICT matters.

Similarly, the 2015 Report[41] reaffirms the principles of international law outlined in the previous report and the application of sovereignty[42] and provides recommendations,[43] albeit without providing clearer insights. Referring to infrastructure does not actually solve the problem because this has a mixed or hybrid character determined by the influence of private companies and is part of a global network.[44]

Despite these efforts, the UN GGE faced challenges, culminating in a deadlock in 2017 due to disagreements over the right to self-defence and the applicability of international humanitarian law to cyber conflicts.[45] Subsequently, the UN established the OEWG in 2018,[46] which operated more inclusively,[47] allowing all interested UN member states to participate. However, like its predecessor, the OEWG failed to provide clear guidance on the application of international law to cyberspace and its work ended in 2021.

Critically, the findings of these reports, while significant, remain limited[48] considering their soft law[49] nature. They highlight the lack of consensus about the application of international law, reflecting the politically influenced nature of these working groups.[50] Despite the impasse, it is essential to recognise that the failure to reach a consensus and

---

40 The wording of the Report is the following: 'State sovereignty and the international norms and principles that flow from it apply to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure with their territory'. A/68/98 § 20., 27., 28.

41 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 17th sess item 93 of the provisional agenda UNGA UN Doc A/70/174 (22 July 2015).

42 UN Doc A/70/174, § 13(h), §§ 24., 26.

43 Paul Meyer, 'Norms of Responsible State Behaviour in Cyberspace' in Markus Christen, Bert Gordijn, Michele Loi (eds), *The Ethics of Cybersecurity* (Springer 2020) 353, DOI: https://doi.org/10.1007/978-3-030-29053-5_18

44 Dimitri Van Den Meerssche, 'Compressing All Data into Actionable Risk Scores': The Construction of Virtual Borders' (2022) 33 (1) The European Journal of International Law 176, DOI: https://doi.org/10.1093/ejil/chac007; Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 (4) The European Journal of International Law 799–839, DOI: https://doi.org/10.1093/ejil/chn040

45 Stefan Soesanto, Fosca D'Incau, 'The UN GGE is dead: Time to fall forward. Commentary' (2017) <https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance> accessed 15 October 2024.

46 Developments in the field of information and telecommunications in the context of international security GA Res 73/27 UN Doc A/RES/73/27 (5 December 2018).

47 Tolppa (n 32).

48 Bruno Lété, Peter Chase, 'Shaping Responsible State Behavior in Cyberspace' (2018) The German Marshall Fund of the United States Workshop Briefing Paper 6.

49 Dinah Shekton, 'International Law and Relative Normativity' in Malcolm D. Evans (ed), *International Law* (Oxford University Press 2014, Oxford) 159.

50 Soesanto, D'Incau (n 45).

adopt cyber norms[51] does not equate to an unregulated cyberspace. Instead, it highlights the complexities and challenges inherent in governing this dynamic domain.

The primary legal implication of the existence only of soft norms or quasi-norms[52] is that breaching obligations does not involve international responsibility for states, as outlined in the Draft Articles on State Responsibility,[53] and does not trigger identical legal remedies. Typically, a breach of an international obligation involves restitution.[54] When applied to cyber operations, if a state's cyber activity breaches another state's sovereignty, the affected state would theoretically be entitled to restitution, but this remains an unresolved issue. The ongoing reinterpretation of existing norms and rules in this domain may prove crucial in the future formulation of regulations applicable to states in cyberspace. The International Court of Justice's *Advisory Opinion on Namibia* may be significant in this regard as it states that an 'international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of interpretation'.

IV The Cyber Right to Access Information

Access to information as a part of the right to freedom of expression is guaranteed by several international law instruments in similar terms. These include Article 19 of the Universal Declaration of Human Rights[55] and the International Covenant on Civil and Political Rights (hereinafter ICCR),[56] Article 10 of the European Convention on Human Rights,[57] Article 13 of the Inter-American Convention on Human Rights,[58] Article 9 of the African Charter of Human and Peoples' Rights.[59] It constitutes a topic of interest for the UN from different perspectives[60] and for regional organisations.

---

51 Tim Maurer, 'A Dose of Realism: The Contestation and Politics of Cyber Norms' (2020) 12 (2) Hague Journal on the Rule of Law 285, DOI: https://doi.org/10.1007/s40803-019-00129-8

52 Toni Erskine, Madeline Carr, 'Beyond 'Quasi-Norms: The Challenges and Potential of Engaging with Norms in Cyberspace in Anna-Maria Osula, Henry Rõigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCDCOE Publications 2016, Tallinn) 100.

53 Responsibility of States for Internationally Wrongful Acts, GA Res 56/83, UN GAOR, 56th sess, 85th plen mtg, Supp No 49, UN Doc A/RES/56/83 (28 January 2022, adopted 12 December 2001).

54 *The Factory at Chorzow* (Germany v Poland) (Claim for Indemnity) (The Merits) [1927] PCIJ (ser A) No 13, 28.

55 *Universal Declaration of Human Rights* (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR).

56 *International Covenant on Civil and Political Rights* opened for signature 19 December 1966, 999 UNTS 171 (ICCPR).

57 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force on 3 September 1953).

58 *American Convention on Human Rights*, opened for signature 22 November 1969, 123 UNTS 1144 (entered into force 18 July 1978).

59 *African Charter on Human and Peoples' Rights*, opened for signature 27 June 1981, 217 UNTS 1520, (entered into force 21 October 1986).

60 Eneken Tikk, Mika Kerttunen, *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, (Cyber Policy Institute 2017) 14.

The scope of freedom of expression and of the right to receive and impart information and ideas is similar in all international legal instruments. For the purpose of this paper, only the provisions of Article 19 of the Universal Declaration on Human Rights and of ICCPR will be analysed. The Universal Declaration provides that 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers'. Article 19 of the ICCPR has similar wording and also mentions the requirements that the states must comply with when interfering with its exercise.

Creating a national cyberspace under the full control of the state cannot be considered a legitimate restriction in the sense of paragraph 3 of Article 19. When applying restrictions to freedom of expression, states must comply with their obligations provided by international instruments. China only signed the ICCPR in 1998 and did not ratify it. The Russian Federation signed the Covenant in 1968 and ratified it in 1973.[61] According to Article 2, paragraph 1 of the ICCPR, states have a negative and a positive obligation to ensure rights are recognised. This means that restrictions must be permissible and must prove their necessity and proportionality in pursuing a legitimate aim.[62]

As already mentioned, cyberspace is an environment characterised by communication and the transfer of data and information, which could not have been envisaged by the drafters of all international instruments that regulate freedom of opinion and access to information. However, all of them have a common feature: the safeguards of the freedom of expression and access to information are recognised regardless of frontiers.

The Human Rights Council has stressed that 'the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights'.[63] And at the same time, it 'recognizes the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms; and calls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries.[64] The UN Human Rights Council reiterated these conclusions in 2014, and they are at the moment generally accepted. Previously, the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion

[61] <https://indicators.ohchr.org/> accessed 15 October 2024.

[62] Human Rights Committee, *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant* (2004), adopted by the Human Rights Committee at the 80th sess, CCPR/C/21/Rev.1/Add.13 (29 March 2004) § 5., 6., 8.

[63] Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, 26th sess Agenda item 3 UN Doc A/HRC/20/L.13 (29 June 2012).

[64] UN Doc A/HRC/20/L.13.

and expression,[65] Frank La Rue, underlined the implications of the Internet for the freedom of expression and access to information.

Also, at the universal level, UNESCO has engaged in assiduous activity, usually by cooperating with other entities to support Internet freedom and access to information. It is not the purpose of this paper to analyse these works, yet some of them are particularly relevant, taking into consideration the moment they were adopted and their divergence concerning the idea of applying cyber sovereignty as a form of control over national territory. For example, the Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium, drafted in collaboration with the International Telecommunication Union, highlights the importance of access to information for the information society in paragraphs 24–28.

Since freedom of expression is not an unlimited fundamental right, restrictions are admissible if they are in accordance with the requirements of the limitation clause provided by paragraph 3 of Article 19. The 2011 General Comment No. 34 on freedom of expression of the Human Rights Council underlines this conclusion. Nevertheless, free access to the Internet and digital networks without any barriers, technical, structural or educational, is also supported by the OSCE.[66] Even the 2015 UNGGE Reports also expressly mention the need for the respect of fundamental rights, including the right to freedom of expression.[67] As a consequence, there must be a balance between the admissible actions of states and those that constitute interference with the normal exercise of this right and its content.[68] Establishing full state control over the infrastructure and flux of data and information as an effect of state cyber sovereignty would disproportionately and illegitimately impact the right to access information.

V Features of the Principle of State Sovereignty

In order to justify the idea of state sovereignty in cyberspace, the principle of territorial sovereignty is being used. However, there is no comprehensive definition of sovereignty in international law, so identifying its elements and meaning is highly relevant for the current analysis and for the legal consequences applicable in the traditional sense,

---

65 Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* Frank La Rue, 17th sess Agenda item 3 UN Doc A/HRC/17/27 (16 May 2011).

66 Organization for Security and Co-operation in Europe, The Representative on Freedom of the Media, Amsterdam Recommendations, Freedom of the Media and the Internet (14 June 2003), <https://www.osce.org/files/f/documents/4/a/41903.pdf > accessed 15 October 2024.

67 UN Doc A/70/174, § 13(e) Norm 5.

68 Gergely Gosztonyi, 'The European Court of Human Rights: Internet access as a means of receiving and imparting information and ideas' (2020) 6 (2) International Comparative Jurisprudence DOI: http://dx.doi.org/10.13165/j.icj.2020.12.003

some of the most important being state jurisdiction and state immunity,[69] which also constitute limits to other states' sovereignty. The complexity of the concept is amplified by the fact that the modern meaning of sovereignty refers to the peoples within a state, not exclusively to the state itself as a legal entity.[70] Sovereignty as a principle dates back to the 16th century[71] and is one of the concepts developed after the Peace of Westphalia of 1648. The Westphalian system considered States to have sovereignty over their territories and domestic affairs without the intervention of other States.

The principle of state sovereignty is one of the fundamental principles of international law, enshrined in Article 2, paragraph 1 of the Charter of the United Nations[72] and subsequent legal instruments (Declaration on principles of International Law friendly relations and cooperation among States in accordance with the Charter of the United Nations,[73] Helsinki Final Act,[74] Charter of Paris for a New Europe[75]) also mentioned this principle and its significant value for international law and established connections between it and other fundamental principles such as non-intervention, self-determination, territorial integrity and the peaceful solution of disputes.[76]

All interstate relations and the functioning of the state itself are based on this core principle. From a territorial perspective, state sovereignty and other fundamental principles of international law apply to all components of the territory of a state within its borders (terrestrial, maritime, airspace), where it enjoys undisputed exclusivity. All elements of state sovereignty refer to and are analysed in connection with physical state territory according to the stage of evolution of international law rules and concepts. Sovereignty describes the competencies of states and presents, in fact, multiple meanings.

---

69 Christopher Staker, 'Jurisdiction' in Malcolm D. Evans (ed), *International Law* (Oxford University Press 2014, Oxford) 309, DOI: https://doi.org/10.1093/he/9780198791836.003.0010

70 Samantha Besson, 'Sovereignty, International Law and Democracy' (2011) 22 (2) The European Journal of International Law 383, DOI: https://doi.org/10.1093/ejil/chr029

71 Andreas Osiander, 'Sovereignty, International Relations, and the Westphalian Myth' (2001) 55 (2) International Organization 251–287, DOI: https://doi.org/10.1162/00208180151140577

72 Article 2(1) of the Charter of the United Nations reads as follows: 'The Organization is based on the principle of the sovereign equality of all its Members'.

73 Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations (adopted 24 October 1970) 25th sess Supplement no 18 UNGA Res 2625 (XXV), A/RES/26/25 (XXV). The Declaration reads as follows on the principle of sovereignty: 'All States enjoy sovereign equality. They have equal rights and duties and are equal members of the international community, notwithstanding differences of an economic, social, political or other nature. In particular, sovereign equality.'

74 Conference on Security and Cooperation in Europe Final Act (adopted 1 August 1975) <https://www.osce.org/helsinki-final-act?download=true> accessed 15 October 2024.

75 Organization for Security and Co-operation in Europe, *Charter of Paris on a New Europe* (adopted 19-21 November 1990).

76 Helmut Steinberger, 'Sovereignty' in Rudolph Bernhardt (eds), *Encyclopedia of Public International Law* (Volume Four, Elsevier 2000, Amsterdam/New York/Oxford) 513.

Sovereignty is associated with the principle of equality, as enshrined in Article 2(1) of the Charter of the United Nations (sovereign equality), which underlines the independence[77] and the lack of subordination and power of one state over another. Sovereignty is the basic constitutional doctrine of the law of nations[78] seen as an essential and core attribute of the state both at the international and national level[79] and a premise for the existence of states and their international law personality. It is also an attribute of the state and an ideological concept without static or pre-established content,[80] which implies the possibility of different meanings from one period to another and the evolution of its features.

The contemporary meaning of sovereignty is territorial, as the state enjoys exclusive legal competence over its territory *(imperium)* and exercises ownership of real property *(dominium)*[81] within the borders of the state. In addressing the principle of sovereignty, many scholarly papers begin their legal analysis by referring to the conclusions of the *Island of Palmas Case*,[82] which analysed the territorial dimension of sovereignty as follows: 'Territorial sovereignty, as has already been said, involves the exclusive right to display the activities of a state. This right has as corollary a duty: the obligation to protect within the territory the rights of other states, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in foreign territory'.[83] At the same time, it must be stressed that the arbitration award considered the dynamic nature of the concept of sovereignty, as it stated: 'Manifestations of territorial sovereignty assume, it is true, different forms, according to conditions of time and place'.[84] This conclusion may be considered a means of the restrictive interpretation of state cyber sovereignty.

Sovereignty is based on the idea of a state exercising control or a display of authority in a given territory[85] or other space having special legal status. This includes authority and control over all individuals on the territory,[86] which implies exercising jurisdiction (prescriptive jurisdiction, jurisdiction to adjudicate, jurisdiction to enforce). Moreover, sovereignty means the power to freely dispose of the territory, the obligation for other states

---

77 Emmanuel Decaux, Olivier de Frouville, *Droit international public* (Dalloz 2016, Paris) 176.

78 Crawford (n 17) 447.

79 Jean Combacau, Serge Sur, *Droit international public* (12e edn, Librairie Générale de Droit et Jurisprudence 2016, Paris) 238.

80 Mohamed Bennouna, *Le droit international entre la lettre et l'esprit. Cours général de droit international public* (Tome 383, Brill /Nijhoff 2016, Leiden) 42.

81 Crawford (n 17) 204.

82 *Island of Palmas Case (or Miangas)* (United States of America v The Netherlands) (Award of the Tribunal) (Permanent Court of Arbitration, Arbitrator M. Huber, 4 April 1928) <https://pcacases.com/web/sendAttach/714> accessed 15 October 2024.

83 *Island of Palmas Case (or Miangas)* (United States of America v The Netherlands) 839.

84 *Island of Palmas Case (or Miangas)* (United States of America v The Netherlands) 840.

85 *Territorial and Maritime Dispute* (Nicaragua v Colombia) (Judgment) [2012] ICJ Rep 624.

86 Antonio Cassese, *International Law* (Oxford University Press 2005, Oxford) 49.

not to intrude on the state's territory *(jus excludendi alios),* the right to immunity from foreign courts and the right to immunity for state representatives.[87]

The meaning of the principle of sovereignty is the result of evolution, and it has a different significance than the one presented during the 16th and 17th centuries when it appeared as a result of European monarchies' intent to consolidate their position in relation to the church.[88] Therefore, there is an evolutive interpretation of the legal concept of sovereignty, according to which the meaning of sovereignty is subjective and different for states, taking into consideration their historical evolution.[89]

Applying the principle of sovereignty implies a correlative and reciprocal obligation to recognise other states as sovereign and to refrain from intervening in other state's affairs. On the other hand, sovereignty also implies the competences of the state and the exercise thereof from which derive jurisdiction and independence from other states.[90]

VI The Uncertainty of Cyber Sovereignty – Moving from *Iure Imperii* to *Iure Gestionis*?

1 Implications of Cyber Sovereignty

The term cyber sovereignty is used on quite a large scale at the moment. Yet its content and defining elements are unclear and vague.[91] According to the conclusion of UNGGE, a state enjoys sovereignty in relation to the ICT infrastructure on its territory,[92] but it cannot have sovereignty in the sense of control and exclusiveness over the data concerning private persons or private companies (such as personal data and data giving access to the banking digital system). If one transposes the sovereignty idea to the cyber environment, this implies exercising control therein over the elements that support sovereignty. In this regard, the works of GGE and OEWG do not refer to an abstract idea of sovereignty; they take into consideration the ICT infrastructure belonging to the state or located on its territory, which makes sense and is fully compatible with the features and elements of sovereignty. There is no clear position among states concerning the distinction between sovereignty as a principle and sovereignty as a rule.[93]

---

87 Cassese (n 86) 51–52.

88 Bennouna (n 80) 41.

89 Bennouna (n 80) 42.

90 Crawford (n 17) 448.

91 Baezner, Robin (n 10) 2.

92 von Heinegg (n 16) 19.

93 For further details and analysis, Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views,' (2020) The Hague Program for Cyber Norms Policy Brief 4–7. <https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views> accessed 15 October 2024.

On the other hand, the concept of cyber sovereignty is opposed to the idea of a completely free cyber environment accessible to all. It involves the potential of states to control the flow of data and information and to take control of these.[94]

The most important legal effect of recognising cyber sovereignty as implying an international obligation is that, in case of violation, the mechanism of international responsibility will be activated. In this regard, the award associated with the *Nicaragua* case by the International Court of Justice is relevant, which states the following: 'If a State acts in a way *prima facie* incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then whether or not the State's conduct is in fact justifiable on that basis, the significance of that attitude is to confirm rather than to weaken the rule.'[95]

At the same time, we must observe the 'paradox' of sovereignty[96] concerning the connection between the existence of states and international law in this particular environment. In other words, the silence of states or their ambiguous position may be the best way to ensure the application of international law in cyberspace. On the other hand, cyber sovereignty may not refer exclusively to state governance,[97] taking into account the diversity of users and actors in cyberspace.

2 Cyber Sovereignty as a Form of Control

States consider the currently identified rules and principles for their conduct in cyberspace as a putative normative order[98] and the present digital empire should reconcile different types of approaches. State practice will be an essential element in clarifying aspects of sovereignty in cyberspace, as well as its scope and limits. However, states are reluctant to expressly present their position in this regard. Few states have adopted specific regulations in this area apart from declarations of principle expressed within the UN or other bodies, and their views have been publicly expressed.

The concept of cyber sovereignty was first used and intensely promoted by China and includes several prerogatives of the state, under national law, to regulate the conduct of private persons related to the Internet and the use of personal data within its territory as a means of protecting the information space, in accordance with the general policy on

94 Metcalf (n 12) 1.

95 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14, 98 [186].

96 'Is that states must be capable of binding themselves if International Law is to exist, and also incapable of binding themselves through International Law if they are to be absolutely independent.' Besson (n 70) 377.

97 Andrea Leiter, 'Cyber Sovereignty: A Snapshot from a field in motion' (2020) 61 Harvard International Law Journal Frontiers 2.

98 Nicholas Tsagourias, 'The Slow Process of Normativizing Cyberspace' (2019) 113 (71) American Journal of International Law Unbound 73, DOI: https://doi.org/10.1017/aju.2019.9

controlling the Internet and the flux of data.[99] The Golden Shield and Great Firewall of China started as a project in 1996 and was implemented in 2008. It is the perfect example in this regard, as it establishes full state control of information and access to information. It is a comprehensive system of Internet surveillance and censorship implemented by the government of China with the purpose of regulating online content and controlling the flow of information within its borders.[100] Scholars and ONGs have extensively documented the impact of the Golden Shield on freedom of expression and privacy in China. The analysis provides details of the legal and technical mechanisms used to implement Internet censorship and surveillance.[101]

Despite all censorship policies and measures adopted by China, it is building digital infrastructure in many countries around the world[102] together with the surveillance techniques that are acceptable to authoritarian countries. This approach is reflected and extended by the domestic legislation of the Russian Federation, which adopted in 2019 the *'Sovereign Internet Law'*,[103] establishing the legal framework for controlling the Internet inside its borders.[104] The Russian Federation claims that it has created its own national network, tests have already been undertaken, and users have not experienced any trouble or did not even realise the change. Previously, in December 2016, the President of the Russian Federation approved by Decree the Doctrine of Information Security.[105] This means creating its own national Internet and cyber environment and separating it from international cyberspace.[106] The Russian government employs various mechanisms to filter and censor online content, including the use of Internet filtering technology, blocking

---

[99] Broeders, Adamson, Creemers (n 15) 2.

[100] Gergely Gosztonyi, *Censorship from Plato to Social Media* (Springer 2023, Cham) 103–107, DOI: https://doi.org/10.1007/978-3-031-46529-1_7

[101] Maya Wang, 'China's Dystopian Push to Revolutionize Surveillance', (2017) <https://www.hrw.org/news/2017/08/18/chinas-dystopian-push-revolutionize-surveillance> 15 October 2024; Amnesty International, 'Freedom from Censorship! China's Choice, (2008) <https://www.amnesty.org/en/wp-content/uploads/2021/06/asa170322008eng.pdf> accessed 15 October 2024; Jonathon Keats, ''Great firewall', Virtual Words: Language on the Edge of Science and Technology' (Oxford University Press 2010, New York).

[102] Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press, New York, 2023), DOI: https://doi.org/10.1093/oso/9780197649268.001.0001

[103] Moynihan (n 7).

[104] Alena Epifanova, 'Deciphering Russia's "Sovereign Internet Law" Tightening Control and Accelerating the Splinternet' (2020) 2 German Council on Foreign Relations DGAP Analysis.

[105] It stated that 'The Constitution of the Russian Federation, universally recognized principles and norms of international law, international treaties signed by the Russian Federation... form the legal framework of the Doctrine' (§ 4) and that 'Information security activities of government bodies is based on the following principles... (e) compliance with the universally recognized principles and norms of international law, international treaties to which the Russian Federation is a party and laws of the Russian Federation' (§ 34) <http://www.scrf.gov.ru/security/information/DIB_engl/> accessed 15 October 2024.

[106] Elena Sherstoboeva, 'Russian Bans on 'Fake News' about the war in Ukraine: Conditional truth and unconditional loyalty' (2024) 86 (1) International Communication Gazette 36–54, DOI: https://doi.org/10.1177/17480485231220141

access to websites and social media platforms, and imposing restrictions on certain types of online content, such as political dissent or criticism of the government. Russia conducts extensive surveillance of Internet activities, including monitoring online communications, tracking individuals' browsing histories and intercepting electronic communications. This surveillance apparatus is used to identify and suppress dissenting voices, monitor political activists and opposition groups and maintain social control.[107]

The justification given by the Russian President is that these are security measures intended to protect the state in the event of an 'emergency or foreign threat like a cyberattack'.[108] Under the law, the state has the prerogative to control the Internet through Russian-controlled infrastructure and to create a system of domain names. From the perspective of its consequences, such a measure constitutes a disconnection of the Russian infrastructure network from the global network and constitutes censorship for its users.[109]

Such a technical possibility may be put into practice without great difficulty and could be seen as a display of territorial jurisdiction.[110] Yet, if all states created and isolated their national networks in the name of cyber sovereignty, the result would no longer correspond to the idea of an international global network as we know and use it today and would definitely involve sacrificing the Internet.[111] It would involve just an extension of the national territory, entirely controlled by the state, including control over data, the flux of data, users, technical parameters and the overall characteristics of this space.

A different approach, more tempered in this regard, is associated with France and was expressed in its 2017 International Strategy[112] and the 2018 Strategic Review of Cyberdefense.[113] The latter states that 'the principle of sovereignty applies to cyberspace. In this respect, France reaffirms its sovereignty over information and communication technologies (ICT) infrastructure [*systèmes d'information*], persons and cyber activities located within its territory, subject to its international legal obligations.'

In defining the threshold of a sovereignty breach, the approach focuses on the conduct representing the ICT system penetration, not the consequences. France has developed

---

[107] Gergely Gosztonyi, 'Special models of internet and content regulation in China and Russia' (2021) (2) ELTE Law Journal 87–99, DOI: https://doi.org/10.54148/ELTELJ.2021.2.87

[108] <https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html> accessed 15 October 2024.

[109] Gergely Ferenc Lendvai, 'Media in War: An Overview of the European Restrictions on Russian Media' (2023) 8 (3) European Papers 1235–1245, DOI: http://doi.org/10.15166/2499-8249/715

[110] von Heinegg (n 16) 9.

[111] Mueller (n 5) 5.

[112] 'La stratégie internationale de la France pour le numérique' 15 December 2017, France Diplomatie, <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-strategie-internationale-de-la-france-pour-le-numerique> accessed 15 October 2024.

[113] François Delerue, Aude Géry, 'France's Cyberdefense Strategic Review and International Law' (2018) Lawfare <https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law> accessed 15 October 2024.

a national system of defining and qualifying the actions that constitute a cyber security incident.

Another example of a global approach to cyberspace was the National Cyber Strategy[114] of the United States of America. This focused on an open and global cyberspace and promoted 'a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity.[115] These principles should form a basis for cooperative responses to counter irresponsible state actions inconsistent with this framework.'

The new Strategy issued in 2023 focuses on resilience in cyberspace and highlights the threats presented by authoritarian governments such as China and North Korea.[116] The publicly expressed positions of states concerning sovereignty in cyberspace may be very different in practice, which makes it difficult to argue for the existence of an *opinio iuris* on how it applies, yet this does not infer a normative gap.[117] Australia expressed this position at the OEWG session on 2 July 2020, affirming the need to find topics of confluence between states in order to ensure a peaceful and stable cyberspace.[118]

The United Kingdom has also developed a national cybersecurity strategy, created a National Cyber Security Centre[119] and sustains the applicability of sovereignty as a principle, considering that there is no rule of sovereignty in cyberspace.[120] From a theoretical and practical perspective, the differences between the two approaches to sovereignty – as a principle and as a rule – are not very clear, and their effectiveness may not be significant because states have international obligations in each case.

---

[114] 'The White House, 'National Cyber Strategy of the United States of America' (2018) 20, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> accessed 15 October 2024.

[115] cf Roland Kelemen, Ádám Farkas, 'The relationship between social media platforms and hybrid conflicts' (2022) 11 (1) In Medias Res 96–108.

[116] The White House, 'National Cybersecurity Strategy' (2023) <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf> accessed 15 October 2024.

[117] Tolppa (n 32).

[118] *Australian Intervention*, OEWG Virtual Meeting: 2 July 2020, <https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-australia-2-july-2020.pdf> accessed 15 October 2024.

[119] See National Cyber Security Centre <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do> accessed 15 October 2024.

[120] Jeremy Wright, 'Cyber and International Law in the 21st Century' (2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 15 October 2024.

VII Conclusions

Additional efforts by states and international organisations are required to clarify the idea of cyber sovereignty by outlining its dimensions and restrictions in relation to the fundamental principle of state sovereignty. States asserting cyber sovereignty may impose restrictions on online content deemed to be offensive, harmful or contrary to national interests. While states have a legitimate interest in regulating certain types of content, such as hate speech or incitement to violence, overly broad or vague regulations can result in censorship and limit individuals' ability to exercise freedom of expression online.

In cyberspace, the interests of many parties are interconnected. The concept of cyber sovereignty contradicts the idea of global cyberspace governance and ignores the interests of other actors, such as private companies and individuals, who use cyberspace. There are no legal hurdles in international law to the regulation of cyberspace and the behaviour of states and other stakeholders. Actions may involve leveraging existing principles and standards that can be tailored to this unique environment. State sovereignty in cyberspace is limited and distinct from authority over physical territories. A pragmatic approach comprises understanding that state sovereignty in cyberspace pertains to the physical infrastructure underpinning cyberspace's existence while explaining concerns related to state jurisdiction, extraterritorial impacts and defining violations of sovereignty in cyberspace.