Indonesian Journal of International Law

Volume 15
Number 4 *Boundary Affairs III*

Article 5

7-31-2018

Law, Borders and the Territorialisation of Cyberspace

Nicholas Tsaugourias
University of Sheffield, United Kingdom, nicholas.tsagourias@sheffield.ac.uk

Indonesian Journal of International Law (2018), Vol. 15 No. 4, pp. 523 - 551
http://dx.doi.org/10.17304/ijil.vol15.4.738

LAW, BORDERS AND THE TERRITORIALISATION OF CYBERSPACE

Nicholas Tsaugourias*

* University of Sheffield, United Kingdom
Correspondence: Nicholas.Tsagourias@sheffield.ac.uk

Abstract

This article explores the relationship between law and more specifically international law with territory and borders and how this relationship manifests itself in cyberspace. It claims that it manifests itself through two processes: a process of territorialisation of cyberspace that is, the application of territorial notions of international law to persons, activities, and objects existing or operating in or through cyberspace and, secondly, in States asserting their sovereignty in cyberspace by creating national cyberspace zones. All in all, its main claim is that borders are still relevant in the legal regulation of cyberspace.

Keywords: *borders, territory, state sovereignty, international law, cyberspace, cyber zones*

Submitted : 09 October 2017 | Revised : 25 January 2018 | Accepted : 24 March 2018

I. INTRODUCTION

Law and borders –geographic or normative - have an intimate relationship. One may even say that they share some form of a causal relationship. On the one hand, a law produces and determines borders whereas, on the other, borders produce and determine laws. The relationship between law and borders is even more pronounced in international law where borders and indeed territorial borders play a constitutive as well as a functional role in international law. First, borders are constitutive of states and, consequently, they are constitutive of international law. To explain, states are territorially bounded entities; they represent exclusive authority over a discrete patch of territory. International law is the product of interactions between such bounded authorities. Borders thus define international law's source of authority; without states, there would be no international law. Second, borders play a functional role by demarcating international law to wit, by separating international law from domestic law. They determine in other words what lies inside and becomes the subject of domestic law and what lies outside and becomes the subject of international law. Borders are also functional in that they demarcate international law's different domains, for example, international criminal law, environmental law and so on.

The application of each domain depends on criteria and conditions laid down by international law. In this sense, one can speak of normative borders rather than physical ones. All these show that borders shape our conception of international law and of the regulatory frameworks that apply to international phenomena.

This paper will explain the relationship between borders and international law in cyberspace and its implications for the legal governance of cyberspace. This is an important endeavour because cyberspace and its features of a-territoriality and borderlessness seem to defy traditional notions of international legal regulation. The question then of whether international law can act as a regulatory tool in cyberspace and, if it does, what is the scope of its regulatory competence and the question of whether states can remain the source of regulation in cyberspace are closely linked to the question of whether the constitutive and functional role of borders can be replicated in cyberspace. The latter question lies behind the debates on cyber regulation and will be tackled in this article.

The article will thus proceed by elucidating in the second section the relationship between international law, borders, territory, and statehood. The third section will throw a critical gaze on the existing debates concerning the place and role of international law in cyberspace. The fourth section will examine the phenomenon of territorialisation of cyberspace and its implications for the application of international law to cyberspace whereas the fifth section will examine the phenomenon of realigning sovereignty and cyberspace. It is hoped that by understanding the relationship between international law, borders, and sovereignty, this will assist us in understanding how legal governance in cyberspace emerges and is shaped.

II. INTERNATIONAL LAW, BORDERS, TERRITORY, AND STATES

A cursory look at any international law textbook reveals the relationship between international law and states. International law is traditionally defined as the law that regulates the relations between states as sovereign formations. According to Vattel "[t]he law of nations

is the law of sovereigns"[1] and according to a contemporary textbook "[p]ublic international law covers relations between states in all their myriad forms …"[2] This immediately raises the question of what is a state and what is the relationship between states, borders, and territory in international law.

The 1933 Montevideo Convention on the Rights and Duties of States[3] provides a definition of 'state' by identifying its constitutive elements. According to Article 1 of the Convention, "the State as a person of international law should possess the following qualifications: (1) a permanent population; (2) a defined territory; (3) government; and (4) capacity to enter into relations with other states."

Notwithstanding any criticism of under-inclusiveness leveled against this definition, it has acquired customary law status[4] not only because it codified views already existing at the time of its adoption but also because, since its adoption, it has been confirmed on many occasions in international jurisprudence. For example, as early as 1929, it was opined in the *Deutsche Continental Gas-Gesellschaft arbitration that "[a] State does not exist unless it fulfills the conditions of possessing a territory, a people inhabiting that territory, and a public power which is exercised over the people and the territory."*[5] More recently, the Arbitration Commission of the European Conference on Yugoslavia[6]

---

[1] Emer de Vattel, *Le Droit Des Gens ou Principes de la Loi Naturelle, appliques à la Conduite et aux Affaires des Nations et des Souverains*, [*The Law of Nations, or, Principles of the Law of Nature Applied to the Conduct and Affairs of Nations and Sovereigns*] translated by Charles G. Fenwick, Carnegie Institution of Washington, 1916), in Classics of International Law, para xvi. [hereafter referred to as DdG]

[2] Malcom N. Shaw, *International Law*, 5th ed., CUP, 2003, p. 2.

[3] The Montevideo Convention on Rights and Duties of States, signed on 26 December 1933, 165 LNTS 19 (entered into force 26 December 1934) art. 1; James Crawford, *The Creation of States in International Law*, 2nd ed., Clarendon Press, 2006; James Crawford, *The Criteria for Statehood in International Law*, British Yearbook of International Law, vol. 48, 1977, p. 93-182.

[4] *Restatement (Third) of Foreign Relations Law of the United States*, American Law Institute, 1987, § 201.

[5] Deutsche Continental Gas-Gesellshaft v. Polish State (Germano-Polish Mixed Arbitral Tribunal) 1 August 1929, 5 ILR 11, p. 14-15.

[6] Arbitration Commission of the Peace Conference on Yugoslavia, *Opinion No. 1*, reprinted in Alain Pellet, "The Opinions of the Badinter Arbitration Committee a Second Breath for the Self-Determination of Peoples", *EJIL* vol 1, no. 3, 1992, p. 182.

opined that "the state is commonly defined as a community which consists of a territory and a population subject to an organised political authority and that such a state is characterised by sovereignty".

The requirement of defined territory in Article 1 of the Convention alludes to borders. Defined territory means demarcated territory that is, discrete territory separated from other territories. [7] If this element in the Montevideo definition of states is combined with the element of government, territory represents the container over which an authority exercises supreme and exclusive power[8] demarcate the geographic, personal and functional scope of such power and distinguish said territory from other territories over which different authorities exercise exclusive power. Put slightly differently, the territory is the substratum of state authority whereas borders define the allocation of authority between states. As Allen Buchanan put it "territory [means] the area that is circumscribed by boundaries of political units. Land is a geographical concept; the territory is political and, more specifically, a judicial concept."[9] The total, supreme and exclusive power over such territory is called sovereignty. The state as an institution thus embodies a claim of sovereignty over certain territory.[10] In the words of Judge Humber in

[7] Although borders need not be precisely defined as for states to emerge, there needs to be, at least, a continuous and defined portion of territory over which power is exercised. As the ICJ held in the *North Seas Continental Shelf* cases: "The appurtenance of a given area, considered as an entity, in no way governs the precise delimitation of its boundaries, any more than uncertainty as to boundaries can affect territorial rights. There is, for instance, no rule that the land frontiers of a State must be fully delimitated and defined, and often in various places and for long periods they are not, as is shown by the case of the entry of Albania into the League of Nations." North Sea Continental Shelf Cases (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands), 20 February 1969, ICJ Reports 1969, p. 32.

[8] For Crawford, the requirement of territory is merely a component of the effective government criterion rather than a "distinct criterion of its own." Crawford, *The Creation of States in International Law*, see note 4, p. 52

[9] Allen Buchanan, "The Making and Unmaking of Boundaries: What Liberalism Has to Say" in Allen Buchanan and Margaret Moore, eds., *States, Nations, and Borders: The Ethics of Making Boundaries*, CUP, 2003, p. 232-3.

[10] Stephen D. Krasner, "Westphalia and All That" in Judith Goldstein and Robert Keohane, eds., *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change*, Cornell University Press, 1993; Stephen D. Krasner, *Sovereignty: Organized Hypocrisy,* Princeton University Press 1999; Andreas Osiander, "Sovereignty, International Relations, and the Westphalian Myth", *International Organization*, vol. 55, no. 2,

the *Isle of Palmas* case "territorial sovereignty serves to divide between nations space upon which human activities are employed".[11]

Although territorial borders are now synonymous with states and international law, this has not always been the case. It was the Peace of Westphalia of 1648 that is credited with the emergence of the modern concept of the state by recognising the exclusivity of political authority over distinct portions of territory.[12]

Whether this is the case can be debated but the attribution of the modern system of sovereign states to the Peace of Westphalia is one of the foundational myths of international law[13] and it is not my purpose to debunk this myth. Instead, my purpose is to use the Peace of Westphalia as a temporal marker in order to explain and compare the pre-and post-Westphalian state of affairs as far as the relationship between authority, territory, and borders is concerned.

The pre-Westphalian order was characterised by a different organisation of authority which was not necessarily territorial or exclusive. That period was characterised by the unity of the Respublica Christiana with its segmented, often overlapping, and complex system of authority. Authority in that period was not over spaces but over places such as cities or over people through allegiances.[14] There were also overlapping authorities within the same formation with the Pope being the highest authority without however yielding claim to any territory. What characterised these arrangements of authority was the fact that they were based on the notion of control and allegiance and thus obscured distinctions between external and internal authority which, as was said, define the modern concept of statehood and of international law. The concept of international law that applied in that period was closer to the Roman concept of *jus gentium* as the common law that applied to

2001; Leo Gross, "The Peace of Westphalia, 1648-1948", *The American Journal of International Law*, vol. 42, no. 1, 1948, p. 20.

[11] Island of Palmas Case (or Miangas) (United States v Netherlands), 4 April 1928, RIAA II 839.

[12] Peace of Westphalia, signed on 30 January 1648 and 24 October 1648.

[13] Pope Innocent X condemned the treaty as "null, void, invalid, iniquitous, unjust, damnable, reprobate, inane, empty of meaning and effect for all time." David Maland, *Europe in the Seventeenth Century*, Macmillan, 1966, p. 16.

[14] Marc Bloch, *Feudal Society, Volume 2*, University of Chicago Press, 196.

all people regardless of affiliation, place or situation[15] rather than the law that applied to territorially separate authorities which represents the modern (post-Westphalian) definition of international law.[16]

Grotius and Vattel, the 'fathers' of international law, provided theoretical support to the notion of sovereign, territorially bounded, states.[17] They were both writing in an era where political theorists such as Bodin or Hobbes promoted sovereignty as an organising principle of political entities. Sovereignty for Bodin represented the consolidation of power: from fragmentation of powers, towards a central authority.[18] Whereas these theorists explored the internal aspects of sovereignty, Grotius and Vattel explored the external dimension and implications of sovereignty. Grotius decoupled authority and, thus sovereignty, from people or from the universal society. The former construction of authority was grounded on notions of personal allegiance and popular legitimacy whereas the latter was purely normative, based on political or religious allegiances among people. Both constructions of authority were subjective and, even more critically, fragmented and complexified the basis and scope of political authority. In Grotius work, sovereignty became conterminous with the territory and with the state as the political institution representing that territory.[19] In doing so, Grotius objectified and simplified the organisation and practice of sovereignty in that sovereignty as authority ceased to be dependent on affiliations or on allegiance but was determined by territorial borders which are physical and tangible. As a result, all persons and objects within borders fell under a state's exclusive authority, irrespective of any religious, ethnic or other bonds and allegiances they may have had. Moreover,

---

[15] Justinian, *The Institutes of Justinian*, book 1, 15th ed., translation by Thomas Collett Sandars, Longmans 1922, tit. II, para. 1. See also David J. Bederman, *International Law in Antiquity,* CUP, 2001, p. 1-15.

[16] Henry Wheaton, *History of the Law of Nations in Europe and America: From the Earliest Times to the Treaty of Washington, 1842*, Gould, Bank & Company, 1845, p. 26.

[17] Henry S. Maine, *Ancient Law: Its Connection with the Early History of Society and Its Relation to Modern Ideas*, Peter Smith, 1970, p. 92-108.

[18] Jean Bodin, *Les six livres de la Republique*, Chez Iacques du Puys, 1576, livre I, ch. 8, p. 131; F. H. Hinsley, *Sovereignty*, 2nd ed., CUP, 1986.

[19] Hugo Grotius, *De jure belli ac pacis [The Law of War and Peace in Three Books]*, translation by Francis W. Kelsey, book 1, ch. III, § VII, Prolegomena, §§ 35-40, Clarendon Press, 1925.

borders cut off any bonds and allegiances that may have existed with peoples living outside those borders, thus consolidating the exclusivity of state authority. For Vattel, the state is central tenet in his theory.[20] Vattel ponders on the legal implications of state sovereignty by relying on natural law concepts of independence and equality. As he wrote, civil societies require an "authority capable of giving commands, prescribing laws, and compelling those who refuse to obey. ... Such an idea is not to be thought of as between Nations. Each independent State claims to be, and actually is, independent of all others."[21] As a result, "the State, remains absolutely free and independent with respect to all other men, and all *other Nations,* as long as it has not voluntarily submitted to them. "[22]

Although the process of state consolidation was gradual, the Westphalian conceptualisation of statehood as supreme and exclusive authority over a defined territory and its people - having dissolved any competing internal authorities – and externally recognising no other higher authority is omnipresent in international law.

How this conceptualisation of statehood still defines international law can be demonstrated by looking into claims to statehood in the exercise of the right to self-determination in the colonial and post-colonial context.[23]

The right to self-determination denotes the right of peoples to determine freely their political status. At the basis of this right, particularly in the colonial era, is a claim to political authority over a certain territory which often leads to the formation of a new state. Borders have always played an important role in determining and

[20] DdG, see note 2, vol. III, para. 7a, note k.

[21] DdG, see note 2 ,vol III, para. 8a

[22] DdG, see note 2, para. lv-lvi.

[23] Charter of the United Nations, signed on 26 June 1945, art. 1(2), 55; International Covenant on Economic, Social and Cultural Rights, adopted 16 December 1966 (entered into force 3 January 1976), art 1(1); International Covenant on Civil and Political Rights, adopted 16 December 1966 (entered into force 23 March 1976) art. 1(1); Declaration on the Granting of Independence to Colonial Countries and People, (14 December 1960) UNGA Res 1514 (XV); Declaration on Principles of International Law Concerning Friendly Relations, 24 October 1970) UN GA Res. 2625 (XXV); Case Concerning East Timor (Portugal v. Australia), 30 June 1995, ICJ Reports 1995, p. 102.

shaping this right and, particularly, in determining not only the subject of the right to self-determination but also its content and scope. In the colonial context, the right to self-determination meant that it was colonial people located in areas defined by colonial borders that could exercise this right within the existing colonial borders, irrespective of whether the subject of the right -the 'peoples' - were a homogenous group, shared the same identity or had the same aspirations over territory. Hence, borders and territory determined which people could exercise the right to self-determination as well as the territorial scope of the right and of the ensuing state authority, contrary to Judge Dillard's musing that "It is for the people to determine the destiny of the territory and not the territory the destiny of the people".[24] The critical role of borders in the self-determination context was also confirmed by the principle of *uti possidetis accepted by the then Organisation of African States*[25] and by international jurisprudence. This principle confined the new states that emerged from the exercise of the right to self-determination to the previously drawn colonial borders irrespective of how arbitrary or artificial those borders may have been, and, regardless of whether they represented the territory over which the 'peoples' claiming self-determination lived. Existing borders thus acted as law stabilisers and allowed new states to be immediately integrated into international law. As the ICJ opined, "the principle of *uti possidetis* freezes the territorial title; it stops the clock but does not put back the hands".[26] The ICJ further explained the role of *uti possidetis*[27]

> "24. . . . There is no doubt that the obligation to respect pre-existing international frontiers in the event of a State succession derives from a general rule of international law, whether or not the rule is expressed in the formula *uti possidetis. […]*
>
> 25. However, it may be wondered how the time-hallowed principle has been able to withstand the new approaches to international law as

[24] Western Sahara (Separate opinion of Judge Dillard), 16 October 1975, ICJ reports 1975, p. 122.

[25] Resolutions Adopted by the First Ordinary Session of the Assembly of Heads of State and Government Held in Cairo (Resolution 16(1), Border Disputes Among African States), 17 to 21 July 1964.

[26] Case Concerning the Frontier Dispute (Burkina Faso/Republic of Mali), 22 December 1986, ICJ Reports 1986 p. 568.

[27] Ibid, p. 564.

> expressed in Africa, where the successive attainment of independence and the emergence of new States have been accompanied by a certain questioning of traditional international law. At first sight this principle conflicts outright with another one, the right of peoples to self-determination. In fact, however, the maintenance of the territorial status quo in Africa is often seen as the wisest course, to preserve what has been achieved by peoples who have struggled for their independence, and to avoid a disruption which would deprive the continent of the gains achieved by many sacrifices. The essential requirement of stability in order to survive, to develop and gradually to consolidate their independence in all fields, have induced African States judiciously to consent to the respecting of colonial frontiers, and to take account of it in the interpretation of the principle of self-determination of peoples."

The role of borders was also critical in the post-colonial exercise of the right to self-determination by peoples living within federal states. In this case, internal administrative borders which were drawn to delimit internal administrative competences were transformed into external borders, delimiting sovereign authorities and thus triggering the application of international law.[28] The Arbitration Commission of the European Conference on Yugoslavia in an influential pronouncement declared that

> "it is well established that, whatever the circumstances, the right to self-determination must not involve changes to existing frontiers at the time of independence *(uti possidetis juris) except where the states concerned agree otherwise"*.[29]

The Commission also held in Opinion No. 3 that

> "[e]xcept where otherwise agreed, the former boundaries become frontiers protected by international law. This conclusion follows from the principle of respect for the territorial status quo and in particular from the principle of *uti possidetis. […]"*[30]

---

[28] "[I]t has to be remembered that no question of international boundaries could even have occurred to the minds of those servants of die Spanish Crown who established administrative boundaries" Land, Island and Maritime Frontier Dispute (El Salvador/ Honduras: Nicaragua intervening), 11 September 1992, ICJ Reports 1992, p. 387-8

[29] Arbitration Commission of the Peace Conference on Yugoslavia, *Opinion No. 2*, reprinted in Alain Pellet, "The Opinions of the Badinter Arbitration Committee a Second Breath for the Self-Determination of Peoples", *EJIL* vol 1, no. 3, 1992, p. 184.

[30] Arbitration Commission of the Peace Conference on Yugoslavia, *Opinion No. 3*, reprinted in Alain Pellet, "The Opinions of the Badinter Arbitration Committee a Sec-

The preceding discussion also reveals the constitutive and functional role of borders in international law. In the process of state formation, borders demarcate actual claims to political authority over territories and in doing so they also contribute to the consolidation, unification, and centralisation of such authority. A state thus denotes the horizontal and vertical integration of authority over a certain territory. In this sense, borders are constitutive of states. Because borders define states and states are the foundational authority of international law, borders are also constitutive of international law; without states, international law would lack ontological meaning. They are also constitutive of international law because states are the genitor of international law; they create, implement and enforce international law.

Furthermore, borders determine the political and geographic scope of a state's authority by demarcating it from other authorities and they also demarcate the internal from the external dimension of state authority. In doing so they determine when and where international law applies to endow international law with functional relevance. The functional role of borders is also evident in the application of different law regimes or in relation to certain international rules such as the rules on non-intervention, non-use of force or self-defence which rely on the crossing of borders - physical or political-legal – to acquire meaning and relevance.[31] For example, whether the law of international armed conflict or the law of non-international armed conflict applies in a particular situation depends on whether the hostilities cross a frontier. Similarly, the rule on non-intervention applies and acquires meaning when there is a physical crossing of a frontier or interference with the internal aspects of sovereignty. In this sense, borders determine what falls within and what fall outside a state's sovereignty which is also critical in determining what is permissible and what is impermissible intervention. The Tallinn Manual 2.0 makes this clear when it says

> "violation of sovereignty occurs whenever one State physically crosses into the territory or national airspace of another State without either its consent or another justification in international law […]".[32]

.

ond Breath for the Self-Determination of Peoples", *EJIL* vol 1, no. 3, 1992, p. 185.

[31] Charter of the United Nations, see note 24, art. 2(4) and 51.

[32] Michael N. Schmitt, ed., see note 51, rule 4 para. 6.

Whereas this section has explored the relationship between international law, states, territory, and borders, the next section will consider the viability of this relationship in cyberspace.

III. INTERNATIONAL LAW, BORDERS, AND TERRITORY IN CYBERSPACE

A common representation of cyberspace is that it is a-territorial and borderless and that for this reason, it cannot be subject to the law as recognised and practiced in the physical world. Instead, cyberspace is subject to different legal constructions. John Barlow's *Declaration of the Independence of Cyberspace*[33] set the scene by rejecting the application of sovereignty and its concomitant laws to cyberspace. According to the declaration:

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> We have no elected government, nor are we likely to have one, ….. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.
>
> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. […] Cyberspace does not lie within your borders. […]
>
> We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.
>
> Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.
>
> […]
>
> Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

[33] John P Barlow, "A Declaration of Independence for Cyberspace" (Davos, 1996), available at: https://www.eff.org/cyberspace-independence, accessed on 24 August 2017

> Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose. […]
>
> These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.
>
> We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before."

The debate between Professors Johnston and Post on one hand and Professor Goldsmith on the other as to whether law and, more specifically, international law applies to cyberspace and how that law is created, applied and enforced is informed by different views about the role and relevance of borders and of territorially bounded sovereignty in cyberspace.[34]

Johnson and Post reject the possibility of applying existing notions of sovereignty and law to cyberspace due to its distinct non-territorial and borderless character and, for this reason, they propose the development of discrete laws for cyberspace.[35] According to them, in the physical world, borders determine the law that applies within a certain space and there is an overlap between the physical space represented by states and the 'law-space'. However, the borderless character of cyberspace undermines the possibility of legal regulation because it challenges

[34] David R. Johnson & David Post, "Law and Borders - The Rise of Law in Cyberspace", *Stanford Law Review,* 48, 1996, p. 1367; David Post, "Against 'Against Cyberanarchy'", *Berkeley Technology Law Journal*, vol. 17, no. 4, 2002, p. 1365; Jack L. Goldsmith, "Against Cyberanarchy", *University of Chicago Law Review*, 65, 1998 p. 1199*;* Jack L. Goldsmith, "The Internet and the Abiding Significance of Territorial Sovereignty", *Indiana Journal of Global Legal Studies*, vol. 5, no. 2., 1998, p. 475.

[35] David R. Johnson & David Post, see note 34, p. 1367.

the bases upon which law is created and applied. More specifically cyberspace destroys the link between borders and four critical variables, to wit, power, legitimacy, effects, and notice.[36] Power as an authority is as was said the essence of sovereignty and of statehood but the lack of borders deprives sovereigns of the ability to exercise power over defined territories and peoples and deprives sovereigns the legitimising effect of consent. The lack of borders also obscures the links between a cyber activity and a certain 'law-space' and undermines the exclusivity of power. It also deprives people from noticing when they enter a different 'law space'. All the above pose challenges to law and, although cyberspace needs to be regulated, existing territorially based laws are not suitable to cyberspace. For this reason, the authors opt for a system of self-regulation of cyberspace by its participants.[37]

Notwithstanding the forcefulness of their argument, it should be noted that Johnston's and Post's argument is not as radical as it seems because they do not reject the application of law or of international law to cyberspace and, moreover, they still rely on borders for purposes of law-creation, law-application and law-enforcement in cyberspace, albeit a different kind of borders. To explain, they 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. Secondly, although they reject the possibility of applying existing laws and law-making processes to cyberspace because they are territorially-grounded and they are based on notions of physical borders, they do not reject the existence of borders in cyberspace. Instead, the authors introduce a different border consisting of screens and passwords which distinguish the virtual from the real world. This may be a monumental and non-physical border but a border nonetheless. Moreover, according to the authors, this border is placed around cyberspace and thus defines cyberspace as a space separate from real space. What transpires is that borders still play a constitutive as well as a functional role because they define the expanse that is called cyberspace and they determine what falls within the real and what falls within the virtual space. Thirdly, borders continue to define the organisation of power within cyberspace as a separate space. The difference with the physical world of states

[36] Ibid, p. 1370-6.

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

is that, whereas in the latter case authority is organised and practiced within defined territories with no overarching power existing above them, in cyberspace, authority is unmediated, non-fragmented and conterminous with the borders of cyberspace.

Johnson's and Post's position concerning the exceptional nature of cyberspace was challenged by Jack Goldsmith in his article "Against cyber anarchy".[38] For him, there is nothing unexceptional as far as cyberspace is concerned and that contrary views are much exaggerated. What, according to Goldsmith, needs to be realised is that cyberspace consists of persons and objects; thus states can exercise power over people and objects on their territory and regulate their activities. Such regulation has also by default extraterritorial effects expanding in this way the state's regulatory power extraterritorially. Furthermore, there is an extension of the territorial scope of the law when the state regulates the local effects of extraterritorial activities. According to Goldsmith, traditional legal tools can resolve the multi-jurisdictional problems that arise and also address the issue of legitimacy and validity of the law. With regard to law-enforcement, Goldsmith criticises Johnson and Post for confusing the ability to enforce the law which exists in cyberspace with the cost of enforcement; for failing to recognize the deterrent effect of local enforcement; and for building their critique upon a notion of near-perfect enforcement. For him, the standard rules of enforcement based on a person's location, on 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. Goldsmith furthermore makes a distinction between mandatory laws that apply across the board and default laws that apply to specific situations and may also apply to cyberspace, for example, the law concerning technical standards.

The above represent views expressed at the early days of legal encounters with cyberspace and, as was explained, accept explicitly or implicitly the role of physical or normative borders in the application of the law to cyberspace.

By now it is broadly accepted that international law applies to

[38] Jack L. Goldsmith, "Against Cyberanarchy", see note 34, p. 1199.

cyberspace. For example, 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, especially the 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, and to jurisdiction over ICT infrastructure within a State's territory.[39] According to the UN Secretary-General, the recommendations contained in the report "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".[40] The 2015 GGE Report went a step further by spelling 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 aimed at promoting an open, secure, stable, accessible and peaceful ICT environment. They are the following:[41]

1. States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;
2. states should consider all relevant information in case of ICT incidents including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences
3. states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
4. states should consider how best to cooperate to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs
5. states should respect the UN resolutions that are linked to human

[39] 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.

[40] Ibid, p. 4.

[41] UNGA, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 22 July 2015, UN Doc A/70/174, para. 13.

rights on the internet and to the right to privacy in the digital age
6. states should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure;
7. states should take appropriate measures to protect their critical infrastructure from ICT threats;
8. states should respond to appropriate requests for assistance by other states whose critical infrastructure is subject to malicious ICT acts;
9. states should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions;
10. states should encourage responsible reporting of ICT vulnerabilities and should share remedies to these.
11. states should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity;

Furthermore, the list of international law principles applicable to cyberspace includes[42]:

1. state sovereignty;
2. sovereign equality;
3. the settlement of disputes by peaceful means;
4. refraining from the threat or use of force in international relations;
5. non-intervention in the internal affairs of other states;
6. respect for human rights and fundamental freedoms.

The GGE failed to produce a report in 2017 due to lack of consensus on how specific norms and principles apply to cyberspace but, that notwithstanding, previous reports attest to the view that principles and norms developed for and applicable to the physical world and linked to

[42] Ibid, para 26.

territorially bounded spaces are deemed to apply to cyberspace. This phenomenon can be described as the territorialisation of cyberspace; namely the application to cyberspace of territorialist and, by consequence, of sovereigns notions of authority and law.[43]

IV. THE TERRITORIALISATION OF CYBERSPACE AND INTERNATIONAL LAW

In order to explain the epistemic premises of this phenomenon, it is important to explain the nature of cyberspace and whether cyberspace falls within the categorical schemes of territory and state sovereignty which, as explained above, define international law. According to Kuehl 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".[44]

It transpires from this definition that cyberspace has a physical layer which consists of computers, integrated circuits, cables, communications infrastructure and the like; a logical layer which consists of the software logic data packets and electronics[45] and a social layer which includes human beings. Consequently, a state can extend its sovereignty over the physical layer that is, over the infrastructure located on its territory. It can also exercise sovereign power over the social layer that is, over persons on its territory. The state can also assert its sovereignty over the effects of cyber activities that are felt on its territory regardless of their provenance. Furthermore, the state can assert its sovereignty over information that passes through its infrastructure or begins or

[43] Nicholas Tsagourias, "The Legal Status of Cyberspace" in Nicholas Tsagourias & Russell Buchan, eds., *Research Handbook on International Law and Cyberspace*, Edward Elgar, 2015; Geoffrey Herrera, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space", in Myriam Dunn Cavelty, Victor Mauer, Sai Felicia Krishna-Hensel, eds., *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, Ashgate, 2007, p. 67-93.

[44] Daniel T Kuehl, "From cyberspace to cyberpower: Defining the problem" in Franklin D. Kramer, Stuart H. Starr, Larry K Wentz, eds., *Cyberpower and National Security* (National Defense University Press, 2009, p. 28. [italics in the original]

[45] Lior Tobanksy, "Basic concepts in cyber warfare", *Military and Strategic Affairs*, vol. 3, no. 1, 2011, p. 77-78.

ends on its territory. All the above show that existing international law norms which are territorially bounded can extend to and regulate cyber activities.

This phenomenon can be understood better by using the alleged Russian interference in the 2016 US elections as an example.[46] The incident involved hacking into the Democratic National Committee emails and the release by WikiLeaks of emails with information to embarrass or undermine the campaign of Hillary Clinton, the Democratic candidate. The incident thus involved the use of cyber infrastructure and cyber means to influence the US political process. The Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) issued a joint statement claiming that the Russian government was responsible for the hack and publication of the materials in its attempt to "interfere with the US election process."[47] According to reports, President Obama told President Putin that "international law, including the law for armed conflict, applies to actions in cyberspace"[48] and considered US responses to the incident. The FBI[49] report *Joint Analysis Report: GRIZZLY STEPPE*—Russian Malicious Cyber Activity reinforced the view that Russia was behind the WikiLeaks releases. Furthermore, according to the report Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution, the intention of the leaks was to

---

[46] Jens David Ohlin, "Did Russian Cyber interference in the 2016 Election Violate International Law?" *Texas Law Review*, no. 95, 2017.

[47] Director of National Intelligence, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security" (7 October 2016), available at: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national, accessed on 24 August 2017.

[48] William M. Arkin, Ken Dilanian & Cynthia McFadden, "What Obama Said to Putin on the Red Phone About the Election Hack", NBC News (19 December 2016), available at:
http://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hackn697116, accessed on 24 August 2017.

[49] U.S. Department of Homeland Security & Federal Bureau of Investigation, "Joint Analysis Report: GRIZZLY STEPPE—Russian Malicious Cyber Activity" (29 December 2016), available at: https://www.uscert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZL Y%20STEPPE-2016-1229.pdf, accessed on 24 August 2017.

"undermine public faith in the US democratic process."[50]

Departing from the assumption that Russia was responsible for the hacking, the incident implicates two international law principles identified by the GGE as being applicable to cyberspace: one is the principle of sovereignty and the other is the principle of non-intervention.[51] These two principles are central to and, indeed, manifestations of the territorially-bound approach to international law.

The principle of sovereignty denotes "the collection of rights held by a state".[52] These rights cover the internal as well as the external aspects of state sovereignty. As explained above, the internal aspect of sovereignty denotes *summa potestas* over territory and people,[53] that is, exclusive and supreme authority to regulate comprehensively human action and to enforce the law within a certain territory.[54] The external aspect of sovereignty denotes the state's supreme, original and total power in its international relations. Being all-encompassing, the principle of sovereignty can be dissected into more specific principles rights with non-intervention being one such specific right which has acquired independent legal status.[55] Non-intervention protects the

[50] ICA, "Assessing Russian Activities and Intentions in Recent US Elections" in Office of the Director of National Intelligence, "Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution" (6 January 2017) ICA 2017-01D, p. 1, available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf accessed on 24 August 2017.

[51] For the application of these principles to cyberspace see Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, CUP, 2017, rules 1-4, rule 66.

[52] James Crawford, *Brownlie's Principles of Public International Law,* 8th ed., OUP, 2012, p. 448.

[53] Samantha Besson, "Sovereignty" in Rüdiger Wolfrum, ed., *Max Planck Encyclopedia of Public International Law,* OUP, 2012.

[54] "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", *International Studies Quarterly*, vol. 39, no. 2, 1995, p. 213, 223.

[55] Montevideo Convention, see note 4, art. 8; UNGA, "Declaration on Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of the Independence and Sovereignty" 21 December 1965, UN Doc A/RES/20/2131; Declaration on Principles of International Law Concerning Friendly Relations, see note 24; Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America), 27 June 1986, ICJ Reports 1986, paras. 202, 204.

internal dimension of sovereignty[56] By prohibiting any coercive interference into the domestic affairs of a state.[57] This has been expressed in the 1965 UN General Assembly resolution in the following words: "no state has the right to intervene, directly or indirectly, for any reason whatever, in the internal […] affairs of any other state" and every "state has an inalienable right to choose its political, economic, social and cultural systems without interference in any form by another state' As the ICJ also said in the Nicaragua case

> "the principle [of non-intervention] forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely".[58]

The ICJ went on to offer examples of matters that fall within a state's sovereign prerogative such as the choice of a political, economic, social and cultural system and the formulation of foreign policy. The list is not exhaustive[59] and can change depending on developments in international law and relations but, if a state's sovereign prerogatives are unduly compromised, the principle of non-intervention is violated.

Applying the above considerations to the case at hand, would Russia's alleged interference amount to unlawful intervention into US domestic affairs? According to Former Department of State Legal Adviser Brian Egan "a cyber operation by a State that interferes with another State's ability to hold an election or that manipulates a State's election results would be a clear violation of the rule of non-intervention".[60] That notwithstanding, whether this is the case depends

---

[56] Military and Paramilitary Activities in and against Nicaragua, see note 53, para. 251: "The effects of the principle of respect for territorial sovereignty inevitably overlap with those of the principles of the prohibition of the use of force and of nonintervention."

[57] Hersch Lauterpacht, ed., *Oppenheim's International Law: a treatise, vol. 1*, D. McKay, 1955, p. 305; Robert Jennings and Adam Watts eds., *Oppenheim's International Law*, Longman, 1996) p. 432.

[58] Military and Paramilitary Activities in and against Nicaragua, see note 53, para. 205.

[59] Ibid.

[60] Brian J. Egan, "Remarks on International Law and Stability in Cyberspace at Berkeley Law School" (10 November 2016), available at: https://www.law.berkeley.

on affirmatively answering two sub-questions: first, whether Russia's action impinged on sovereign prerogatives; and, second, whether it was coercive. With regard to the first sub-question, the choice of a political system and the choice of government is a state prerogative; it is one of the highest manifestations of internal sovereignty. Hence, to the extent that Russia's actions were intended to interfere with the political process of electing the next US President, they would have impinged on sovereign matters which should remain immune from outside interference. The answer to the second sub-question - whether the interference was coercive – is more nuanced. Coercion means that the will of the state is manipulated in order to do something that it would not otherwise do. Coercion is not the same as influence or interference but it is imperative pressure to do or to abstain from doing something. Put in different words, it is not an interference in sovereign prerogatives that constitutes unlawful intervention but interference in sovereign prerogatives that rises to the level of compulsion.[61] Consequently, the answer to the question of whether Russian interference in the US electoral process constitutes intervention depends on whether the US electorate was actually compelled to vote for someone that they would not otherwise have voted for. In my opinion, Russia's actions did not reach that threshold; they may have influenced some voters but it seems to not have compelled voters to change their mind since the targeted candidate - Hillary Clinton - received more votes than her opponent.[62] The conclusion would have been different however if there was tampering with the voting machines.

If Russia's meddling does not constitute unlawful intervention into

edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf, accessed on 24 August 2017.

[61] Dov H. Levin, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results", *International Studies Quarterly*, vol 60, no 2, 2016, p. 189–202. [it uses the word intervention in generic sense and not in the legal sense]

[62] Harriet Agerholm, "Hillary Clinton's lead over Donald Trump in popular vote passes 2.5 million" (2 December 2016), available at: http://www.independent.co.uk/news/world/americas/us-elections/hillary-clinton-donald-trump-popular-vote-lead-25-million-a7451661.html, accessed on 24 August 2017. *Contra* Steven J. Barela, "Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion", (12 January 2017) available at: https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion, accessed on 24 August 2017.

US domestic affairs in the absence of coercion, will it amount to a violation of the principle of sovereignty? The view that it violated US sovereignty has been put forward by certain commentators.[63] Whether this so depends on the content of the principle of sovereignty and on whether it is a legal norm, triggering legal consequences.

As explained above, sovereignty is a 'catch-all' principle which can be dissected into more specific norms but remains the fall-back principle that captures any interference within a state's exclusive internal and external authority which is not captured by other more specific rules such as those on non-intervention or non-use of force. For example, in the *Nicaragua Case,* the ICJ determined that US over flights of Nicaragua which did not constitute uses of force or intervention violated Nicaragua's sovereignty.[64] Hence, any interference in a state's political process or decision-making power would violate its sovereignty even if it does not rise to the level of intervention. Moreover, any unauthorised interference with a state's cyber infrastructure affecting its function or integrity would constitute a violation of that state's sovereignty. That having been said, the next question is whether the principle of sovereignty is a legal norm whose violation can produce legal consequences. Sovereignty is often referred to as a principle or a norm, both alluding to its more general nature in contrast to rules which are specific prescriptions or proscriptions. This fact alone or the fact that it has not been codified does not deprive it of legal status. Sovereignty constitutes a customary law norm having been recognised as such by states and courts. The ICJ has, for example, treated sovereignty as a legal norm in the *Corfu Channel case* where the Court held that "Between independent States, respect for territorial sovereignty is an essential foundation of international relations" and it went on by saying 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".[65] Likewise, in the *Nicaragua case*

[63] Sean Watts, "International Law and Proposed U.S. Responses to the D.N.C. Hack" (14 October 2016), available at: https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack, accessed on 24 August 2017.

[64] Military and Paramilitary Activities in and against Nicaragua, see note 53, paras 88, 251

[65] Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), 9 April 1949, ICJ Reports 1949, p. 35, 36.

the Court held that US over flights violate Nicaragua's sovereignty.[66] In *Costa Rica/Nicaragua case,* 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".[67]

It follows from the above that to the extent that sovereignty is a legal norm, interference with the US political process and the unauthorised entry into its cyber infrastructure to retrieve emails would amount to a violation of US sovereignty.

V. REALIGNING SOVEREIGNTY AND CYBERSPACE

The preceding discussion has shown how international rules based on territorially-bound notions of sovereignty can apply to cyberspace. In this section, I will explain how states realign their sovereignty to cyberspace and in particular how states assert their sovereignty in cyberspace by curving out cyberspace into distinct areas corresponding to national territorial borders. Although, as was said previously, the application of the principle of sovereignty to cyberspace has been broadly accepted, certain states have particularly insisted on the notion of cyber sovereignty as the centrepiece of their political and legal approach to cyberspace and to cyber-regulation. China is such a state.[68] In 2010 a White Paper entitled "The Internet in China" was published which stressed the sovereign implications of the internet.[69] In 2015,

[66] Military and Paramilitary Activities in and against Nicaragua, see note 53, para 251.

[67] 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.

[68] Hao Yeli, "A Three-Perspective Theory of Cyber Sovereignty", Prism: Journal of the Center for Complex Operations, vol 7, no. 2 (2017), 109, available at: http://cco.ndu.edu/Portals/96/Documents/prism/ prism_7-2/10-3-Perspective%20Theory.pdf accessed on 24 August 2017

[69] "The Internet in China" (White Paper, 8 June 2010) available at: http://en.people.cn/90001/90776/90785/7017201.html accessed on 24 August 2017, "IV. Basic Principles and Practices of Internet Administration:

[…] China advocates the rational use of technology to curb dissemination of illegal information online. Based on the characteristics of the Internet and considering the actual requirements of effective administering of the Internet, it advocates the exertion of technical means, in line with relevant laws and regulations and with reference to common international practices, to prevent and curb the harmful effects of

China and Russia together with Tajikistan, Uzbekistan, Kazakhstan, and Kyrgyzstan, submitted to the General Assembly of the United Nations a proposal of an 'International Code of Conduct for Information Security' which contained a pledge to respect the 'sovereignty, territorial integrity and political independence of all States'.[70] Chinese President Xi Jinping stressed the importance of cyber-sovereignty during his address to the Second World Internet Conference in Wuzhen in 2015 and claimed that cyber sovereignty is critical to national sovereignty.[71] At the 7th International Safe Internet Forum conference in 2016, Fang BinXing member of the Chinese Academy of Engineering and chief architect of China's Golden Shield Project (Firewall) said 'Sovereignty in general, and digital sovereignty in particular, is the inherent right of every nation and its citizens.'[72] In 2016, China's Ministry of Foreign

illegal information on state security, public interests and minors. The Decision of the National People's Congress Standing Committee on Guarding Internet Security, Regulations on Telecommunications of the People's Republic of China, Measures on the Administration of Internet Information Services, Measures on the Administration of Security Protection of the International Networking of Computer Information Networks, and other laws and regulations clearly prohibit the spread of information that contains contents subverting state power, undermining national unity, infringing upon national honor and interests, inciting ethnic hatred and secession, advocating heresy, pornography, violence, terror and other information that infringes upon the legitimate rights and interests of others. According to these regulations, basic telecommunication business operators and Internet information service providers shall establish Internet security management systems and utilize technical measures to prevent the transmission of all types of illegal information."

[70] Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, Russia
n Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General A/69/723 (13 January 2015)

[71] "Why Does Cyber Sovereignty Matter?" China Daily, December 16, 2015, available at: http://www.chinadaily.com.cn/business/tech/2015-12/16/content_22728202.htm accessed on 24 August 2017

[72] Safe Internet Forum (2016) Moscow safer internet Forum adopts Russia-China cybersecurity cooperation roadmap, 29 April. Available at: http://safeinternetforum.ru/en/novosti/moscow-safer-internet-forum-adopts-russia-china-cybersecurity-cooperation-roadmap.html accessed on 24 August 2017

Affairs and the Cyberspace Administration of China jointly released a White Paper, 'International strategy of cooperation on cyberspace', which asserts that, as a basic norm in international relations, the principle of territorial sovereignty includes cyberspace.[73] The protection of sovereignty in cyberspace is also one of the ways for ensuring national security according to the Law of Cyber-security of China.[74]

China deploys the principle of cyber sovereignty in order to stress the need for an inter-governmental approach to cyber regulation in contradistinction to the mainly western multi-stakeholder approach and it also deploys the principle of sovereignty in order to protect its internal sovereignty in the sense of protecting its exclusive and supreme power over its territory and people.[75] In the latter instance, cyber sovereignty for China denotes power over the state's cyber infrastructure and over the information entering or becoming available within its sovereign domain. The manner in which China asserts its cyber sovereignty is through filtering, Filtering involves technical, political, legal, or social techniques to deny access to certain information or activities from the state or deny such information or activities entry into the sovereign space of a state. For example, the content of information is filtered on the basis of political, social, security or other grounds.[76] Such national

[73] Available at: http://usa.chinadaily.com.cn/epaper/2017-03/02/content_28410278.htm accessed on 24 August 2017

[74] Available at: https://www.cfr.org/blog/chinas-new-cybersecurity-law accessed on 24 August 2017

[75] Yi Shen "Cyber Sovereignty and the Governance of Global Cyberspace: Chin. Polit. Sci. Rev. (2016), 81–93, 90 ' … cyber sovereignty can be understood: the first key parts of cyber sovereignty refers to the sovereignty of the state to manage the information flow inside the territory; the second is that every single state has the power to make cyber related policy independently; the third is that every state should have roughly equalized rights to participate in the decision making process of the rules, norms, or code of conduct that governs global cyberspace; and the respect of sovereignty should be one of the most important guiding principles to deal with cyber related issues internationally'.

[76] Ronald J. Deibert, "The geopolitics of internet control: censorship, sovereignty, and cyberspace" in Andrew Chadwick & Philip N. Howard, eds., *The Routledge Handbook of Internet Politics*, Routledge, 2009, p. 323-36; Jonathan Zittrain , John Palfrey, Ron Deibert & Rafal Rohozinski, *Access denied: The practice and policy of global internet filtering*, MIT Press, 2008; Ronald Deibert, John Palfrey, Rafal Rohozinski & Jonathan Zittrain, , *Access controlled: The shaping of power, rights, and rule in*

restrictions and control over the flow of information was dubbed as the 'Great Firewall of China' or less charitably as "information curtain".[77]

A more advanced method of asserting sovereignty in cyberspace is the creation of national cyberspace zones by disconnecting national networks from the world wide web and by creating a national internet. North Korea's 'Kwangmyong' internet or Iran's 'Halal internet' are such examples.[78] The North Korean internet consists of a search engine, news, email, and a browser and, according to reports, it has only 28 websites.[79] Iran's 'national internet' replaces the existing system of filtering the internet and is based on domestic hosting, internet protocol network and fibre optic networks.[80]

These examples show that states can curve their own sovereign cyberspace by erecting borders through technical means in order to control activities from outside or in order to insulate national services.[81]

cyberspace, MIT Press, 2010.

[77] Jill Dougherty & Doug Gross, "Clinton: Internet 'information curtain' is dropping" (21 January 2010), available at: http://edition.cnn.com/2010/TECH/01/21/clinton.internet/index.html, accessed on 24 August 2017.

[78] Simurgh Aryan, Homa Aryan, J. Alex Halderman, "Internet censorship in Iran: A first look" *Proceedings of the 3rd USENIX Workshop on Free and Open Communications on the Internet*, August 2013; Warf, B. (2015); "The Hermit Kingdom in cyberspace: unveiling the North Korean internet" *Information, Communication & Society*, vol. 18, no. 1, 2014, p. 109-120.

[79] Cara McGoogan, "North Korea's internet revealed to have just 28 websites" (21 September 2016), available at: http://www.telegraph.co.uk/technology/2016/09/21/north-koreas-internet-revealed-to-have-just-28-websites/. accessed on 24 August 2017. Saira Asher, "What the North Korean internet really looks like" (21 September 2016), available at: http://www.bbc.com/news/world-asia-37426725, accessed on 24 August 2017.

[80] Article 19, "Tightening the Net: Internet Security and Censorship in Iran, Part 1: The National Internet Project 2016" (2016), available at: https://www.article19.org/data/files/The_National_Internet_AR_KA_final.pdf, accessed on 24 August 2017.

[81] As China submitted "… 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", 18 July 2006, UN Doc A/61/161, p. 4

These borders correspond to the physical borders delimiting and defining state sovereignty but they also reaffirm state sovereignty in its political, social, economic, cultural and territorial organisation. Above all, it shows how states project the Westphalian concept of state sovereignty to cyberspace. Whether such a Westphalian 'moment' will lead to the division of cyberspace into sovereign zones depends on many factors. Whereas technology is an important factor because it can assist in actually curving cyberspace in the same way that the territorial notion of sovereignty was facilitated by technological advances such as in cartography which permitted the demarcation of expanses of territory in an abstract manner,[82] it is mainly political, economic and a number of other factors that are the primary motivators of such curving. For example, an open or closed cyberspace depends on political approaches to regulation, on states' approaches to sovereignty, on the relationship between citizens, society and the government as well as on the economic or other benefits states expect to gain from cyberspace. It is interesting in this regard to recall how Major General Hao Yeli of the Chinese People's Liberation Army divides cyber sovereignty into three levels. According to him, at the bottom level, that of cyberinfrastructure, 'states should be willing to collectively transfer authority in the interest of standardization and interconnectivity'; at the middle level of application 'the degree of cyber sovereignty should be adapted to local conditions' whereas at the top level of 'regime, law, political security, and ideology, which is unchallengeable and includes the governing foundations and embodies the core interests of the country', the leading role of the government remains. [83]

Although the above relate to active assertions of sovereignty in cyberspace, it should be noted that the opposite trend namely, states not claiming sovereignty in cyberspace or states promoting common regulatory regimes to maintain the common use of cyberspace[84] are

[82] Jordan Branch, *The Cartographic State: Maps, Territory, and the Origins of Sovereignty*, CUP, 2014.

[83] Hao Yeli, "A Three-Perspective Theory of Cyber Sovereignty" see note 69, 113-4

[84] For cyberspace as a global commons see Dan Hunter, "Cyberspace as place and the tragedy of the digital anticommons" *California Law Review*, vol. 91, no. 2, 2003, p. 439; Abraham M. Denmark & James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World*, Centre for New American Century, 2010.

also expressions of state sovereignty. Unilateral or collective abstention from the exercise of sovereign rights as well as voluntary limitations on sovereign rights are indeed expressions of state sovereignty.[85]

The question I want to explore is whether cyberspace can itself become sovereign. If sovereignty represents a claim over a portion of territory or otherwise over a space, cyberspace is such a space having, as was said, a physical, logical and social component. The difficulty however with the idea of sovereign cyberspace is that its physical and social components can never be disassociated from existing states; objects and people exist within states. Moreover, whereas in the physical world people or powerful authorities can claim a portion of territory as in the exercise of the right to self-determination and, if successful, create their own state with distinct borders separating themselves from people and objects residing in other territories, neither objects nor persons can move to cyberspace and sever their links with their own states. People may move certain activities and actions to cyberspace, they may experience cyberspace or they may nooumentally inhabit cyberspace but they can never remove themselves from the real world. This means that cyberspace and its organisation cannot be independent of states and therefore cyberspace cannot be sovereign because the authority in cyberspace is mediated by states. As for the purely virtual part of cyberspace, it cannot be sovereign because an inanimate, ethereal, space cannot be sovereign.

VI.CONCLUSION

The article portrayed constitutive and functional relationship between borders and territory with the institution of the state and international law. Borders were claimed to define territories and further determine which states and over which sovereignty can be exercised. Consequently, international law as the creation of sovereign states is dependent on borders. The article then explored the question of how the relationship between borders and territory manifests itself in cyberspace. It does so in the process of territorialisation of cyberspace in

[85] Case of the S.S. "Wimbledon" (17 August 1923) PCIJ Reports, Series A, no. 1, p. 25.

the sense of extending territorial notions of sovereignty and of international law to cyberspace with respect to activities, persons and objects. This relationship also manifests itself in the curving of national cyber zones. As to whether cyberspace itself can become sovereign, the article claimed that authority in cyberspace cannot be decoupled from real people and objects over whom states exercise sovereignty. Consequently, cyberspace cannot be sovereign in itself.

The question then is not whether cyberspace is subject to territorially bounded notions of sovereignty and international law but about the scope of state sovereignty over cyberspace and in cyberspace. This is a political question for individual states but also for the society of states. It is a question whose answer depends on states' political, legal, economic, social, and cultural interests, on perceptions about what is cyberspace or what cyberspace should be and on how states' interests are promoted, facilitated or constrained by or in cyberspace.