1. The legal status of cyberspace

Nicholas Tsagourias

INTRODUCTION

Cyberspace is often presented as a purely non-legal domain. According to John Barlow's *Declaration of the Independence of Cyberspace* 'legal concepts do not apply to cyberspace'.[1] This 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.[2]

The second assumption is that cyberspace, true to its original conceptualisation and design, should remain an open, decentralised and participatory space, not hampered by legal regulations.[3]

Yet, the view that cyberspace is subject to law and indeed to international law is not in dispute anymore.

For example, a report of the United Nations Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security affirmed that international law, especially the United Nations (UN) Charter, applies to cyberspace and that State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities[4], and to jurisdiction over ICT infrastructure within a State's territory.[5] 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'.[6]

This view is often supplemented by a qualification: namely, that international law should adapt its rules in order to grapple with the particularities of cyberspace. As the US President opined in the 2011 International Strategy for Cyberspace:

---

[1] John P Barlow, 'A Declaration of Independence for Cyberspace' (Davos, 1996) <https://projects.eff.org/~barlow/Declaration-Final.html> accessed 22 July 2014.

[2] David R Johnson and David G Post, 'Law and borders: The rise of law in cyberspace' (1996) 48 *Stanford L Rev* 1367. *Contra* Jack L Goldsmith, 'Against cyberanarchy' (1998) 65 *U Chi L Rev* 1199.

[3] Tim Wu and Jack Goldsmith, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006) 23.

[4] Information and Communication Technology.

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

[6] Ibid., 4.

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.[7]

It is important to note at this juncture that the question as to whether cyberspace is subject to law is a deeply political question. Cyberspace, as any technology in general, is not an abstract entity that exists in isolation from politics but, instead, as the debates mentioned above attest, is subject to political debates. Such debates may eventually lead to common understandings about its ontology or use which are then normativised in the form of legal rules. Law thus constructs the ontology and function of cyberspace by embedding in the legal norms that apply to cyberspace authoritative choices about the nature and use of cyberspace whilst at the same time it moulds such choices through its own principles and standards. In other words, law serves a normative as well as a performative function.

Yet, even if now is widely accepted that cyberspace is subject to law or indeed to international law, scholars and practitioners usually focus on how international rules apply to cyberspace and to cyber activities with relatively little consideration being given to the legal status of cyberspace. This is therefore the main focus of this chapter. Before exploring that question however, an enquiry into 'what is cyberspace' is necessary.

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. For example, Koepsell, in his book on the ontology of cyberspace, set himself the task of answering the following questions:

> What is cyberspace? Is it dimensional? Are there things in cyberspace? Are things in cyberspace properly called objects? Are such objects, or cyberspace itself, substance or process? Is cyberspace or the objects in it real or ideal? What is the categorical scheme of cyberspace? How should cyberspace fit into a broader categorical scheme?[8]

---

[7] The White House, 'International Strategy for Cyberspace' (May 2011) 9 <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> accessed at 23 July 2014; Harold H Koh, 'International Law in Cyberspace' (*U.S. Department of State*, USCYBERCOM Inter-Agency Legal Conference, 18 September 2012) <http://www. state.gov/s/l/releases/remarks/197924.htm> accessed 25 February 2014.

[8] David Koepsell, *The Ontology of Cyberspace: Law, Philosophy, and the Future of Intellectual Property* (Open Court Publishing 2003) 10. Julie Cohen spoke of the representations of cyberspace as 'utopia' that is, as a separate space; as 'isotopia' that is, as a space that continues existing space and as 'heterotopia' as a space where ordinary rules of behaviour or conduct are suspended or transformed. Heterotopia preserves its relational aspect which, with

I will not engage here with the various debates concerning the ontology of cyberspace due to lack of expertise, but I will offer a basic description of cyberspace in order to grasp the object of enquiry and because it is its features and attributes that shape the way law understands and consequently treats cyberspace.

Cyberspace has been defined as 'a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'[9]. Although this is not the most exact definition of cyberspace as it does not mention, at least explicitly, software programmes, yet it is a starting point because it identifies certain common traits that most academic or institutional definitions of cyberspace contain. A more comprehensive definition is that offered by Kuehl according to which 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*'.[10]

It transpires from the above that cyberspace has three layers: a physical layer which consists of computers, integrated circuits, cables, communications infrastructure and the like; a second layer which consists of the software logic; and, finally, a third layer which consists of data packets and electronics.[11]

What also transpires is that, whereas the core of cyberspace may form a virtual space, it is nonetheless supported by physical objects such as computers, which connect the irreducible part of cyberspace to the physical world;[12] and interactions in cyberspace are independent of time or space constraints and are conducted through logistics rather than through physical acts.[13]

Having provided a basic decription of cyberspace and of its features, in the remainder of the chapter I will focus on the legal representation of cyberspace and more specifically on its status in international law.

For international lawyers, their conception of cyberspace is influenced by their understanding of how spaces are represented in international law. For this reason, they

---

regard to cyberspace, refers to its connection to 'real' space. Julie E Cohen, 'Cyberspace as/and space' (2007) 107 *Columbia L Rev* 210.

[9] US Department of Defense, 'Department of Defense Dictionary of Military and Associated Terms', Joint Publication 1-02 (8 November 2010, as amended through 15 March 2014), 64; II.9. See also 'The UK Cyber Security Strategy Protecting and promoting the UK in a digital world' (2011) 11 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> accessed 11 October 2014.

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

[11] Lior Tobanksy, 'Basic concepts in cyber warfare' (2011) 3(1) *Military and Strategic Affairs* 75, 77–78.

[12] Rebecca Bryant, 'What kind of space is cyberspace?' (2001) 5 *Minerva – An Internet J of Philosophy* 138.

[13] Lawrence Lessig, 'The path of cyberlaw' (1995) 104(7) *Yale L J* 1743, 1745–6; William S Byassee, 'Jurisdiction of cyberspace: Applying real world precedent to the virtual community' (1995) 30 *Wake Forest L Rev* 197, 207–8.

not only look for analogies with physical spaces but also apply certain fundamental international law principles such as that of sovereignty to cyberspace pondering at the same time on how this principle applies in cyberspace and how it models its status.

Cyberspace and Sovereignty

I will now explore the question of whether the principle of sovereignty applies to cyberspace and, if it does, what are the implications for the status of cyberspace. These are important questions because sovereignty is a fundamental principle of international law; it is in fact the basic organising principle of international law.[14] In its traditional definition, sovereignty denotes *summa potestas*.[15] It denotes authority and control which in legal terms is translated as the power to promulgate laws and the power to enforce these laws.[16]

The two pertinent questions to ask then with regard to cyberspace are, first, whether cyberspace can be subject to sovereignty and, secondly, whether cyberspace can itself be sovereign.

Regarding the first question, there are those that maintain that cyberspace should be free from sovereignty. According to Johnson and Post, for example, cyberspace cannot be subject to sovereignty but instead, cyberspace should be subject to its own distinct system of legal regulation based on self-regulation.[17] For them, it is not only the borderless and a-territorial nature of cyberspace that make it adverse to the standard systems of territorially based international legal regulation 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.[18] 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 of the need to have an effective regulatory system appropriate to cyberspace that cyberspace should develop its own legal system based on self-regulation.[19] All in all, the no-sovereignty thesis is based on a concept of cyber-exceptionalism.

The descriptive and normative premises of the no-sovereignty thesis have been challenged by Jack Goldsmith in his article 'Against cyberanarchy'. For him, the jurisdictional and enforcement inadequacies of sovereign power in cyberspace identified by Johnson and Post have been exaggerated. In fact, sovereigns can regulate the local effects of extraterritorial activities.[20] Moreover, traditional legal tools can resolve

---

[14] Alan James, *Sovereign Statehood* (Allen & Unwin 1986) 267–9.

[15] Samantha Besson, 'Sovereignty' in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (OUP 2012).

[16] 'In short, authority concerns rule-making and control, rule-enforcement.' Janice E Thomson, 'State sovereignty in international relations: Bridging the gap between theory and empirical research' (1995) 39 *Intl Studies Quarterly* 213, 223.

[17] Johnson and Post (n 2).

[18] Ibid., 1370–76.

[19] Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006) 3.

[20] Goldsmith (n 2).

the multi-jurisdictional problems implicated in cyberspace and thus overcome issues of legitimacy and validity.

Yet, whether cyberspace can be subject to sovereignty depends on how the concept of sovereignty is understood and used in legal discourse.

As was said, sovereignty refers to supreme and full authority and in international law it connotes authority and power over a certain territory and over its people to the exclusion of any other authority. In the words of Judge Alvarez, by sovereignty 'we understand 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'.[21] What transpires from the above is that in international law sovereignty has a strong territorial dimension.[22] The territorial dimension of sovereignty is 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. As Judge Humber said in the *Isle of Palmas* case 'territorial sovereignty serves to divide between nations the space upon which human activities are employed'.[23]

By elevating territory and the polity attached to that territory into components of sovereignty,[24] sovereignty became bounded. To explain, whereas sovereignty as *summa potestas* is unbounded, territory localises sovereignty and acts as the 'constraint that unravels the assertion of unconstrained sovereignty'.[25] In other words, territory has become not only the object but also the container of sovereignty by drawing its legal and political borders.

It follows from the above that whereas internal sovereignty, that is sovereignty over a territory, is in principle full and exclusive, external sovereignty is relative.[26] External sovereignty denotes power over externalities but, because all sovereigns are equal and

---

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

[22] Jens Bartelson, *A Geneology 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).

[23] *Island of Palmas Case (or Miangas)* (*United States v Netherlands*) [1928] Reports of International Arbitral Awards 839.

[24] 'The state is the land, the people, the organization of coercion and a majestic idea, each supporting and even defining the other, so that they [become] indivisible.' Nicholas G Onuf, 'Sovereignty: Outline of a conceptual history' (1991) 16(4) *Alternatives: Global, Local, Political* 425, 437.

[25] Joel P Trachtman, 'Cyberspace, sovereignty, jurisdiction and modernism' (1998) 5(2) *Indiana JGLS* 560, 567. 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.

[26] Stephen D Krasner, *Sovereignty: Organized Hypocrisy* (Princeton University Press 1999) 1–42.

have an equal claim to external sovereignty, the exercise of sovereign power outside the allocated territory by one of them will encroach on the sovereignty of the others. Thus, external manifestations of sovereignty are coordinated and managed through consent. Consent is a sovereign act of voluntary acquiescence. As the Permanent Court of International Justice opined in the *Lotus case* 'international law governs the relations between independent States. The rules of law binding upon States … emanate from their own free will'.[27]

That having been said, it is important to disentangle sovereignty as a concept from territory. Territory as an element of sovereignty is a lego-political construct: it is 'about organising space for political [or legal] purposes'.[28] With that I mean that the carving of territories upon which sovereignty is exercised is a political act; it is the end result of a political process involving claims, counterclaims and successful assertions of power. The Peace of Westphalia, for example, which is treated as the foundation of the modern territorially-bound sovereignty was in fact about the redrawing of political boundaries.[29] Thus, there is no inherent nexus between territory and sovereignty, although territory offers a tangible space where sovereignty can manifest itself effectively in political and legal terms. As was observed, 'state territory can be regarded as a container of power and not just as a place where powers are located'.[30] Moreover, even the territorially-based concept of sovereignty has an element of abstraction. As Ford observed, territory 'is abstractly and homogeneously conceived' which means that 'the space of a jurisdiction is conceived of independently of any specific attribute of that space' and '[o]ne consequence of this abstract presentation of space is that it eliminates the need for the specific enumeration and classification by kind'.[31]

If the essence of sovereignty is power and not territory, it can extend not only beyond any allocated territory but also to non-territorial entities. Whether this will happen or how this will happen, is a completely different question. Moreover, sovereignty as a concept is not monolithic, but a 'sponge concept'[32] that can manifest itself in different forms.

These observations can assist us in answering the question of whether sovereignty can be asserted in cyberspace which, as was said, has a physical as well as a virtual component and where activities may defy space or time constraints but nonetheless have real effects on spaces, humans, or institutions. In this regard and since the focus of this chapter is law and in particular international law, we should speak of jurisdiction.[33] Jurisdiction is a concomitant of sovereignty and in fact it is the legal instantiation of

---

[27] *The Case of the S.S. "Lotus"* (Judgement) [1927] PCIJ Rep Series A No 10 18.

[28] Thomas Forseberg, 'Beyond sovereignty, within territoriality: Mapping the space of late-modern (geo) politics' (1996) 31(4) *Cooperation and Conflict* 355, 362; John G Ruggie, 'Territoriality and beyond: Problematising modernity in international relations' (1993) 47 *Intl Organization,* 139.

[29] Daniel Bethlehem, 'The end of geography: The changing nature of the international system and the challenge to international law' (2014) 25(1) *EJIL* 9, 13.

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

[31] Richard T Ford, 'A history of jurisdiction' (1999) 97 *Michigan L Rev* 843, 853–4.

[32] Bartelson (n 22) 237.

[33] For jurisdiction in cyberspace see Kohl (Ch 2 of this book).

sovereignty.[34] Jurisdiction refers to legal authority and power and as an ingredient of sovereignty translates sovereign power into prescription, enforcement and adjudication.[35] Through jurisdiction sovereignty becomes operational and is substantiated. Being attendant on sovereignty, jurisdiction has an internal as well as an external aspect. Internally, 'jurisdiction extends (and is limited) to everybody and everything within the sovereign's territory and to his nationals wherever they may be' and externally '[l]aws extend so far as, but no further than the sovereignty of the State which puts them into force'.[36]

With regard to cyberspace, a State can exercise jurisdiction over cyber infrastructure located on its territory and over its nationals[37] when engaged in cyber activities. It can also do so over non-nationals located in its territory.[38] A State can exercise jurisdiction over information circulated through cyberspace at the point of delivery as well as the point of reception or when the information crosses through wires and lines falling within its jurisdiction.[39] A State can exercise jurisdiction over web addresses to the extent they are registered in a specific country. In sum, the State can exercise its prescriptive and enforcement jurisdiction over cyberspace and over cyber activities on the basis of nationality and territoriality.

Yet, territoriality and nationality as bases of jurisdiction can be interpreted quite extensively and expand even further the scope of a State's jurisdiction and thus sovereignty. More specifically, a State may exercise jurisdiction over its nationals regardless of where their acts have been committed. This refers to the active nationality principle and in cyberspace it means that if a national of a certain State commits a wrongful cyber act in a foreign jurisdiction, for example a cybercrime, her/his State of nationality may still exercise jurisdiction over her/him.

Moreover, a State can extend its jurisdiction extraterritorially if one of its nationals has been the victim of a wrongful act. This refers to the passive nationality principle which has been asserted by certain States in particular with regard to terrorism.[40] For example, if nationals of a particular State have been victims of cyber terrorism which has been committed by non-nationals from a foreign jurisdiction, this can trigger the jurisdiction of the victims' State of nationality.

---

[34] 'Jurisdiction is an aspect or an ingredient or a consequence of sovereignty,' James Crawford, *Brownlie's Principles of Public International Law* (8th edn, OUP 2012) 456–7.

[35] Michael Akehurst, 'Jurisdiction in International law' (1972) 46 (145) *BYIL* 9197 15. And *Wedding v Meyler*, 192 U.S. 573 (84 1904).

[36] Frederick A Mann, 'The doctrine of international jurisdiction revisited after twenty years' in Academie De Droit International De La Haye, *Recueil Des Cours 1984* (Martinus Nijhoff Publishers 1984) 9.

[37] *Nottenbohm Case (Lichtenstein v Guatemala)* [1955] ICJ Rep 4 23.

[38] *T-Mobile West Corp. v Crow*, No. CV08-1337-PHX-NVW, (D. Ariz. Dec. 16, 2009) 15–16); *CompuServe, Inc v Patterson* 89 F. 3d 1257 (6th Cir.1996); *The Case of the S.S. "Lotus"* (Dissenting Opinion by Judge Moore) [1927] PCIJ Rep Series A No 10.

[39] *R v Sheppard & Amor* [2010] EWCA Crim 65; Sean Kanuck, 'Sovereign discourse on cyber conflict under international law' (2010) 88(7) *Tex L Rev* 1571, 1573–5.

[40] *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.

A State may also exercise its jurisdiction when a certain cyber activity has effects within that State's territory.[41] The effects doctrine was first enunciated by the Permanent Court of International Justice in the *Lotus* case[42] and has now been accepted as a jurisdictional ground applicable in many different areas of law[43] although there are differing views about its scope. The controversy revolves around a number of issues, for example whether the effects should have already been felt; whether they should be substantial; whether they should be detrimental or whether foreseeable effects[44] would also suffice in order to trigger a State's jurisdiction. A problem with applying the effects doctrine to cyberspace is that effects may have been felt in a number of different jurisdictions. If all affected States were to assert jurisdiction, the practical difficulties become more than evident. 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 avoid jurisdictional overlaps and preserve jurisdictional fairness, the threshold for the effects doctrine has been raised from 'certain minimum contacts'[45] to substantial contacts.[46] Moreover, the principle of targeting has been developed, according to which it is the State targeted by the impugned behaviour that can exercise jurisdiction irrespective of any effects felt in other jurisdictions.[47] As was said, targeting is 'something more than effects, but less than physical presence'.[48]

A State can also assert its jurisdiction over activities that endanger important national interests regardless of where, or by whom, they have been committed.[49] This refers to the protective head of jurisdiction.[50] A State for example can exercise jurisdiction over cyber espionage if its security has been compromised.

In addition to the aforementioned bases for exercising jurisdiction, it is also important to mention at this juncture the indirect exercise of jurisdiction over cyberspace. States or private actors may partition cyberspace territorially by regulating access to cyberspace on the basis of geolocation or by blocking websites. Secondly, a

---

41 For the effects doctrine see also Kohl (Ch 2 of this book).

42 *The Case of the S.S. "Lotus"* (n 27) 23.

43 *Arrest Warrant of 11 April 2000* (n 40) para 47.

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

45 *International Shoe Co v Washington* 326 US 310 [1945].

46 *CompuServe v Patterson* (n 38):

> This court has repeatedly employed three criteria to make this determination: First, the defendant must purposefully avail himself of the privilege of acting in the forum state or causing a consequence in the forum state. Second, the cause of action must arise from the defendant's activities there. Finally, the acts of the defendant or consequences caused by the defendant must have a substantial enough connection with the forum to make the exercise of jurisdiction over the defendant reasonable.

See also *Zippo Mfg Co v Zippo Dot Com Inc* 952 F Supp 1119 (WD Pa 1997).

47 Thomas Schultz, 'Carving up the Internet: Jurisdiction, legal orders, and the private/public international law interface' (2008) 19(4) *EJIL* 799, 816.

48 Ibid., 817.

49 *The Case of the S.S. "Lotus"* (n 27) (Dissenting opinion by Judge Loder) [1927] PCIJ Rep Series A No 10 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.'

50 Cedric Ryngaert, *Jurisdiction in International Law* (OUP 2008) 96.

State can assert jurisdiction over cyberspace by regulating cyberspace technology. As was said, 'the actor who reigns over the architecture of technology also defines the rights and constraints existing within this architecture'.[51] A state can do this by regulating the functions and activities of software or by imposing conditions such as passwords. Thirdly, the assertion of jurisdiction by one State may have 'spill over' effects on other jurisdictions or on areas outside any jurisdiction, for example on the virtual domain of cyberspace. For instance, if a State regulates access to terrorist materials, it makes their circulation through cyberspace more difficult in the absence of a common regulatory regime, although eventually not impossible.[52]

This leads to the question of whether a State can exert jurisdiction over objects or activities in the virtual part of cyberspace. If sovereignty connotes authority and power and is not inherently territorial, nothing prevents a State from exercising its jurisdiction unilaterally or in cooperation with other States over objects or activities in the virtual domain since they do not fall within any specific jurisdiction. This is based on the permissive rule introduced by the Permanent Court of International Justice (PCIJ) in the *Lotus* case according to which, in the absence of a prohibition, a State is free to assert its jurisdiction 'its title to exercise jurisdiction rests in its sovereignty'.[53] That said, whether a State will be able to actually exercise jurisdiction depends on its technological capabilities.

What we observe then with regard to cyberspace is, on the one hand, the territorialisation of cyberspace and of cyber activities and on the other, the de-territorialisation of sovereignty.[54] With territorialisation I do not mean the territorial carving of cyberspace or its treatment as tangible territory but the extension to cyberspace and to cyber activities of configurations of authority and power linked to territorial spaces. This process links cyberspace to the traditional notion of sovereignty and, in fact, reinforces State sovereignty. On the other hand, we observe the deter-ritorialisation of sovereignty as far as cyberspace is concerned. Deterritorialisation has been defined as 'the detachment of regulatory authority from a specific territory'.[55] This has two aspects. The first is about the diverse norm-setting authorities, sources of normativity and plurality of norm addressees.[56] In cyberspace rules and regulations are laid down by States but also by a variety of public and private authorities whereas the addressees of such rules and regulations are equally States and other legal or natural persons. For example ICANN (Internet Corporation for Assigned Names and Numbers)

---

[51] Christoph B Graber, 'Internet Creativity, Communicative Freedom and a Constitutional Rights Theory Response to "Code is Law"' (i-call Working paper no. 03, University of Lucerne 2010) 5 <http://ssrn.com/abstract=1737630> accessed 28 June 2014.

[52] Goldsmith (n 2), 1240–42.

[53] *The Case of the S.S. "Lotus"* (n 27) 19.

[54] These terms have been used albeit differently in Geoffrey L Herrera, 'Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space' (1st International CISS/ETH Conference on "The Information Revolution and the Changing Face of International Relations and Security" Lucerne, Switzerland, May 23–25, 2005) 30.

[55] Catherine Brölmann, 'Deterritorializing international law: Moving away from the divide between national and international law' in Janne E Nijman and André Nollkaemper (eds), *New Perspectives on the Divide between National and International Law* (OUP 2007) 84–109.

[56] Ibid.

is a 'not-for-profit public-benefit corporation' incorporated in the USA being responsible for assigning Internet namespaces and for keeping the Internet secure, stable and interoperable. As it declares on its website ICANN, 'bring[s] together individuals, industry, non-commercial and government representatives to discuss, debate and develop policies about the technical coordination of the Internet's Domain Name System'.[57] The other aspect of de-territorialisation of sovereignty concerns the State itself and finds expression in the extraterritorial exercise of jurisdiction. When the State exercises its jurisdiction with regard to cyber activities extraterritorially, its locus of jurisdiction is not the sovereign territory.

Having examined the question of whether cyberspace can be the locus of sovereignty, the next question is whether cyberspace itself can be a sovereign entity.[58] The a-territorial nature of cyberspace may provoke some reservations but, as was said previously, territory is not necessarily integral to the concept of sovereignty. Moreover, territory is not just a geographical notion with political and legal connotations but it is also a social construct and a perception. Territory is about the relationships between humans, actions and spaces as well as about attachments and allegiances to spaces. To this it should be added that space is a cognitive construction. As Cohen argued '[t]o say that humans reason spatially is not to say that we are place-bound, or property-bound, but simply to say that we are embodied, situated beings, who comprehend even disembodied communications through the filter of embodied, situated experience'.[59]

Following from this, one can say that cyberspace has, in addition to its physical infrastructure and to its human users, a conceptual and a perceptual dimension as well. Conceptually, cyberspace is 'the sense of space generated within the mind as we interact with computer technology', and perceptually it is 'the sense of space generated by the computer-user interface, through one or a combination of our senses.'[60] Interestingly, William Gibson coined the term 'cyberspace' by watching video game kids and computer users who seemed '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'.[61] One may thus describe cyberspace as a 'figurative' or 'noumental' space 'inhabited' and 'experienced' through machines by people who are located in real spaces.[62]

The question that can be asked then is whether these people or the cyberspace community at large can declare the sovereignty of cyberspace. Put differently, can the

---

[57] https://www.icann.org/.

[58] Timothy S Wu, 'Cyberspace sovereignty? The Internet and the international system' (1997) 10(3) *Harvard J of L & Technology* 648.

[59] Cohen (n 8) 213 .

[60] Lance Strate, 'The varieties of cyberspace: Problems in definition and delimitation' (1999) 63(3) *Western J of Communication* 382, 412.

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

[62] According to Julie Cohen cyberspace 'is constituted via the interactions between and among practice, conceptualisation, and representation. It is a nexus of social practice by embodied human beings; a site for the enactment of visions of the ideal organisation of social and economic activity; and a catalyst for impressionistic re-imaginings of socio-spatial practice'. Cohen (n 8) 236.

cyberspace community in exercising its right to self-determination determine the political and legal status of cyberspace as a sovereign entity? Indeed, that was the gist of the famous *Declaration of the Independence of Cyberspace*.

It should be noted in this respect that at the basis of the principle of self-determination is the notion that people have a say in the internal organisation and the external representation of the space within which they live and that people entitled to self-determination and States are distinct entities.[63] It should also be recalled that sovereignty in its political journey was separated from the person of the sovereign and according to current democratic theories of sovereignty, the source and holder of sovereignty are the people who can exercise their right to self-determination through democratic process.

Such a constitutive act by the cyber community even if it were to happen would be devoid of any legal as well as practical significance. First, there are questions as to whether the cyberspace community constitutes a 'people' for self-determination purposes. In international law there is no universally accepted definition of the term 'people'[64] but a UNESCO report mentioned a number of characteristics which are 'inherent in a description (but not a definition) of a people'. They include: a common historical tradition; racial or ethnic identity; cultural homogeneity; linguistic unity; religious or ideological affinity; territorial connection; common economic life. The Report also noted 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'.[65] If we apply these characteristics to the cyber community, it does not satisfy any of the above criteria. Also, the cyber community cannot be defined as a group of people because membership of the cyber community is infinite. Furthermore, membership of cyberspace does not translate itself into forging strong normative ties beyond certain agreement on rules of behaviour. Nor is there a shared feeling among users of constituting a unit based on collective identity and a sense of common destiny.[66] Granted, users may have the consciousness of being cyberspace users and they may share some common interests but their interaction does not translate itself into any overriding political, social, legal, or ethical association. Although cyberspace in principle 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 or languages and the lack of structures make the possibility of such deliberation difficult. For most part, cyberspace users associate themselves and place their allegiances with their own States and people.

---

[63] See Article 1 of the ICCPR and ICESCR. 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.

[64] Rupert Emerson, Self-determination' (1971) 65 *AJIL* 459, 462.

[65] 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 <http://unesdoc.unesco.org/images/0008/000851/085152eo.pdf> accessed 11 October 2014.

[66] Dieter Grimm, 'Does Europe need a constitution?' (1995) 1 *European L J* 282.

Secondly, the inhabitants of cyberspace are embodied individuals who live in real spaces. Cyberspace users even as inhabitants of that figurative space do not suddenly lose physicality or become displaced figures. They live in real geographic and time spaces and are under the jurisdiction of their respective States. Any decision to proclaim the sovereignty of cyberspace and any laws or regulations they may promulgate will be subject to the scrutiny of their own State.

Thirdly, even if they declare the sovereignty of cyberspace, the normative, institutional, or legal structure needed to support sovereignty in cyberspace cannot be independent of State structures. Cyberspace does not have any central authority to promulgate or enforce laws. Instead it is the laws of real spaces that are projected in cyberspace.

It transpires then that cyberspace does not have its own 'people' or its own independent and self-generating mechanisms to declare and sustain a claim to internal as well as external sovereignty.

That being the case, the next question is whether sovereignty can be attributed to cyberspace by States. States as the original subjects of international law with plenary sovereign powers can create other entities and attribute them with certain powers. They can do so as far as cyberspace is concerned but it will not make it a sovereign entity even if, in the process, it expands its powers. In international law, the only depositories of sovereignty are the States. Their creations may be attributed with powers over issues that hitherto belonged to States, however they do not have plenary sovereign powers and any attributed powers can be recalled.

From the preceding discussion it can be concluded that cyberspace can never become sovereign but can be subject to sovereignty. I have already explained how States can assert their sovereignty in cyberspace but in what follows I will also discuss a different legal representation of sovereignty in cyberspace.

CYBERSPACE AS GLOBAL COMMONS

Often cyberspace is identified as a global commons or a *res communis*.[67] The founder of the World Wide Web for example dedicated the protocol to the whole world, preventing anyone from attaining property over it.[68]

Global commons are resource domains that lie outside the exclusive sovereignty of States.[69] Global commons share certain broad characteristics. First, their utility as a

---

[67] Dan Hunter, 'Cyberspace as place and the tragedy of the digital anticommons' (2003) 91 *California L Rev* 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); *Canada's Cybersecurity Strategy: For a stronger and more prosperous Canada* (Government of Canada 2010) 4 <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx> accessed 28 July 2014.

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

[69] 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> accessed 28 July 2014; John Vogler, 'Global

whole is greater than if broken down into smaller parts; second**,** States and non-state actors with the requisite technological capabilities are able to access and use them for economic, political, scientific and cultural purposes; and third**,** in most cases they are governed collectively.[70]

International law has recognised a number of global commons such as the High Seas, Antarctica and the Outer Space,[71] which have been characterised as the 'cyberspaces' of a previous generation.[72]

With regard to the high seas, the *mare liberum* principle was first promulgated by Grotius as reaction to the prevalent at the time theory of enclosed sea (*mare clausum*). Grotius compared the sea with the air in the following terms:

> the air belongs to this class of things [*res communis*] for two reasons: First it is not susceptible of occupation; and secondly its common use is designed for all mankind. For the same reasons the sea is common to all, 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.[73]

In another passage he said:

> the sea … cannot become subject to private ownership. The extent of the ocean is in fact so great that it suffices for any possible use on the part of all peoples … the same thing would need to be said, too, about the air. There is, furthermore, a natural reason which forbids that the sea, considered from the point of view mentioned, should become a private possession. The reason is that occupation takes place in the case of a thing which has definite limits.[74]

In contrast, if water is enclosed, it can be possessed as in the case of lakes.[75]

Commons revisited' (2012) 3(1) *Global Policy*, 61; Mika Aaltola, Joonas Sipilä and Valtteri Vuorisalo, 'Securing Global Commons: A small state perspective' (FIIA Working Paper 71, June 2011).

[70] Denmark and Mulvenon (eds) (n 67) 11.

[71] United Nations Convention on the Law of the Sea (signed 10 December 1982, entered into force 16 November 1994) art 157(1); The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (signed 18 December 1979, entered into force 11 July 1984) art 11(7)(d); Tara Murphy, 'Security challenges in the 21st century global commons' (2010) 5(2) *Yale J of Intl Affairs* 28.

[72] United Nations Environment Programme (n 57); Paul S Berman, 'The globalisation of jurisdiction' (2002) 151(2) *U of Pennsylvania L Rev* 311, 494.

[73] 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.

[74] 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

[75] Ibid., Ch III, VIII.

It becomes thus apparent that Grotius' designation of the high seas as global commons was premised on the nature of the seas and on its public utility accompanied by generous doses of natural law theory and by Grotius' political support of free trade.[76]

This principle has been confirmed in Article 2 of the Geneva High Seas Convention (1958) as well as in Articles 87 and 89 of United Nations Convention on the Law of the Sea. According to that Convention, 'no State may validly purport to subject any part of the high seas to its sovereignty' and 'no State shall claim or exercise sovereignty or sovereign rights over any part' of the seabed and ocean floor and subsoil thereof, beyond the limits of national jurisdiction.'[77]

As far as the Outer Space is concerned, it 'is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means'.[78] The Outer Space Treaty lays down a number of fundamental principles for the exploitation and use of outer space by recognising outer space as a 'province of all mankind'.[79] More specifically, nations can only use the moon and other celestial bodies for peaceful purposes, including scientific research, and should not launch any nuclear weapon or other weapon of mass destruction into orbit.

The legal status of Antarctica is more complex. A number of States – Australia, Argentina, Chile, France, New Zealand, Norway and the UK – have made conflicting claims to parts of Antarctica.[80] With the introduction of the Antarctica Treaty System, States 'agreed to disagree' over territorial claims[81] and compromised on the issue of sovereignty over parts of Antarctica.[82] According to the Antarctic Treaty '[n]o new claim, or enlargement of an existing claim, to territorial sovereignty in Antarctica shall be asserted while the treaty is in force'.[83] Moreover, nations can only use the Antarctic for peaceful purposes, including scientific research, and should not test nuclear weapons or dispose nuclear waste in the Antarctica.[84] The Antarctic Treaty also

---

[76] Mireille Hildebrandt, 'Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace', (2013) 63 *U of Toronto L J* 196, 210–16; Nico Schrijver and Vid Prislan, 'From Mare Liberum to the Global Commons: Building on the Grotian Heritage' (2009) 30(1) *Grotiana* 168, 173.

[77] United Nations Convention on the Law of the Sea (n 71) art 89, 139.

[78] 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) art 2.

[79] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (n 78) arts 1, 2, 7, 8; Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (n 71) art 4(1). See also UNGA Res 1962 (XVIII) (13 December 1963).

[80] Elizabeth K Hook, 'Criminal jurisdiction in Antarctica' (1978) 33 *U of Miami L Rev* (1978) 489.

[81] *The Antarctic Treaty* (signed 1 December 1959, entered into force 23 June 1963) art IV; Jill Grob, 'Antarctica's frozen territorial claims: A meltdown proposal' (2007) 30 *Boston College Intl & Comparative L Rev* 461, 468.

[82] Rolph Trolle-Anderson, 'The Antarctic scene: Legal and political facts' in Gillian D Tiggs (ed), *The Antarctic Treaty Regime* (CUP 2009) 57.

[83] The Antarctic Treaty (n 81) art 4(2).

[84] Ibid., art 5.

defines global commons as 'south of 60 [degrees] South Latitude, including all ice shelves'.[85]

One may say that Antarctica is not a global commons *stricto sensu* but an international commons in that a number of States enjoy certain rights over Antarctica.[86]

In a world of sovereignty, the concept of global commons appears to be an anomaly. The idea however persists in legal and political thinking. Why this is so, can be explained by the fact that it does not contradict basic international legal and political principles such as the principle of sovereignty. If sovereignty connotes authority and power, the *res communis* concept concerns the type and scope of authority and power that is exercised over certain objects.

This will become evident if we recall the categorisation of objects in Roman law from which the *res communis* concept derives. Roman law is broadly divided into the law that pertains to persons and the law that pertains to objects (*res*). In Roman law *res* included both corporeal and incorporeal objects and the law pertaining to objects concerned the type of power that can be exercised over them in view of their nature and function.[87] More specifically, *res in patrimonio* were subject to ownership whereas *res extra patrimonium* were divided into those subject to divine law and those subject to human law but cannot be privately owned.

Those subject to human law 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.[88]

Applying the Roman law analogies but also historical analogies to cyberspace it transpires that cyberspace even as a virtual space can be subject to law and that it exhibits some of the characteristics of those objects that have been designated *res communis* in Roman law. A historical account of the development of the *res communis* concept going back to Grotius also reveals that the designation of certain areas such as the sea or the air as *res communis* was due to the accumulated resources of these areas; the indivisibility of assets and 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.

The designation of an area as *res communis* does not mean that States cannot extend their authority over the designated area or that these areas are not subject to law; what it means is that States agree to refrain from claiming ownership over that area, accept that they will exercise their authority concurrently with that of other States and devise a common regulatory regime to fulfil its designation of global commons. As was seen, most of the current areas designated as *res communis* are subject to treaty regimes, the product of State consent, which define the rights and obligations of States over such areas. This shows that the *res communis* or global commons concept is a lego-political

---

[85] Ibid., art 6.

[86] Silja Vöneky and Sange Addison-Agyei, 'Antarctica' in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Max Planck Institute for Comparative Public Law and International Law 2011) para 19. Susan J Buck, 'The global commons: An introduction' (Island Press 1998) 6.

[87] Max Radin, 'Fundamental concepts of the Roman law' (1925) 13 *California L Rev* 207.

[88] George Mousourakis, *Fundamentals of Roman Private Law* (Springer 2012) 119–21.

construct[89] which is not adverse to the principle of sovereignty. When States decide to designate a certain area as *res communis* and consequently agree to abstain from exercising their full sovereign power over such an areas is an act of sovereign authority. Auto-limitation is an expression of sovereignty. As the PCIS 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'.[90]

In order for cyberspace to be designated a global commons, States should consent and agree on the rules and principles that will govern that area. At this point in time, there is no political or legal impetus to designate cyberspace a legal commons and whether such impetus develops depends on many variables crucial among which is whether cyberspace warrants to be so designated if compared to existing ones.

That said, it should be noted that there are differences between cyberspace and other global commons. First, whereas global commons refer to natural resources, cyberspace is a technical man-made resource domain. Second, whereas global commons have some physical and geographical boundaries, this is not the case in cyberspace where its virtual part permeates all 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.[91] Fourth, whereas global commons are non-excludable in the sense that others cannot be excluded, to the extent that cyber infrastructure belongs to States means that others can be excluded. Finally, the physical part of cyberspace such a computers and the like is nationally owned which means that they should be 'de-owned' or that what will fall under the global commons domain will be the 'un-owned' part of cyberspace. Still, questions remain as to how this would affect the owned part of cyberspace due to the interconnectedness of cyberspace.

It is for this reason that it has been claimed that cyberspace is an 'imperfect commons'.[92]

CONCLUDING THOUGHTS

It is apparent from the preceding discussion that cyberspace has not acquired any special legal status in international law but instead existing legal categories and principles have been applied to cyberspace. By doing so, a *non liquet* has been avoided; a finding that is of a substantive or interpretative gap in international law.

Yet if cyberspace is a domain that offers possibilities but also contains risks and dangers, a regulatory system based on common values, principles and rules of conduct is needed to foster cooperation and good citizenship in cyberspace. This may require a comprehensive and globally negotiated treaty to establish rules of behaviour and

---

89 Garrett Hardin, 'The tragedy of the commons' (1968) 3859 *Science* 1243.
90 *S.S. 'Wimbledon'* (Jugement of 17 August 1923) [1923] PCIJ Rep Series A No 1 25.
91 This relates to Hardin's 'tragedy of the commons'. Hardin (n 89); Trachtman (n 25).
92 Joseph S Nye, *The Future of Power* (PublicAffairs 2011) 143.

conduct, outlaw certain behaviours and provide rules on jurisdiction.[93] Yet agreement on a comprehensive legal framework for cyberspace faces huge challenges.

To mention just a few, certain characteristics of cyberspace such as anonymisation; place shifting; and rapid technological development make any legal regulation immediately inadequate or even redundant. Secondly, the technological disparities that exist between States as well as between States and non-state actors, such as big enterprises, affect participants' choices and preferences of legal regulation or as to whether legal regulation is needed at all. For example, because cyberspace as a growing environment offers capabilities and opportunities, States or private actors may not want to limit their future opportunities. Thirdly, cyberspace is used by governments and individuals for different purposes therefore consensus and compromise is difficult to achieve. Fourth, because of the nature and use of cyberspace, any agreement needs to involve governments but also public and private sector bodies, a combination of stakeholders that international law is not always capable of managing.

So the outlook for such a comprehensive regime is not auspicious. Instead existing international rules and principles will continue to apply to cyberspace followed by calls for responsible behaviour by States or non-state actors. Undoubtedly, international law shapes State behaviours and interests in cyberspace and perhaps rationalises them but it rarely pre-empts legislation.

[93] Ahmad Kamal, *The Law of Cyber-Space: An invitation to the table of negotiations* (United Nations Institute of Training and Research 2005) 1–4 <http://www.un.int/kamal/thelawofcyberspace/The%20Law%20of%20Cyber-Space.pdf> accessed 29 July 2014.