1. The legal status of cyberspace: sovereignty redux?

Nicholas Tsagourias

1. INTRODUCTION

Cyberspace is sometimes described as a purely non-legal domain. According to John Barlow's *A Declaration of the Independence of Cyberspace* 'legal concepts do not apply to cyberspace'.¹ The view of cyberspace as a non-legal domain is based on a number of assumptions. The first assumption is that cyberspace is different from real spaces: its a-territorial, borderless and ubiquitous character differentiates it from the physical and bounded spaces that are subject to legal regulation. The second assumption is that cyberspace, true to its original conceptualisation and design and the involvement of multiple stakeholders, should remain an open, decentralised and participatory space not hampered by legal regulation or, at least, not subjected exclusively to State-led regulation.²

Yet, the view that cyberspace is subject to law and indeed to international law is not in dispute anymore. The 2013 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security [GGE] affirmed that international law and in particular the United Nations [UN] Charter as well as State sovereignty and the international norms and principles that flow from sovereignty apply to cyberspace.³ As the UN Secretary-General also noted in the foreword to the report, '[t]he recommendations point the way forward for anchoring ICT security in the existing framework of international law and understandings that govern State relations and provide the foundation for international peace and security'.⁴ The 2015 GGE Report went even further by setting out specific international norms and principles that apply or should apply to cyberspace. The Report lists 11 'voluntary, non-binding norms, rules or principles of responsible behaviour of States' to promote an open, secure, stable, accessible and peaceful cyber environment.⁵ It also lists six international law principles that apply to cyber space and cyber activities, one of which is the principle of sovereignty as also reaffirmed

¹ John P Barlow, 'A Declaration of the Independence of Cyberspace' (Davos 1996) <https://www.eff.org/cyberspace-independence>.

² David R Johnson and David G Post, 'Law and borders: The rise of law in cyberspace' (1996) 48 *Stanford Law Review* 1367. *Contra* see Jack L Goldsmith, 'Against cyberanarchy' (1998) 65 *University of Chicago Law Review* 1199.

³ UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/68/98 (24 June 2013) paras 19–20.

⁴ *Ibid.*, 4.

⁵ UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/70/174 (22 July 2015) para 13.

in the 2021 GGE Report.⁶ Various States or international organisations have also affirmed the application of international law to cyberspace.⁷

Applying international law to cyberspace is important for many reasons. The first reason is that international law performs a regulatory function by setting out the principles and rules that apply to cyberspace thus shaping conduct and determining what is legal and what is illegal. Second, it plays a performative function by constructing in legal terms the ontology, identity, and status of cyberspace. Third, international law embeds in its principles and rules authoritative choices about the nature, content, and use of cyberspace whilst at the same time moulds such choices through its own principles and rules. In doing so, international law ‘naturalises’ cyberspace because it embeds it into known legal categories and models of regulation and promotes stability and order not only in cyberspace but also in the international environment to which cyberspace is an appendix.

This chapter will thus examine the legal status of cyberspace as well as the status and import of the principle of sovereignty in cyberspace. The chapter is structured as follows. Section 2 discusses the nature of cyberspace and argues that cyberspace combines a physical, a social and a logical layer. Section 3 explores the question of whether the principle of sovereignty applies to cyberspace. In order to do this, the chapter explains the place, role and content of the principle sovereignty in international law and concludes that cyberspace is subject to the principle of sovereignty. Section 4 considers the legal status and import of the principle of sovereignty in cyberspace in view of claims that deny its legal significance in cyberspace. It contends that the principle of sovereignty is a legal principle that produces legal consequences. Section 5 explores the question of whether cyberspace itself can become sovereign but con-

⁶ Ibid., para 26. ‘Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security’, UN Doc A/76/135 (14 July 2021) para 71(b).

⁷ Finland, *International law and cyberspace: Finland’s national position* (2020) 1–3, <https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859>; *Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace* (July 2020) <https://www.aldiplomasy.com/en/?p=20901>; Kersti Kaljulaid, President of Estonia, *President of the Republic at the opening of CyCon 2019* (29 May 2019) <https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html>; République Française, Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberspace* (2019); The Netherlands, *Letter to the parliament on the international legal order in cyberspace* (5 July 2019) <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>; Portugal, *National Strategy for Cyberspace Security 2019-2023* Portuguese Official Journal, Series 1 - No. 108 - 5 June, 2019, Annex, section 1; UK United Kingdom Attorney General’s Office, *Cyber and International Law in the 21st Century* (23 May 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>; Australia, *Australia’s International Cyber Engagement Strategy* (4 October 2017) Annex A: Australia’s position on how international law applies to state conduct in cyberspace, available at <https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australias-international-cyber-engagement-strategy>; Brian Egan, ‘International Law and stability in cyberspace’ (2017) 35 *Berkeley Journal of International Law* 169; Harold Hongju Koh, ‘International law in cyberspace’ (2012) 54 *Harvard Journal of International Law Online* 1. For the views of OAS member States see OEA/Ser.Q, CJI/doc. 603/20 rev.1, 5 March 2020, 18–20 and OEA/Ser.Q, CJI/doc. 615/20 rev.1, 7 August 2020, 28–32. For China’s views on sovereignty see Huang and Ying (Ch 26 of this Handbook). For NATO, see Wales Summit Declaration, 5 September 2014 para 62, available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm and Hill (Ch 24 of this Handbook).

cludes that this is impossible because it is intermediated by States and their people. It also contends that big tech companies that control cyberspace and its infrastructure are not sovereigns. Section 6 discusses but rejects the proposition that cyberspace can become a global commons because it does not fulfil the requisite criteria and because States have expressed no desire to designate it as such. Section 7 contains concluding remarks.

2. WHAT IS CYBERSPACE?

Questions as to what cyberspace is, and more specifically whether cyberspace is a corporeal entity, an intangible entity or a bundle of functions have technical, philosophical, political, sociological, and legal origins and ramifications.⁸ Although I will not engage here with the various debates concerning the ontology of cyberspace for lack of expertise, I will offer a description of cyberspace in order to grasp the object of the enquiry because its features and attributes shape the way international law understands and, consequently, treats cyberspace. International law can then apply its principles and rules to cyberspace on the basis of legal assumptions, analogies, and categorisations or develop purpose-built legal principles and rules.

According to Kuehl's definition, cyberspace is 'a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies'.⁹ According to another definition, cyberspace is composed of three layers: a physical layer composed of the cyber infrastructure; a second layer of software logic; and, a third layer of data.¹⁰ These definitions highlight the physical and informational dimensions of cyberspace but omit the human dimension of cyberspace. In my opinion, the most inclusive definition and the one adopted for the purposes of this chapter is the definition provided by the US Department of Defense which identifies three co-joint components of cyberspace. As it explains 'cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona'.¹¹ The physical layer consists of the IT devices and infrastructure such as computers, integrated circuits, cables, communications infrastructure, servers, routers, switches; the logical layer consists of the software logic, data packets and electronics; and the cyber-persona layer consists of 'digital representations of an actor or entity identity in cyberspace'.¹² Cyber-personas may relate to real people but may also be artificial whereas a person may have multiple digital personas. This layer can alternatively be described

⁸ David Koepsell, *The Ontology of Cyberspace: Law, Philosophy, and the Future of Intellectual Property* (Open Court Publishing 2003) 10; Julie E Cohen, 'Cyberspace as/and space' (2007) 107 *Columbia Law Review* 210.

⁹ Daniel T Kuehl, 'From cyberspace to cyberpower: Defining the problem' in Franklin D Kramer, Stuart H Starr and Larry K Wentz, *Cyberpower and National Security* (National Defense University Press 2009) 28.

¹⁰ Lior Tobanksy, 'Basic concepts in cyber warfare' (2011) 3 *Military and Strategic Affairs* 75, 77–8.

¹¹ US Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (8 June 2018) I-2. See also AJP-3.20, Allied Joint Doctrine For Cyberspace Operations, Edition A Version 1 (January 2020) 1.9–1.12.

¹² US Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (8 June 2018) I-4.

as the social layer of cyberspace and this is how it will be referred to in the remainder of this chapter. These layers are not separate but intertwined. Even if the core of cyberspace is virtual and cyber interactions are conducted through logistics rather than through physical acts, they are dependent on the physical and social layer of cyberspace.

Understanding the nature of cyberspace is also important because different disciplines may focus on different layers; for example, computer science usually focuses on the logical layer whereas law, and international law for that matter, focuses on the physical and social layer of cyberspace to the extent that law governs objects, persons, spaces, relations, or effects.

Having explained the nature of cyberspace and having identified its layers, in the next section I will examine the application of the principle of sovereignty to cyberspace because sovereignty is a foundational principle of international law.

3. CYBERSPACE AND SOVEREIGNTY

In its traditional definition, sovereignty denotes *summa potestas* that is, supreme and plenary authority and power.¹³ According to Bodin who introduced the concept of sovereignty in political theory, sovereignty is an organising principle representing the consolidation and indivisibility of power within a political entity.¹⁴ Bodin identified the holder of such power in the person or institution of the sovereign and, in doing so, he subjectivised sovereignty.

Sovereignty is also a foundational principle of international law. As the International Court of Justice (ICJ) said in the *Nicaragua Case*, the whole international law rest upon sovereignty.¹⁵ Sovereignty is constitutive of international law because it gives international law its ontology; it is an organising principle in that it identifies the units of authority in international law and international relations and defines and delimits their competences and powers; it is an operational principle because it is the engine that generates, applies, and enforces international law; and it is functional principle because it determines whether and to whom international law applies.

In international law, the holder of sovereignty is the State. As a State attribute, sovereignty is a unitary concept joining together its internal aspect of supreme, plenary and exclusive authority and power within the State¹⁶ and its external aspect of autonomy and independence vis-à-vis other States, plenary power to regulate externalities, and power to create, implement, and enforce international law. In the words of Judge Alvarez, by sovereignty ‘we understand

¹³ Alan James, *Sovereign Statehood* (Allen & Unwin 1986) 267–9; Francis Harry Hinsley, *Sovereignty* (CUP 1986); Stephen D Krasner, *Sovereignty: Organized Hypocrisy* (Princeton University Press 1999) 1–42; Samantha Besson, ‘Sovereignty’ in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP 2012).

¹⁴ Jean Bodin, *Les six livres de la République*, 1576, livre I, ch. 8, 131.

¹⁵ *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, Judgment (Merits) [1986] ICJ Rep 14, para 263.

¹⁶ As was said in *The Exchange v McFaddon*, 11 U.S. (7 Cranch 116) 116 (1812):

The jurisdiction of a nation within its own territory, is exclusive and absolute. It is susceptible of no limitation not imposed by itself. Any restriction deriving validity from an external source would imply a diminution of its sovereignty to the extent of that restriction, and an investment of that sovereignty to the same extent in that power which could impose such restriction.

the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States'.¹⁷

That having been said, it is true that sovereignty in international law has a strong territorial dimension.¹⁸ This can be explained by the fact that its emergence as a political and legal concept coincided with the emergence of the State as a political unit following the apportionment of territories and the political and legal recognition of such territorial compartmentalisation by the Treaty of Westphalia.¹⁹ The Peace of Westphalia redrew the political boundaries of authority from the previous state of overlapping authorities within the same territory to that of consolidated, supreme and plenary authority over a distinct piece of territory which was carved out because of the successful assertion of power by a single authority, the sovereign.

It follows from this that territory is not just a geographical or physical construct but a legal and political construct: it concerns the organisation of spaces for political and legal purposes or, put differently, it refers to a mode of organising sovereign power.²⁰ Territory provides a bounded and defined space where sovereignty can manifest itself exclusively and be realised effectively; it draws internal as well as external physical, legal and political borders without which sovereignty would remain abstract and unsubstantiated; it organises sovereignties and provides order in the international society by allowing States to coexist side by side without encroaching onto another's sovereignty. However, even if territory is an aspect of sovereignty and is protected by sovereignty, it is not synonymous with sovereignty. It is a container of sovereignty but sovereignty as authority and power can extend beyond territory. In other words, sovereignty is both territorial and a-territorial. In the latter case, the expanse of sovereignty and any limitations thereto are subject to sovereignty itself and not to territory.²¹ It is for this reason that in this chapter I use the term 'principle of sovereignty' or 'State sovereignty' rather than 'territorial sovereignty'.²²

Having explained the meaning of sovereignty in international law and its relation to territory, the question to ask is whether the principle of sovereignty can apply to cyberspace. Barlow's *Declaration of the Independence of Cyberspace* envisioned cyberspace as a space not subject to sovereignty. In academic writings, Johnson and Post argued that cyberspace cannot be subject to sovereignty but instead, cyberspace should be subject to its own distinct system of

¹⁷ *Corfu Channel Case (UK v Albania)* (Separate Opinion of by Judge Alvarez) [1949] ICJ Rep 43.

¹⁸ Jens Bartelson, *A Genealogy of Sovereignty* (CUP 1993) 26. See also Montevideo Convention on the Rights and Duties of States (signed 26 December 1933, entered into force 26 December 1934).

¹⁹ Peace of Westphalia, signed on 30 January 1648 and 24 October 1648. The Peace of Westphalia and its contribution to international law is one of the foundational 'myths' of international law notwithstanding any contrary views. See Daniel Bethlehem, 'The end of geography: The changing nature of the international system and the challenge to international law' (2014) 25 *European Journal of International Law* 9, 13; Nicholas G Onuf, 'Sovereignty: Outline of a conceptual history' (1991) 16 *Alternatives: Global, Local, Political* 425, 437.

²⁰ Thomas Forsberg, 'Beyond sovereignty, within territoriality: Mapping the space of late-modern (geo) politics' (1996) 31 *Cooperation and Conflict* 355; John G Ruggie, 'Territoriality and beyond: Problematising modernity in international relations' (1993) 47 *International Organization* 139. As Judge Max Huber opined, 'territorial sovereignty serves to divide between nations the space upon which human activities are employed'; *Island of Palmas Case (or Miangas) (United States v Netherlands)* [1928] Reports of International Arbitral Awards 839.

²¹ Richard T Ford, 'A history of jurisdiction' (1999) 97 *Michigan Law Review* 843, 853–4.

²² Peter J Taylor, 'The state as container: Territoriality in the modern world-system' (1994) 18 *Progress in Human Geography* 151.

legal regulation.²³ For them, it is not only the borderless and a-territorial nature of cyberspace that make it adverse to the standard system of territorially-based international legal regulation based on the overlap between the physical space represented by States and the ‘law-space’, but also the fact that sovereignty’s principles of validity exhibited in territorially-based entities in the form of power, legitimacy, effects and notice are impossible or at best diluted in cyberspace. More specifically, the lack of borders in cyberspace deprives sovereigns of the ability to exercise their power over defined peoples and territories and deprives sovereign power from the legitimising effect of consent. It also deprives users from notice when entering a different jurisdiction. It is because of these features and the need to have an effective regulatory system appropriate to cyberspace that cyberspace should develop its own regulatory system based on self-regulation.²⁴

The no-sovereignty thesis described above is based on a concept of cyber-exceptionalism and on a territorial reading of sovereignty. It should be noted however that Johnson and Post do not deny that law has a role to play in cyberspace but they propose a different regulatory system which is more appropriate to the features of cyberspace.

The normative premises of the no-sovereignty thesis were challenged by Jack Goldsmith in his article ‘Against cyberanarchy’.²⁵ For him, there is nothing unexceptional as far as cyberspace is concerned whereas the jurisdictional and enforcement inadequacies of sovereign power in cyberspace identified by Johnson and Post have been exaggerated. As he explains, cyberspace consists of persons and objects and for this reason States can exercise power over people and objects on their territory. States can also regulate the local effects of extraterritorial activities. Also, traditional legal tools can resolve the multi-jurisdictional problems implicated in cyberspace and thus overcome the problem of legitimacy and validity. Furthermore, the standard rules of enforcement based on a person’s location, personal jurisdiction or extradition can also apply to cyber activities. Regarding the issue of notice, Goldsmith says that there is a general notice that data may cross frontiers. In sum, according to Goldsmith, territorial sovereigns can regulate cyberspace through existing techniques.

From the preceding discussion it transpires that whether sovereignty applies to cyberspace boils down to the question of whether a State can exercise jurisdiction over cyberspace or, more specifically, over its layers. The reason that jurisdiction emerges as the defining attribute is because jurisdiction is the instantiation of the legal dimension of sovereignty in the form of prescription, application, enforcement, and adjudication.²⁶

In cyberspace, a State can assert its sovereignty by exercising jurisdiction over the cyber infrastructure located on its territory, over its nationals within its territory as well as over non-nationals, including legal persons such as companies within its territory.²⁷ A State can also exercise jurisdiction over nationals outside its territory on the basis of active or passive

²³ Johnson and Post (n 2).

²⁴ Also see Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006).

²⁵ Goldsmith (n 2).

²⁶ For jurisdiction in cyberspace see Kohl (Ch 4 of this Handbook). See also James Crawford, *Brownlie’s Principles of Public International Law* (OUP 2012) 456–7; Frederick A Mann, ‘The doctrine of international jurisdiction revisited after twenty years’ in *Academie De Droit International De La Haye, Recueil Des Cours* (Martinus Nijhoff 1984).

²⁷ *Nottenbohm Case (Lichtenstein v Guatemala)* [1955] ICJ Rep 4, para 23; Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317, paras 32–41.

nationality.²⁸ Passive nationality can, for example, establish jurisdiction in relation to acts of cyber terrorism.²⁹

Furthermore, a State can exercise jurisdiction over information circulated through cyberspace at the point of delivery, the point of reception, or when the information crosses through wires and lines falling within its jurisdiction.³⁰ A State can also exercise jurisdiction over web addresses to the extent they are registered in that State.

More than that, a State can exercise jurisdiction over the effect of cyber acts if they were felt within its territory.³¹ The effects doctrine was first enunciated by the Permanent Court of International Justice in the *Lotus* case and since then it has been accepted as a jurisdictional ground.³² Nonetheless, some questions remain including whether the effects should have been materialised before exercising jurisdiction or whether foreseeable effects can be taken into account;³³ whether the effects should be substantial; or whether they should be detrimental in order to trigger a State's jurisdiction. A particular problem in relation to cyberspace is that cyber effects may be felt in a number of different jurisdictions. If all affected States were to assert jurisdiction, the practical difficulties are considerable. Even if international law contains rules on conflicts of jurisdiction, the assertion of jurisdiction in such situations may affect the principle of fairness. In order to address these issues, certain States require 'substantial contacts'³⁴ with that State or ascribe to the principle of targeting according to which it is the State targeted by the impugned behaviour that can exercise jurisdiction irrespective of any effects felt in other jurisdictions.³⁵ That having been said, the effects doctrine is not universally accepted.

A State can also assert its jurisdiction over cyber conduct that endangers its vital interests regardless of where, or by whom, such conduct has been committed.³⁶ This refers to the protective principle of jurisdiction³⁷ which provides States with an additional ground to protect themselves against injuries by non-State actors. This would allow, for example, a State to exercise

²⁸ *Arrest Warrant Case (Democratic Republic of Congo v Belgium)* (Joint Separate Opinion of Judges Higgins, Kooijmans and Buergenthal) [2002] ICJ Rep 3, para 47; Restatement of the Law Third, The Foreign Relations Law of the United States (1986) para 402.

²⁹ *US v Bin Laden*, 92 F.Supp.2d 189 221 (S.D.N.Y., 13 March 2000).

³⁰ *R v Sheppard & Amor* [2010] EWCA Crim 65; Sean Kanuck, 'Sovereign discourse on cyber conflict under international law' (2010) 88 *Texas Law Review* 1571, 1573–5.

³¹ For the effects doctrine see also Kohl (Chapter 4 of this Handbook).

³² *The Case of the S.S. "Lotus"* (Judgment) [1927] PCIJ Rep Series A No 10 18, para 23; *Arrest Warrant of 11 April 2000* (n 28) para 47.

³³ *U.S. v Yousef*, 327 F.3d 56, 112 (2d Cir., 2003).

³⁴ *CompuServe, Inc v Patterson* 89 F. 3d 1257 (6th Cir.1996); *Zipco Mfg Co v Zipco Dot Com Inc* 952 F Supp 1119 (WD Pa 1997).

³⁵ Thomas Schultz, 'Carving up the Internet: Jurisdiction, legal orders, and the private/public international law interface' (2008) 19 *European Journal International Law* 799, 816.

³⁶ *The Case of the S.S. "Lotus"* (n 32) (Dissenting opinion by Judge Loder) 35–6 (when the 'offences [...] are directed against the State itself or against its security or credit [t]he injured State may try the guilty persons according to its own law if they happen to be in its territory or, if necessary, it may ask for their extradition').

³⁷ Research on International Law under the Auspices of the Harvard Law School, Part II, 'Jurisdiction with Respect to Crime' (1935) 29 *American Journal International Law* (Supp.) 435, 543; *Attorney-General of Israel v Eichmann* (1961) (District Court), 36 ILR 5 and *Eichmann v Attorney-General* 36 ILR 277 (Supreme Court); Ian Cameron, *The Protective Principle of International Criminal Jurisdiction* (Dartmouth 1994).

jurisdiction over remotely conducted cyber espionage if its security has been compromised. However, the problem with this head of jurisdiction is that the notion of ‘essential’ or ‘vital’ State interests is not settled or well-defined.

In sum, a State can assert its sovereignty over the physical layer of cyberspace located on its territory and over information passing through its infrastructure or beginning and ending on its territory. It can also assert its sovereignty over the social layer that is, over all persons on its territory as well as over its nationals outside its territory. A State can finally assert its sovereignty over the effects of cyber activities that are felt within the State or affect its vital interest regardless of their provenance.

The above describe direct assertions of sovereignty by a State but a State can assert its sovereignty also indirectly when the application of its law has ‘spill over’ effects on cyberspace. For instance, if a State regulates access to certain materials such as pornographic or terrorist materials, it makes their circulation through cyberspace more difficult, although not impossible, in the absence of a common regulatory regime in cyberspace. A State can also do so by globalising the application of its own laws. The dispute between Google and France’s *Commission Nationale de l’Informatique et des Libertés* (CNIL) concerning the ‘right to be forgotten’ that is, the right to remove links containing personal information, is instructive. Google removed material from google.fr and introduced a geoblocking feature to prevent European users from being able to see delisted links whereas CNIL however demanded worldwide delisting. Google appealed to the Conseil d’État which referred the case to the Court of Justice of the European Union for a preliminary ruling.³⁸ Google argued that such a demand shows ‘disregard of public international law’s principles of courtesy and non-interference’³⁹ which are part of the principle of sovereignty. The Court ruled that Google does not have an obligation to comply globally with the EU law on the right to be forgotten, however it did not preclude this possibility. Instead, the Court effectively recognised the competence of national authorities to do so when it opined that:

a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights ... a data subject’s right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine.⁴⁰

The Court also said that the EU can lay down an obligation of global de-referencing.⁴¹

The most radical assertion of sovereignty is when States partition cyberspace by creating sovereign cyber zones. For example, China is promoting the principle of cyber sovereignty.⁴² In 2010, a White Paper entitled “The Internet in China” was published which stressed the

³⁸ C-507/17, *Google Inc v Commission nationale de l’informatique et des libertés (CNIL)*, Judgment of 24 September 2019 ECLI:EU:C:2019:772.

³⁹ *Ibid.*, para 37. Although the EU is not a sovereign State, the ruling concerns the General Data Protection Regulation (GDPR) which EU States apply as national law.

⁴⁰ *Ibid.*, para 72.

⁴¹ *Ibid.*, para 58. Although the EU is not a State and does not have sovereignty, the point made here is that national laws (including the EU law) can have extraterritorial regulatory scope.

⁴² Hao Yeli, ‘A Three-Perspective Theory of Cyber Sovereignty’ (2017) 17 *Prism: Journal of the Center for Complex Operations* 108; Yi Shen, ‘Cyber Sovereignty and the Governance of Global

sovereign implications of the internet.⁴³ Chinese President Xi Jinping stressed the critical importance of cyber sovereignty to national sovereignty.⁴⁴ The protection of sovereignty in cyberspace is also part of China's national security doctrine.⁴⁵ The *International Strategy of Cooperation on Cyberspace* released in 2017 states that 'the principle of sovereignty enshrined in the UN Charter covers all aspects of State-to-State relations, which also includes cyberspace'.⁴⁶

China's approach to cyber sovereignty extends to cyber infrastructure under its jurisdiction, over all online activities taking place within Chinese jurisdiction, and over people within China's jurisdiction. In addition to this, sovereignty extends to information entering or becoming available within China's sovereign domain. China asserts its cyber sovereignty in the latter instance through filtering.⁴⁷ Filtering involves technical, political, legal, and social techniques to deny access to certain information from within China or deny entry into China of such information. Filtering takes place at the international gateways of Chinese networks and it has been referred to as the 'Great Firewall' of China. Other ways of asserting sovereignty is by requiring international actors such as tech companies to have local presence; requiring foreign tech companies to comply with local laws in order to do business in China; managing domain names; and requiring the local storage of all personal data, including those of non-nationals.

China deploys the principle of cyber sovereignty in order to protect its internal sovereignty that is, its exclusive and supreme power over its territory and people and in order to maintain its freedom in the way it exercises its sovereignty internally.⁴⁸ The external dimension of cyber sovereignty aligns with China's demand for equal participation in the international governance

Cyberspace' (2016) 1 *Chinese Political Science Review* 81. See also Huang and Ying (Ch 26 of this Handbook).

⁴³ The Internet in China Information Office of the State Council of the People's Republic of China (2010) https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm.

⁴⁴ 'Why Does Cyber Sovereignty Matter?', *China Daily* (16 December 2015) http://www.chinadaily.com.cn/business/tech/2015-12/16/content_22728202.htm.

⁴⁵ Council on Foreign Relations, 'China's New Cybersecurity Law' (2015) <https://www.cfr.org/blog/chinas-new-cybersecurity-law>.

⁴⁶ Ministry of Foreign Affairs of the Peoples Republic of China, *International Strategy of Cooperation on Cyberspace* (2017) https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtw_665250/t1442390.shtml. In its submissions to the second substantive session of the OEWG in 2020, China stated in relation to sovereignty in cyberspace the following:

States should exercise jurisdiction over the ICT infrastructure, resources as well as ICT-related activities within their territories. States have the right to make ICT-related public policies consistent with national circumstances to manage their own ICT affairs and protect their citizens' legitimate interests in cyberspace. States should refrain from using ICTs to interfere in internal affairs of other states and undermine their political, economic and social stability. States should participate in the management and distribution of international Internet resources on equal footings.

<https://www.un.org/disarmament/open-ended-working-group/>.

⁴⁷ Ron Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, *Access Denied: The Practice and Policy of Global Internet Filtering* (MIT Press 2008); Ron Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press 2010).

⁴⁸ According to the *International Strategy of Cooperation on Cyberspace*:

China is committed to upholding peace and security in cyberspace and establishing a fair and reasonable international cyberspace order on the basis of state sovereignty, and has worked actively to build international consensus in this respect. China firmly opposes any country using the Internet to interfere in other countries' internal affairs and believes every country has the right and responsi-

of cyberspace which, for China, should be multilateral that is, inter-State. China rejects the multi-stakeholder model of governance where the private sector has equal standing to States and, although it does not reject the participation of non-State actors, their role, in China's opinion, should be secondary.

Another way of asserting sovereignty in cyberspace is by isolating the national internet. For example, countries such as North Korea,⁴⁹ Iran,⁵⁰ Russia⁵¹ have disconnected or are planning to disconnect national networks from the internet and create national segments of the internet. Such moves are also accompanied by quite far-reaching internal legislation to control information and activities on the national cyber domain such as legislation on blocking and blacklisting, data localisation and access to data, foreign ownership of information providers, encryption and so on. In this way, they can assert their digital sovereignty.

The preceding examples have shown that certain States project a Westphalian concept of State sovereignty to cyberspace. They curve their own sovereign cyberspace by erecting borders through technical means in order to control activities from outside or in order to insulate their national cyber domain. These borders correspond to the borders defining and demarcating territorial sovereignty and, even more critically, they reaffirm sovereignty in its political, social, economic, cultural and territorial dimension.⁵² Whether such a Westphalian 'moment' will take hold and lead to the division of cyberspace into sovereign zones depends on many factors. Technology is a critical factor because it can assist in actually curving cyberspace in the same way that the territorial notion of sovereignty was facilitated by tech-

bility to maintain its cyber security and protect the legitimate rights and interests of various parties in cyberspace through national laws and policies

International Strategy of Cooperation on Cyberspace (n 46).

⁴⁹ Barney Warf, 'The Hermit Kingdom in cyberspace: unveiling the North Korean internet' (2015) 18 *Information, Communication & Society* 109; Saira Asher, 'What the North Korean internet really looks like' (21 September 2016) <https://www.bbc.co.uk/news/world-asia-37426725>.

⁵⁰ 'Iran says its intranet almost ready to shield country from 'harmful' internet' (20 May 2019) <https://en.radiofarda.com/a/iran-says-its-intranet-almost-ready-to-shield-country-from-harmful-internet/29952836.html>.

⁵¹ Robert Morgus and Justin Sherman, 'Analysis: Russia's plans for a national internet', *New America* (19 February 2019) <https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/russias-plans-for-a-national-internet/>; Timothy Lee, 'Putin signs "Internet sovereignty" bill that expands censorship' (5 February 2019) <https://arstechnica.com/tech-policy/2019/05/putin-signs-bill-tightening-government-grip-on-the-russian-internet/>; Lily Hay Newman, 'Russia takes a big step toward internet isolation', *Wired* (5 January 2020) <https://www.wired.com/story/russia-internet-control-disconnect-censorship/>; Alena Epifanova, 'Deciphering Russia's "Sovereign Internet Law" tightening control and accelerating the splinternet', DGAP (German Council of Foreign Relations) Analysis (2020) <https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law>. Also see Julian Nocetti, 'Contest and conquest: Russia and global internet governance' (2015) 91 *International Affairs* 111; Timothy Thomas, 'Russia's expanding cyber activities: exerting civilian control while enhancing military reform' in Stephen J Blank (ed), *The Russian Military in Contemporary Perspective* (Carlisle Barracks, PA., US Army War College Press 2019) 491–574 and Sayapin (Ch 25 of this Handbook).

⁵² According to China's submissions to the UN:

the free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded and that the historical, cultural and political differences among countries be respected; each country has the right to manage its own cyberspace in accordance with its domestic legislation ...

UNGA, *Developments in the field of information and telecommunications in the context of international security*, Report of the Secretary-General, UN Doc A/61/161 (18 July 2006) 4.

nological advances, in particular in cartography, which permitted the demarcation of expanses of territory.⁵³ Beyond technology, there are political, economic, social, and a number of other factors that inform such attempts or consult against such curving. Regardless of how this will pan out, what remains true is that States apply to cyberspace and to cyber activities sovereign configurations of authority and power, albeit with variations and gradations. In view of this, the next question to consider is what is the legal status and import of the principle of sovereignty in cyberspace.

4. THE LEGAL STATUS AND SCOPE OF THE PRINCIPLE OF SOVEREIGNTY IN CYBERSPACE

Although, as explained previously, the importance and place of the principle of sovereignty in international law and in cyberspace is undisputed, recently it has been claimed in relation to cyberspace that sovereignty is just a principle and not a legal rule and, for this reason, it does not engender legal consequences.⁵⁴ It has also been claimed that there is no clear State practice and *opinio juris* supporting the view that sovereignty is a rule (compared to political principle) in cyberspace and that the only rules that have legal import in cyberspace are those prohibiting the use of force and intervention.⁵⁵

In response, I argue that the principle of sovereignty is a stand-alone legal principle that applies to cyberspace and produces legal consequences. In order to prove this point, I will first discuss the relationship between ‘principles’ and ‘rules’⁵⁶ and, following this, I will discuss the legal status, content, and scope of the principle of sovereignty in international law and in cyberspace.

Principles are general normative propositions containing standards and objectives. They may have political or moral origins but principles become legal when they enter a legal system and translate in legal terms the standards and objectives they represent. Legal principles are also consequential; they produce legal consequences themselves and they may also give rise to more specific rules. Rules are specific proscriptions or prescriptions which individuate specific aspects of the underlying legal principle.

As I explained previously, sovereignty is a fundamental principle of international law. It denotes the aggregate of rights that a State has as a State and vis-à-vis other States.⁵⁷ This has

⁵³ Jordan Branch, *The Cartographic State: Maps, Territory, and the Origins of Sovereignty* (CUP 2014).

⁵⁴ United Kingdom Attorney General’s Office (n 7); Paul C. Ney, Jr, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference* (2 March 2020) <https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>; Gary P Corn and Robert Taylor, ‘Sovereignty in the age of cyber’ (2017) 111 *American Journal of International Law Unbound* 207. For the opposite view see Harriet Moynihan, ‘the application of international law to state cyberattacks: sovereignty and non-intervention’ (Chatham House Research Paper, December 2019) <https://reader.chathamhouse.org/application-international-law-state-cyberattacks-sovereignty-and-non-intervention?preview=1>.

⁵⁵ The inclusion of non-intervention, which is usually referred to as a principle, seems to be a contradiction. In my opinion, it strengthens my view that sovereignty is a legal principle as explained in this chapter.

⁵⁶ Ronald Dworkin, *Taking Rights Seriously* (Harvard University Press 1978) Chs 2 and 3.

⁵⁷ Crawford (n 26) 448.

been affirmed in General Assembly and Security Council resolutions as well as in international instruments.⁵⁸ This is also how the ICJ treats sovereignty. In the *Corfu Channel* case the Court held that '[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations' and it went on to say that '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'.⁵⁹ Moreover, sovereignty is a principle that produces legal consequences. In the *Nicaragua* case, the Court held that US overflights violate Nicaragua's sovereignty.⁶⁰ In *Costa Rica v Nicaragua*, the ICJ held that by 'excavating three *carios* and establishing a military presence on Costa Rican territory, Nicaragua has violated the territorial sovereignty of Costa Rica'.⁶¹

Treating sovereignty as a legal principle is not very different from treating it as a 'rule' regarding its legal consequences with the caveat that, as a principle, its normative content is broad and its application is case and context specific in contrast to rules that lead to specific determinations. As a matter of fact, the ICJ uses the concept of legal principle and legal rule interchangeably when referring to certain important principles/rules. In the *Nicaragua* case for example the ICJ treated non-intervention and the non-use of force as both principles and rules.⁶² The Court also explained in another case that:

the association of the terms 'rules' and 'principles' is no more than the use of a dual expression to convey one and the same idea, since in this context 'principles' clearly means principles of law, that is, it also includes rules of international law in whose case the use of the term 'principles' may be justified because of their more general and more fundamental character.⁶³

Moreover, according to the Court, a violation of a specific rule such as the rule on the non-use of force can also be a violation of State sovereignty which alludes to what I said above that sovereignty can give rise to specific rules. These rules individuate and protect certain of its elements.⁶⁴ Among these rules are, as was said, the rule prohibiting the use of force and the rule prohibiting intervention.⁶⁵ The former protects the territorial integrity of a State (an element

⁵⁸ UNGA Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (Oct. 24, 1970); Charter of the Organization of American States art. 17, Apr. 30, 1948, 2 U.S.T. 2394, 119 U.N.T.S. 3, art 25.

⁵⁹ *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania)* [1949] ICJ Rep 35, 36.

⁶⁰ *Nicaragua* (n 15) para 251.

⁶¹ *Certain Activities Carried out by Nicaragua in the Border Area (Costa Rica v Nicaragua)* and *Construction of a Road in Costa Rica Along the San Juan River (Nicaragua v Costa Rica)*, 16 December 2015, ICJ Reports 2015, para 229.

⁶² *Nicaragua* (n 15) paras 202, 205.

⁶³ *Delimitation of Maritime Boundary in Gulf of Maine Area (Canada v US)* [1984] ICJ Rep 246, para 79.

⁶⁴ France speaks of 'international norms and principles that flow from State sovereignty'; *Droit International Appliqué aux Opérations dans le Cyberspace* (n 7) 1.1.1.

⁶⁵ Montevideo Convention (n 18) art 8; United Nations, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, Article 2 (4); *Nicaragua* (n 15) paras 202, 204–205; *Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of the Congo v Uganda)* (Jurisdiction and Admissibility) [2006] ICJ Rep 6, paras 46–48. For a discussion of the non-use of force principle see Rossini (Ch 14 of this Handbook) and for non-intervention see Kilovaty (Ch 5 of this Handbook).

protected by sovereignty) from external aggression, whereas the latter protects the political authority of the State (again an element protected by sovereignty) from external coercion. Because these rules derive from and are linked to sovereignty, I call them 'sovereignist' rules. The emergence of such rules does not however extinguish the principle of sovereignty because its scope is broader than these rules. Instead, sovereignty stands as the background, residual and independent legal principle protecting a State's sovereign rights beyond those protected by any specific rule.

In relation to cyberspace and with the exception of the UK, States that have expressed their views publicly support the view that sovereignty is a stand-alone legal principle that produces legal consequences. For example, Finland has categorically declared that it 'sees sovereignty as a primary rule of international law, a breach of which amounts to an internationally wrongful act and triggers State responsibility'.⁶⁶ Likewise, France has affirmed that State sovereignty applies to cyberspace and that cyber operations can violate the principles of sovereignty, non-intervention or the prohibition of the threat or use of force.⁶⁷ In the same vein, Iran declared that 'the sovereignty of states is not an extra-legal matter'.⁶⁸ The Netherlands declared that 'respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act'.⁶⁹ In Estonia's view 'Sovereignty entails not only rights, but also obligations. States are responsible for their internationally wrongful cyber operations just as they would be responsible for any other activity based on international treaties or customary international law'.⁷⁰ China stated that 'no infringement of sovereignty in cyberspace will be tolerated'.⁷¹ As the victim of a cyber-attack in 2019, Georgia issued a statement condemning the cyber-attack, 'which goes against international norms and principles, once again infringing Georgia's sovereignty'.⁷²

As far as the USA is concerned, its views are quite nuanced. For example, according to the DOD General Counsel 'it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law' but continues by saying that lawyers should 'take into account the principle of State sovereignty' and that 'States have sovereignty over the information and communications technology infrastructure within their territory'.⁷³

From this, it transpires that the main point of contention is not whether sovereignty is legally consequential but what is its scope and content.

In determining its scope and content, it is important to recall what was said previously namely, that sovereignty denotes exclusive and supreme power over territory and people and

⁶⁶ *International law and cyberspace: Finland's national position* (n 7).

⁶⁷ *Droit International Appliqué aux Opérations dans le Cyberspace* (n 7) 1.1 and 1.1.1. For similar views by OAS member States see n 7.

⁶⁸ Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace (July 2020) <https://www.aldiplomasy.com/en/?p=20901>.

⁶⁹ Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace Appendix: International law in cyberspace (n 7).

⁷⁰ Estonia (n 7).

⁷¹ International Strategy of Cooperation on Cyberspace (n 46).

⁷² Statement of the Ministry of Foreign Affairs of Georgia 20 February 2020 available at: [https://mfa.gov.ge/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-\(7\).aspx?CatID=5](https://mfa.gov.ge/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5).

⁷³ DOD General Counsel Remarks at US Cyber Command (n 54); Egan (n 7).

that it represents the aggregation of rights and duties a State holds as a State and vis-à-vis other States. Thus any non-consensual or not legally justified interference within a State's sovereign legal sphere will constitute violation of its sovereignty.⁷⁴ For example, any unauthorised or not legally justified cyber operation on another State's cyber infrastructure which does not reach the level of violence required by the rule on the non-use of force or the level of coercion required by the non-intervention rule will violate the latter State's sovereignty. Otherwise, sovereignty will be denied full legal meaning if its scope and content is to be reduced to those rights protected by the non-use of force and non-intervention rule.⁷⁵ Such a view will also create legal and, consequently, responsibility gaps which can be exploited by States.

On the basis of the above it can be said that the Sony attack which involved the hacking and leaking of data from a private company seated in the USA constitutes a violation of US sovereignty because it involved unauthorised entry into US sovereign domain as does the 2019 attack on Georgia which targeted governmental websites and websites of financial institutions, academia and NGOs in Georgia. Likewise, cyber-attacks on hospitals treating COVID-19 patients or information gain operations against R&D facilities in the UK or other States amount to violation of the respective States sovereignty.⁷⁶ In contrast, the taking down of the Redatup botnet in 2019 does not violate the principle of sovereignty because the C&C servers that were replaced by French police were situated in France, even if most of the infected computers were outside France. Cyber espionage can also violate a State's sovereignty because it involves operations on foreign networks and indeed operations that exfiltrate or compromise data held in a foreign State's cyber infrastructure without the latter's consent notwithstanding the absence of a specific rule proscribing cyber espionage during peace-time.⁷⁷

An issue that deserves further consideration is whether, in order to constitute a breach of the principle of sovereignty, a cyber operation should reach a certain threshold or produce certain effects. The Tallinn Manual, for instance, mentions certain factors to be taken into account such as death, injury, physical damage, loss of functionality and also speaks of infringements falling below the threshold of loss of functionality.⁷⁸ However, it does not indicate the required degree of damage or infringement because they can be quite limited. The Tallinn Manual also mentions 'interference with or usurpation of inherently governmental functions of another State' as another factor to be taken into account but again this refers to the nature of the infringement and not to the degree of infringement. In any case, it should be noted that sovereignty and sovereign rights are not only about governmental functions.

In my opinion, any unauthorised or not legally justified operation that interferes with a State's sovereign rights violates the principle of sovereignty regardless of the degree of interference or damage and regardless of whether it produces physical or non-physical effects

⁷⁴ *International law and cyberspace: Finland's national position* (n 7) 2–3.

⁷⁵ See *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1996] ICJ Rep 226, 393–4 (Dissenting Opinion of Judge Shahabuddeen).

⁷⁶ NCSC, 'UK and allies expose Russian attacks on coronavirus vaccine development' (16 July 2020) <https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development>.

⁷⁷ See the chapters on cyber espionage by Buchan and Navarrete (Ch 11 of this Handbook) and the use of force by Roscini (Ch 14 of this Handbook). See also Russell Buchan, *Cyber Espionage and International Law* (Hart 2018) 48–69.

⁷⁸ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 17–20. See also Moynihan (n 54) paras 51–4.

or whether the operation targets governmental services and infrastructure or not.⁷⁹ The harm in this case is normative; it is the harm to the principle of sovereignty and the rights protected by it. It is interesting in this regard to recall France's view that '[a]ny cyberattack against French digital systems or any effects produced on French territory by digital means ... constitutes a breach of sovereignty'. France defines cyber-attack as any 'deliberate, offensive and malicious action taken via cyberspace that is intended to cause damage (in terms of availability, integrity or confidentiality) to information or the systems that process it and that may harm the activities of which it or they are the medium'.⁸⁰ For France, the principle of sovereignty is violated not only when there are effects but also when there is interference with its information systems since it 'exercises its sovereignty over the information systems located on its territory'.⁸¹ Finland has also taken the same view when it considers as violation of sovereignty '... a non-consensual intrusion in the computer networks and systems that rely on the cyber infrastructure in another State's territory' as well as 'an unauthorized intrusion by cyber means ... if it interferes with data or services that are necessary for the exercise of inherently governmental function'.⁸²

One could say however that, without any *de minimis* threshold, the principle of sovereignty is trivialised or that the possibility of conflict increases. In response, it can be said that having a *de minimis* threshold does not comport with the importance attached to the principle of sovereignty and with the fact that States may construct their sovereignty differently; some States may adopt an all-inclusive definition covering political, legal, economic, social, cultural aspects, whereas other States may adopt a less inclusive definition of sovereignty. States may also ascribe different degrees of importance to the different values and rights protected by sovereignty. As to whether the absence of any threshold can lead to more conflicts, it can be said that the danger of conflict is more serious if States reject the legal import of the principle of sovereignty and instead interpret the rule on the non-use of force and non-intervention expansively.

What transpires from the above is that the content and scope of the principle of sovereignty cannot be fixed *ab initio* other than in relation to certain core sovereign elements. Consequently, determinations as to whether the principle of sovereignty has been violated should take place on a case by case basis by taking into consideration qualitative and quantitative criteria. This is in fact a common trait of all legal principles namely, that their content and how they apply to a set of facts or situations or legal regimes require interpretation and contextualisation.

Finally, in response to the claim that there is no relevant State practice to support the argument that cyber operations can breach the principle of sovereignty, it should be recalled that States' official pronouncements on the legal status of sovereignty in cyberspace constitute relevant practice and *opinio juris*. It should also be noted that whether a State claims that its sovereignty has been violated is a complex question not only because there is no automatic and independent invocation of illegality in international law but also because a lot depends on

⁷⁹ See also *International law and cyberspace: Finland's national position* (n 7) 2 ('The situation is the same irrespective of whether such infrastructure belongs to or is operated by governmental institutions, private entities or private individuals').

⁸⁰ *Droit International Appliqué aux Opérations dans le Cyberspace* (n 7) 1.1.1.

⁸¹ *Ibid.* 6.

⁸² *International law and cyberspace: Finland's national position* (n 7) 2.

a State's technical capacity to attribute the impugned operation to another State as well as its political will to invoke another State's responsibility. This means that drawing inferences from State practice or silence needs to be more nuanced.

In order to conclude, this section made two main points: first, that sovereignty is a legal principle that applies to cyberspace and produces legal consequences; and, second, that unauthorised interference with a State's sovereign rights in cyberspace constitutes a breach of its sovereignty although such assessments can be made on a case by case basis because the content, scope and application of sovereignty as a principle require interpretation and contextualisation.

5. CYBERSPACE: A SOVEREIGN ENTITY?

In Sections 3 and 4 I examined the question of whether the principle of sovereignty can apply to cyberspace and whether it is legally consequential which I answered in the affirmative. In this section I will examine the question of whether cyberspace itself can be sovereign. The a-territorial and borderless nature of cyberspace may immediately provoke a negative response but, as was said previously, territory is a legal and political construct which is not synonymous with sovereignty. Furthermore, territory is also a social construct; it is about the relationships between humans, activities and spaces and about attachments and allegiances. Also, territory and, more generally, space, is a perception, a cognitive construction.⁸³ Cyberspace can thus be described as 'the sense of space generated within the mind as we interact with computer technology' and 'the sense of space generated by the computer-user interface, through one or a combination of our senses'.⁸⁴ In this respect, it is quite instructive to recall that William Gibson coined the term 'cyberspace' by watching a video game that appeared to cause kids and computer users 'to develop a belief that there is some kind of actual space behind the screen, some place you cannot see but you know is there'.⁸⁵ In light of the above, one can say that cyberspace, in addition to its physical, social and logical dimension, it is also a noumenal space 'inhabited' and 'experienced' through machines and virtual interactions by people who are located in real spaces and use physical instruments.⁸⁶ These people are the 'netizens' who make up the cyber community.

The question that can immediately be asked is whether 'netizens' can exercise their right to self-determination and declare the sovereignty of cyberspace. In fact, that was what the *Declaration of the Independence of Cyberspace* called for. This may be a possibility in view of the fact that the 'people' who are the subject of the right to self-determination and the institution of the State are distinct entities and also in view of the fact that sovereignty, at least according to contemporary democratic theories, is vested in the people who, on the basis of the

⁸³ Cohen (n 8) 213.

⁸⁴ Lance Strate, 'The varieties of cyberspace: Problems in definition and delimitation' (1999) 63 *Western Journal of Communication* 382, 412.

⁸⁵ Sue Barnes, 'Cyberspace: Creating paradoxes for the ecology of self' in Lance Strate, Ronald L Jacobson and Stephanie B Gibson (eds), *Communication and Cyberspace* (Hampton Press 1996) 195.

⁸⁶ Cohen (n 8) 236.

right to self-determination, have a say in the internal organisation and external representation of the space within which they live.⁸⁷

Whether this is probable in cyberspace and whether such a declaration will have any legal significance or consequences is, however, doubted. In the first place, questions can be asked as to whether 'netizens' constitute a 'people' for self-determination purposes. Although there is no universally accepted definition of the term 'people' in international law, the cyberspace community does not fit any of the different articulations of the term that have been used. For example, a UNESCO report spells out a number of characteristics 'inherent in a description (but not a definition) of a people' which refer to: a common historical tradition; racial or ethnic identity; cultural homogeneity; linguistic unity; religious or ideological affinity; territorial connection; common economic life. The report also notes that 'the group must be of a certain number', that the 'group as a whole must have the will to be identified as a people or the consciousness of being a people' and that the group must have 'institutions or other means of expressing its common characteristics and will for identity'.⁸⁸ It immediately becomes apparent that 'netizens' do not satisfy any of the aforementioned indicators such as language, ethnicity and so on but it is their manifestation in the real world that is projected in cyberspace. This also raises the question of how 'netizens' can be differentiated from other communities in order to claim sovereignty. Furthermore, cyber membership is infinite and too heterogeneous to translate into strong consciousness of people-hood beyond certain common interests. Also, the cyber community is broader than the 'netizens'; it is a multi-stakeholder community. However, who are all the stakeholders and what is their stake on the community and on cyberspace are open questions. For instance, tech companies who own and operate cyber infrastructure are part of the cyber community but their interests vary greatly from those of other 'netizens'. Including them in the definition of 'denizens' means that the cyber community will be defined by power differentials at its source which is contrary to the idea of 'people' comprising equal participants.

Even if we move away from such essentialist descriptions of 'people-hood' and consider how the term 'people' has been defined in the post-1945 practice of self-determination, 'netizens' still fall outside such definitions. The 'people' who exercised the right to self-determination and formed their own independent States were those living under colonial rule⁸⁹ but 'netizens' cannot claim that they 'inhabit' a territory or a space that is under foreign subjugation or domination. Furthermore, self-determination claims were made and fought on behalf of 'peoples' by groups or individuals who were able to mobilise them and who enjoyed legitimacy, but who among the cyber community can act as a legitimate leader? Moreover,

⁸⁷ See arts 1(2) and 55 of the UN Charter; art 1 of the International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, 171 (ICCPR) and International Covenant on Economic, Social and Cultural Rights, 16 December 1966, United Nations, Treaty Series, vol. 993, 3 (ICESCR).

⁸⁸ UNESCO 'International Meeting of Experts on further study of the concept of the rights of peoples' (22 February 1990) SHS-89/CONF.602/7 para 22; <https://unesdoc.unesco.org/ark:/48223/pf0000085152>.

⁸⁹ Declaration on the Granting of Independence to Colonial Countries and People (14 December 1960) UNGA Res 1514 (XV). See also principle 1 and 5 of the Declaration on Principles of International Law concerning Friendly Relations and cooperation among States in accordance with the Charter of the United Nations, UNGA Res 2625 (XXV) of 24 October 1970. *Case Concerning the Frontier Dispute (Burkina Faso/Republic of Mali)*, 22 December 1986, ICJ Reports 1986, paras 24–25.

who among 'netizens' can rise above their particularistic interests to fight for the political emancipation of cyberspace as a whole?

Finally, if the 'people' who make up the 'netizens' are artificial persons, they are programmed by real persons and lack the generalised intelligence and fully autonomous mind needed for self-awareness, consciousness, deep logic and independent decisions.⁹⁰ This means that their claim to self-determination is not fully self-guided but mediated by real humans.

If 'external' self-determination is not possible, can the cyberspace community instead claim internal self-determination? This refers to the post-colonial articulation of the right to self-determination whereby ethnic, religious, linguistic or other groups are granted some form of autonomy and self-rule, albeit within the State.⁹¹ One can say that the 'cyber exceptionalism' thesis mentioned above according to which cyberspace is subject to regulation by its users alludes to this. Yet, said self-regulation is more about private governance than about self-rule and autonomy. Furthermore, there are no claims to autonomy by cyber groups and even offline groups that enjoy the right to internal self-determination have not claimed autonomy in cyberspace.

There are many other reasons why a declaration of sovereignty by 'netizens' is improbable. First, 'netizens' do not suddenly lose their physicality or become displaced figures; they are embodied individuals who live in real spaces which are under State sovereignty. Consequently, any decision to proclaim the sovereignty of cyberspace and any 'laws' or regulations they may promulgate will be subject to scrutiny by the laws of their own State. In fact, such declaration will immediately be declared null and void by States which will use their powers to arrest, try and imprison those individuals. Even if they use encryption, they cannot keep the State out. Secondly, it is the institutional and legal structure of the State that will eventually support cyberspace sovereignty because cyberspace does not have any central authority to promulgate and enforce laws. Put in other words, cyberspace is intermediated by the State and therefore it cannot be sovereign. Thirdly, in relation to the question of whether the cyber community forms a polity where sovereignty can reside, there is no shared feeling among its members that they constitute a political unit based on collective identity and a sense of common destiny upon which the sovereignty of cyberspace can rest. Although 'netizens' may have the consciousness of being cyber users and may share certain common interests, their membership or interactions do not translate into any overriding political, social, legal, or ethical association. Even if cyberspace offers an open and easily accessible public space where questions about common destiny and association can be deliberated and reflected upon, the sheer volume of users and languages and the lack of structures according to which such deliberations can take place and decisions can be made, negate that possibility. In fact, members of the cyber community associate themselves and place their allegiances with their own States and people. The State, even for the cyber community, remains the most legitimate and effective institution to serve human needs, provide protection and secure justice; and remains the only space where popular sovereignty and self-determination can be realised.⁹²

⁹⁰ Of course technology advances and may create such artificial persons emulating human beings but again the question is to what extent they are separated from their creators.

⁹¹ *Reference re Secession of Quebec* [1998] 2 S.C.R. 217.

⁹² '[T]he concept of sovereignty satisfies a deep-seated need to protect a society's political identity and self-determination and that this keeps it alive'; Dieter Grimm, *Sovereignty: The Origin and Future of a Political and Legal Concept* (Columbia University Press 2015) 9.

If cyberspace cannot become sovereign because it does not have its own ‘people’ or polity and does not have its own mechanisms to declare and sustain a claim to sovereignty but all these are intermediated by States and their polities, the immediate question is whether States can attribute sovereignty to cyberspace.

States as the original subjects of international law enjoying full sovereign power can create other entities and delegate their powers but this does not mean that they forfeit their sovereignty. Consequently, even if States were to recognise cyberspace as a separate political entity and endow it with organs and governmental powers such as legislative or judicial powers over issues that hitherto belonged to them, this will not make cyberspace a sovereign entity. As in the case of international organisations, cyberspace will remain circumscribed by State sovereignty.

An issue I will discuss now is whether big tech companies such as Apple, Microsoft, Google or Facebook are in fact sovereign. Often the language used by big tech companies invokes State symbolisms. For example, Brad Smith, the President of Microsoft, said that the tech sector should operate as a neutral digital Switzerland, that ‘cyberspace is us’, and that ‘instead of nation-state attacks being met by responses from other nation-states, they are being met by us’.⁹³ Another example is the Cybersecurity Tech Accord adopted by tech companies from around the world where they make a number of pledges in order to defend and advance the benefits of the online technologies for society, among which is the pledge to protect users and customers – whether an individual, organisation or government – from cyber-attacks.⁹⁴ Above all, it is their power to regulate through their own norms human, social, political, cultural life; enforce their norms through their own institutions and processes; and provide security, a quintessential State function, that makes them State-like entities. Julie Cohen for example opines that such companies are sovereign:⁹⁵ they have territories defined by protocols, data flows, and algorithms; they have populations, their users, over whom they exercise authority and power; they practice diplomacy; and they are important participants in the global legal order.⁹⁶ This is true to a large extent but it is more about the power of tech companies, financial and otherwise, and about their influence which is a genuine concern for democracies and for the rule of law. However, such power does not make them sovereign in the sense of having full and ultimate

⁹³ Brad Smith, ‘The need for a Digital Geneva Convention’ (14 February 2017) <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>; Brad Smith, ‘Keynote Address at the RSA Conference 2017: The Need for a Digital Geneva Convention’ (14 February 2017) 12, <https://blogs.microsoft.com/wp-content/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf>.

⁹⁴ See <https://cybertechaccord.org/>.

⁹⁵ Julie E Cohen, Law for the Platform Economy (2017) 51 *U.C. Davis Law Review* 133, 199–203; Anupam Chander, ‘Facebookistan’ (2012) 90 *North Carolina Law Review* 1807, 1808.

⁹⁶ This includes e.g., meetings between governments and CEOs and other managers. Also, Denmark has appointed a Tech Ambassador who engages in techplomacy. According to the Office of Denmark’s Tech Ambassador:

[t]here are two overall aspects in the operationalization of Techplomacy: (i) Like all other embassies we bring forward concerns or questions on behalf of Danish authorities in a direct and frank dialogue with the tech companies in order to try and influence the direction of technology and our own preparedness. (ii) Influence the international agenda around tech policy questions in accordance with Danish interests and values, including through new alliances, multilateral fora, and multi-stakeholder partnerships.

<https://techamb.um.dk/en/>.

power as States do; neither is there any transfer of allegiance from States to tech companies.⁹⁷ Tech companies are subject to the sovereignty of the State where they operate or are seated and, actually, we are witnessing the gradual curbing of their powers and their subjection to more intense and wide-ranging regulation and scrutiny through legislation, penalties, and judicial enforcement. In short, States assert their sovereignty over tech companies and this is even more evident in authoritarian States.

In order to summarise, it was claimed that cyberspace cannot become sovereign because it lacks the human substratum and autochthonous mechanisms needed to establish and support its sovereignty but instead it is intermediated by States. Also, even if States were to recognise cyberspace as a distinct legal-political entity, this does not make it sovereign. Finally, big tech companies are not sovereign but subject to State sovereignty. That said, I will now discuss a different legal representation of sovereignty in cyberspace.

6. CYBERSPACE AS GLOBAL COMMONS

Cyberspace has sometimes been characterised as a global commons, a *res communis*.⁹⁸ The founder of the World Wide Web, for example, dedicated the protocol to the whole world, preventing anyone from attaining property over it.⁹⁹ Also, according to the 2017 US National Security Strategy ‘the United States will provide leadership and technology to shape and govern common domains—space, cyberspace, air, and maritime—within the framework of international law’.¹⁰⁰

The global commons concept in international law concerns the type and scope of authority exercised over spaces or, to put it differently, how spaces are governed. Global commons describe resource domains that lie outside States’ exclusive sovereignty and are subject to collective use.¹⁰¹

⁹⁷ For example Mark Zuckerberg, Facebook’s CEO, envisages ‘creating a large-scale democratic process to determine standards with AI to help enforce them’; *Building Global Community* (18 February 2017) <https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10103508221158471/>. However, previous attempts at direct democracy were unsuccessful; Adi Robertson, ‘Mark Zuckerberg wants to democratize Facebook—here’s what happened when he tried’, *The Verge* (5 April 2018) <https://www.theverge.com/2018/4/5/17176834/mark-zuckerberg-facebook-democracy-governance-vote-failure>.

⁹⁸ Dan Hunter, ‘Cyberspace as place and the tragedy of the digital anticommons’ (2003) 91 *California Law Review* 439; Abraham M Denmark and James Mulvenon (eds), *Contested Commons: The Future of American Power in a Multipolar World* (Centre for New American Century 2010).

⁹⁹ Tim Berners-Lee and Mark Fischetti, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web* (Texere 2000) 124.

¹⁰⁰ *National Security Strategy of the United States* (December 2017) 41, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>; National Cyber Security Strategy: Canada’s Vision for Security and Prosperity in the Digital Age (2018) 34, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtrg-ntnl-cbr-scrtrg-en.pdf>; Mark Barrett *et al.*, *Assured Access to the Global Commons* (North Atlantic Treaty Organisation 2011) xii, http://www.alex11.org/wp-content/uploads/2013/01/aagc_finalreport_text.pdf.

¹⁰¹ UNEP, ‘IEG of the Global Commons: Background’ (United Nations Environment Programme Division of Environmental Law and Conventions) <http://www.unep.org/delc/GlobalCommons/tabid/54404/Default.aspx>; John Vogler, ‘Global Commons Revisited’ (2012) 3 *Global Policy* 61; Mika

The modern concept of global commons has its roots in Roman Law. Roman Law was broadly divided into the law that pertains to persons and the law that pertains to objects (*res*). The latter included both corporeal and incorporeal objects and the law that applied to them depended on their nature and function. Whereas *res in patrimonio* were subject to ownership, *res extra patrimonium* were divided into objects that were subject to divine law and objects that were subject to human law. The latter were further divided into *res communes* (belonging to all mankind); *res publicae* (belonging to a State for use of its citizens); and *res universatis* (belonging to a city for use of its citizens).¹⁰²

Early international lawyers used these Roman Law concepts to describe the legal status and regulation of certain spaces. Grotius characterised the high seas as *res communis* because ‘... it is so limitless that it cannot become a possession of anyone, and because it is adopted for the use of all, whether considered from the point of view of navigation or of fisheries’. For him, if water is enclosed, it can be subject to possession.¹⁰³ In the same vein, Vattel treated the high seas as global commons not subject to appropriation in contrast to areas near the coasts which can be susceptible to ownership.¹⁰⁴

The modern instantiation of the global commons concept can be found in Article 2 of the Geneva High Seas Convention (1958) and in Articles 87, 89 and 139 of the 1982 United Nations Convention on the Law of the Sea concerning the high seas;¹⁰⁵ in the 1966 Outer Space Treaty in relation to outer space;¹⁰⁶ and in the Antarctic Treaty System which deals with issues of sovereignty and use in Antarctica and defines global commons as ‘south of 60 [degrees] South Latitude, including all ice shelves’.¹⁰⁷

From the spaces designated as global commons it transpires that global commons share certain characteristics which contribute to their legal designation as global commons and their subjection to a system of collective governance in order to enjoy the accrued benefit. They include the accumulated resources of these areas; the indivisibility of assets; the benefits that their exploitation would deliver to each and every State; and the difficulties in apportioning them due to their size and to the fact that their boundaries are not clearly demarcated.

It also transpires that the designation of a space as global commons is not a legal inevitability but depends on broadly defined political considerations that are represented in the legal

Aaltola, Joonas Sipilä and Valtteri Vuorisalo, ‘Securing global commons: a small state perspective’ (FIIA Working Paper 71, June 2011).

¹⁰² Max Radin, ‘Fundamental concepts of the Roman Law’ (1925) 13 *California Law Review* 207; George Mousourakis, *Fundamentals of Roman Private Law* (Springer 2012) 119–21.

¹⁰³ Hugo Grotius, *The Freedom of the Seas, or, the Rights which Belongs to the Dutch to take part in the East Indian Trade* (edited by James B Scott, OUP 1916) 28. See further Hugo Grotius, *The Classics of International Law: De Jure Belli Ac Pacis Libri Tres: Vol. II Book II* (translated by Francis W Kelsey et al, Clarendon/Carnegie Endowment for International Peace 1925) Ch II para III.

¹⁰⁴ Emer Vattel, *Le Droit Des Gens ou Principes de la Loi Naturelle, appliques à la Conduite et aux Affaires des Nations et des Souverains* (Liberty Fund 2008) Ch XXIII, 125–7.

¹⁰⁵ United Nations Convention on the Law of the Sea (signed 10 December 1982, entered into force 16 November 1994).

¹⁰⁶ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (19 December 1966) arts 1, 2, 7, 8.

¹⁰⁷ *The Antarctic Treaty* (signed 1 December 1959, entered into force 23 June 1963) Articles IV, V and VI. It can be said however that Antarctica is not a global commons *stricto sensu*. See Silja Vöneky and Sange Addison-Agyei, ‘Antarctica’ in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (2011) para 19.

concept of global commons. States can still extend their authority over the designated area if they wish but, for the reason explained above, States agree to refrain from claiming ownership over that area and agree to exercise their authority concurrently with that of other States. For this reason, they devise a common regulatory regime to fulfil the designation of the referent area as global commons.

This indicates that the global commons concept is a legal-political construct which is not adverse to the principle of sovereignty. When States decide to designate a certain area as global commons and, consequently, agree to abstain from exercising their full sovereignty over such an area, this is an act of sovereign authority. Auto-limitation is an expression of sovereignty. As the PCIJ said in the *S.S. Wimbledon* case: 'The Court declines to see, in the conclusion of any treaty by which a State undertakes to perform or refrain from performing a particular act, an abandonment of its sovereignty ... the right of entering into international engagements is an attribute of State sovereignty.'¹⁰⁸

All this means that cyberspace can in principle be designated a global commons if States agree to do so and subsequently design the rules and principles to govern that area. However, at this point in time, there is no political or legal impetus to do so and whether such impetus will emerge depends on many variables – political, legal, social, cultural – but the underlying question is whether cyberspace warrants to be so designated if compared to existing global commons. In this regard it should be noted that, although cyberspace exhibits some of the characteristics of global commons, for example borderless, there are also important differences between cyberspace and other global commons. First, whereas global commons refer to natural resources and have a physical dimension, cyberspace is a technical, man-made, resource domain which also has a virtual dimension. Second, global commons have outward physical and geographical boundaries which delineate the space, however, this is not the case in cyberspace where its virtual part permeates all boundaries whereas its physical part in the sense of infrastructure and humans falls within State boundaries. Third, whereas global commons are created in order to avoid depletion of natural resources, this is not the case in cyberspace where resources cannot be depleted naturally but expanded or depleted technically.¹⁰⁹ Fourth, whereas global commons are non-excludable in the sense that others cannot be excluded, the extent that cyber infrastructure belongs to States means that others can be excluded as was mentioned above. Finally, the physical part of cyberspace, such as computers, is under national jurisdiction and in most cases it is privately owned which means that it should be 'de-owned' in order for cyberspace to form a global commons but this would be legally difficult. It is for these reasons that cyberspace was at best described as an 'imperfect commons'.¹¹⁰

¹⁰⁸ *S.S. 'Wimbledon'* (Judgment of 17 August 1923) [1923] PCIJ Rep Series A No 1, 25.

¹⁰⁹ This relates to Hardin's 'tragedy of the commons'; see Garrett Hardin, 'The tragedy of the commons' (1968) 162 *Science* 1243.

¹¹⁰ Joseph S Nye, *The Future of Power* (Public Affairs Press 2011) 143; James A Lewis, 'Sovereignty and the role of government in cyberspace' (2010) 16 *Brown Journal of World Affairs* 55, 62.

7. CONCLUDING THOUGHTS

It has become apparent from the preceding discussion that cyberspace has not acquired any special legal status in international law but, instead, existing legal categories and principles such as the principle of sovereignty have been applied to cyberspace and are used to explain its legal status. The chapter has also shown that the principle of sovereignty is not only a stand-alone legal principle but also that it produces legal consequences. In other words, there is definitely a sovereignty redux in cyberspace. This does not however mean that there are no disputes about its scope and content or that no further clarifications are needed. But this is what principles require; they require interpretation and contextualisation.

One may ask why sovereignty, which as was said is the engine behind the creation of international law, has not produced a global and comprehensive regulatory regime for cyberspace. In response, it should be said that law-production is not an inevitable outcome of sovereignty because sovereignty can also thwart the international law-production process. Yet, if States' sovereign interests and needs begin to coalesce around certain issues, sovereignty can generate new law.¹¹¹ Although this seems to be unattainable at this point in time, the principle of sovereignty applies and will continue to apply in cyberspace shaping and rationalising State behaviour and the international rules that apply or will apply in the future to cyberspace.

¹¹¹ Nicholas Tsagourias, 'The slow process of normativizing cyberspace' (2019) 113 *American Journal of International Law Unbound* 71.