2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment

Przemysław Roguski
Lecturer
Chair of Public International Law
Jagiellonian University
Kraków, Poland
przemyslaw.roguski@uj.edu.pl

Abstract: The question of how to define sovereignty in cyberspace is currently one of the most contentious issues in international law. The traditional understanding of sovereignty is based on the assumption of exclusive control over geographically defined territory. However, the global accessibility of computer networks eliminates distance and geography as limiting factors for the exercise of power by States (and non-State actors). This creates a security dilemma: while modern ICTs allow adversaries to challenge States' exclusive authority over 'their' cyberspace, traditional notions of sovereignty appear to limit the States' ability to actively respond to these challenges in foreign networks.

In this paper I argue for a 'layered' understanding of sovereignty in cyberspace. Recent international practice, including national legislation and court decisions relating to jurisdiction over transboundary activities, shows that while States stress the exclusive nature of authority and jurisdiction over the physical layer of cyberspace, the logical and social layers are open to transboundary assertions of jurisdiction. Applying these findings to the general concept of sovereignty in cyberspace, I argue that while the physical layer is covered by State sovereignty by virtue of the principle of territoriality, the logical and social layers of cyberspace may be open to the exercise of State authority based on a criterion of proximity, i.e. whenever the State can establish a genuine link with the digital objects or online personae over which authority is to be asserted.

Keywords: *sovereignty, cyberspace, jurisdiction, territory, Tallinn Manual*

1. INTRODUCTION

One of the functions of international law as a legal system is to allocate, delimit and protect spheres of competence of States.[1] These spheres of competence are tied to the concept of State sovereignty, which is one of the foundational principles of international law. In the classic, post-Westphalian system, sovereignty is understood as exclusive authority of the State over persons and things within a specified territory.[2] All three elements of this definition – the nature of power/authority, its exclusivity and its territoriality – have been challenged by the invention of interconnected global communications networks, in short: cyberspace. Because cyberspace creates a space for storage of and access to information, as well as social interaction regardless of the user's location and irrespective of distances, it creates the perception of a space not restricted by – or even detached from – geography. In other words, cyberspace is perceived as a-territorial.[3] Similarly, cyberspace constitutes a challenge to the nature and exclusivity of authority. The worldwide accessibility of online content poses questions as to the extent of State jurisdiction in cyberspace and creates the possibility of a multitude of overlapping jurisdictions.[4] Additionally, the ease of access to information and communications technology [ICT] and the interconnectedness of computer networks have led to a rising importance of technology companies, individuals and groups of individuals as actors in cyberspace.

In view of these challenges, the question of how sovereignty applies in (and to) cyberspace has been a topic of constant debate among experts, in academia and in the international community. While the 2013 and 2015 Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security [GGE] have confirmed that sovereignty and the international norms and principles that flow from it apply to State conduct in cyberspace, they have left open the meaning and scope of sovereignty with respect to the cyber domain.[5] Since 2015 there has been little progress in this regard. The failure of the 2016-2017 GGE to adopt a consensus report[6] and, most recently, the adoption by the United Nations General Assembly [UNGA] of two

1 Hermann Mosler, 'Völkerrecht Als Rechtsordnung' (1976) 36 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 6, 39, 48.

2 Arthur Jennings and Robert Watts, *Oppenheim's International Law* (9th edn, Longmans 1992) para 117.

3 Nicholas Tsagourias, 'The Legal Status of Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015) 22.

4 Uta Kohl, 'Jurisdiction in Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015) 31ff.

5 UN GGE, *Report of the 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 [hereinafter GGE Report 2013], para 20; UN GGE, *Report of the 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 [hereinafter GGE Report 2015], para 27.

6 Michelle Markoff, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, 23 June 2017, <https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm> [accessed 11.03.2019].

competing resolutions on the further study of international security dimensions of cyberspace, make clear that the international community is yet to achieve a common understanding on many issues regarding the application of international law in cyberspace, including sovereignty.[7]

Against this background I argue that the Westphalian concept of sovereignty needs to be adjusted to account for the peculiarities of cyberspace. First, I recapitulate the current definition of sovereignty and its connection to the concept of territory. Then I briefly turn to the *Tallinn Manual 2.0* conception of sovereignty and why, in my view, it is too restrictive. After that I discuss examples where the traditional notion of territoriality is challenged in cyberspace and argue that sovereignty in cyberspace should indeed be perceived differently from sovereignty over physical territory. Lastly, I propose to use an analogy to the layered structure of cyberspace to conceptualise how sovereignty operates in cyberspace.

2. THE RELATIONSHIP BETWEEN SOVEREIGNTY AND TERRITORY IN CYBERSPACE

A. The Westphalian Concept of Sovereignty

Sovereignty is a foundational principle of public international law, with its origins going back to Jean Bodin, who understood it as the absolute and indivisible power of the sovereign to make and enforce laws binding his subjects.[8] In its classical form, it signifies *summa potestas, i.e*. the highest authority and the right to exercise its own judgment within a territory.[9] This authority within the State (internal sovereignty) refers to 'the State's exclusive right or competence to determine the character of its own institutions, to ensure and provide for their operation to enact laws of its own choice and to ensure their respect'.[10] By virtue of this sovereignty States have, *inter alia*, the right to: control access to their territory; exercise authority over all persons

7 During the 73rd Session of the UN General Assembly both the US and Russia, together with their respective allies, introduced draft resolutions relating to the further study of norms on responsible State behaviour in cyberspace. The US-sponsored resolution establishes a new Group of Governmental Experts to continue the work of previous GGEs, while the Russia-sponsored resolution establishes an open-ended working group acting on a consensus basis to further develop the rules, norms and principles of responsible behaviour of States in cyberspace. Instead of negotiating a compromise between the two proposals, the UNGA decided to adopt them both: *Developments in the field of information and telecommunications in the context of international security*, 11 December 2018, UN Doc. A/Res/73/27; *Advancing responsible State behaviour in cyberspace in the context of international security*, 2 January 2019, UN Doc. A/Res/73/266.

8 Jean Bodin, *Six Livres de la République* (Chez Jacques Du Puys, France, 1577); *See also* Daniel Lee, *Popular Sovereignty in Early Modern Constitutional Thought* (Oxford University Press 2016) 188.

9 PCIJ, *Customs Régime between Germany and Austria (Protocol of March 19th, 1931)*, Advisory Opinion, 1931 PCIJ Series A/B No 41, sep. opinion Judge Anzilotti at para 13.

10 Nkambo Mugerwa, 'Subjects of International Law' in Max Sorensen (ed), *Manual of Public International Law* (Macmillan 1968) 253.

and things within their territory as well as over their citizens at home and abroad; enact and enforce laws; and determine the State's political and economic system.[11]

The second requirement of sovereignty (in the Westphalian sense), closely linked to the notion of authority, is territory.[12] In its basic meaning, territory is first and foremost a geographical and spatial construct[13] relating to a physical area of the globe.[14] However, in relation to the concepts of statehood and sovereignty, territory ceases to be only a geographical description and instead becomes a legal and political construct.[15] In its interaction with authority, territory is not only the object of sovereignty, but also the spatial framework in which power and authority are manifested.[16] Competences of a State which flow from its sovereignty, such as jurisdiction, are manifest in largely territorial terms.[17] Moreover, it also functions as the 'container' for sovereignty, limiting its reach by drawing legal and political borders.[18] Territory's importance is such that even the notion of statehood is dependent on the nexus between a population which within a specified geographical space forms a community possessing an effective government.[19] The exclusivity of control over territory as a paramount condition for peace and stability[20] is thus protected against violations through the use of force (Art. 2(4) UN Charter), intervention into internal affairs,[21] as well as any other exercise of power within the territory of another State without that State's consent or the existence of a permissive rule.[22]

B. The Peculiarities of 'Territory' in Cyberspace

Given that the traditional understanding of sovereignty rests upon the exercise of authority within a geographical space, the question immediately arises how it can be applied to cyberspace – a global network of computers, including the information stored therein and the interactions between its users,[23] which is often perceived as

11 Samantha Besson, 'Sovereignty' in Rüdiger Wolfrum (ed), *Max Planck Encyclopaedia of Public International Law* (Oxford University Press 2011) para 118ff.

12 Territory has even been described as 'perhaps the fundamental concept of international law', *see* Malcolm N Shaw, 'Territory in International Law' (1982) 1 Netherlands Yearbook of International Law 17, 62.

13 Sara Kendall, 'Cartographies of the Present: "Contingent Sovereignty" and Territorial Integrity' (2016) 47 Netherlands Yearbook of International Law 83, 84.

14 Shaw (n 12) 61.

15 Tsagourias (n 3) 18.

16 Christian Marxsen, 'Territorial Integrity in International Law – Its Concept and Implications for Crimea' (2015) 75 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 7, 10.

17 Daniel Bethlehem, 'The End of Geography: The Changing Nature of the International System and the Challenge to International Law' (2014) 25 European Journal of International Law 9, 14.

18 Tsagourias (n 3) 17.

19 See Art. 1 *Montevideo Convention on the Rights and Duties of States*, LNTS No. 3802.

20 *Indo-Pakistan Western Boundary (Rann of Kutch)* (India v. Pakistan), Award, RIAA XVII 1, 571.

21 ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America); Judgment of 27 June 1986, ICJ Rep. 1986 p. 14, para 205.

22 '[T]he first and foremost restriction imposed by international law upon a State is that, failing the existence of a permissive rule to the contrary, it may not exercise its power in any form in the territory of another State', PCIJ, *S.S. Lotus* (France v. Turkey.), Judgment, 1927 PCIJ Ser. A No. 10, at p. 18.

23 Michael N Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013) 257.

a-territorial.[24] This problem, of course, is not new. Since the 1990s 'territorialists' and 'unterritorialists'[25] have debated whether cyberspace lies beyond the borders of existing States,[26] is akin to *res communis omnium*[27] or is subject to the jurisdiction of States because it operates on the basis of technical infrastructure within a specific geographic location.[28] As these debates are well-known, they need not be repeated for the purposes of this paper. Suffice it to recall that the distinctiveness of cyberspace is rooted in its 'layered' construction. The most popular models describe between three[29] and seven[30] layers,[31] which together create a space for interaction and communication characterised by three main features: interconnectedness, anonymity and ease of entry.[32] These features, in turn, contribute to the main distinction between cyberspace and traditional space: while the technical components which form the backbone of global computer networks have a unique physical location, their location is not perceived by the users of cyberspace. Rather, the impression of a distinct space is formed by the logical and social layers that construct a global platform for the exchange of information, services and activities, without regard for existing borders between States. Since the international community has declared the principle of State sovereignty to be applicable in cyberspace,[33] the question remains whether traditional principles and rules of sovereignty, such as the prohibition against violations of territorial sovereignty, extend to cyberspace unchanged or whether they need to be modified in order to account for the unique technical circumstances of cyberspace.

24 Tsagourias (n 3) 22.

25 Borrowed from Jennifer Daskal, 'Borders and Bits' (2018) 17 Vanderbilt Law Review 179, 181.

26 John P Barlow, 'A Declaration of the Independence of Cyberspace' (1996) <https://wac.colostate.edu/rhetnet/barlow/barlow_declaration.html> [accessed 11.03.2019]; David R Johnson and David Post, 'Law and Borders - The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367, 1370; Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperfections of International Law* (Martinus Nijhoff Publishers 2015) 91.

27 Darrel C Menthe, 'Jurisdiction in Cyberspace: A Theory of International Space' (1998) 4 Michigan Telecommunications and Technology Law Review 69, 93–94.

28 Jack Goldsmith and Timothy Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006) 73.

29 The three layer model, consisting of physical, social and logical layers has been first proposed by Yochai Benkler and is applied, with slight modifications, e.g. by the *Tallinn Manual 2.0* or the US military (which distinguishes between physical, logical and cyber-persona layers); see, respectively, Yochai Benkler, 'From Consumers to Users: Shifting the Deeper Structures of Regulation toward Sustainable Commons and User Access' (2000) 52 Federal Communications Law Journal 561, 561; Michael N Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 12 [hereinafter: *Tallinn Manual 2.0*]; Joint Chiefs of Staff, 'Cyberspace Operations, JP 3-12' (2018) I-2.

30 The Open Systems Interconnection (OSI) Model divides the process of data transmission into seven layers/steps: physical, data link, network, transport, session, presentation and application, see James E Goldman, 'Network Concepts' in Jerry C Whitaker (ed), *Systems Maintenance Handbook* (2nd edn, CRC Press) 17–1; some authors group these into five layers (geographical, physical, logical, cyber persona, persona), Dieter Fleck and Terry D Gill, 'Military Cyber Operations' in Dieter Fleck and Terry D Gill (eds), *The Handbook of the International Law of Military Operations* (2nd edn, Oxford University Press 2015) 458.

31 For the purposes of this paper I will apply the three-layer model as developed by Benkler and described by the Tallinn Manual 2.0.

32 Ido Kilovaty, 'Cyber Warfare and the Jus Ad Bellum Challenges' (2014) 5 National Security Law Brief 91, 94.

33 GGE Report 2013, para 20; GGE Report 2015, para 27.

C. The Tallinn Manual 2.0 approach to Sovereignty – the Primacy of Territorial Effects

The authors of the Tallinn Manual 2.0 seem to subscribe to the first view. They argue that 'the physical, logical, and social layers of cyberspace are encompassed in the principle of sovereignty'.[34] The most important feature is that 'cyber activities occur on territory and involve objects (…) over which States may exercise their sovereign prerogatives'.[35] In particular, even if cyber activities are conducted in such a way that they cross multiple borders, the acting individuals and entities remain subject to the jurisdiction of particular States.[36] In consequence, traditional notions of sovereignty are applied to conduct in cyberspace by way of a territorial analogy.[37] The primacy of territorial effects in the *Tallinn Manual 2.0* is best seen with regard to its approach to cloud computing. According to the *Manual*, operations against cloud infrastructure 'would generally not violate the sovereignty of other States that are affected by the operations unless the consequences that manifest in those States are of the requisite nature [*i.e*. with physical effects on the territory of the State – P.R.] as discussed in this Rule.'[38] Sovereignty over data stored abroad is rejected,[39] with an exception for government data under the 'inherently governmental functions' test.[40]

3. A 'LAYERED' APPROACH TO SOVEREIGNTY IN CYBERSPACE

A. Challenges to a Westphalian Understanding of Sovereignty in Cyberspace

Both the traditional understanding of sovereignty and recent State practice and *opinio iuris* are clear that sovereignty is primarily territorial. This means above all, as the *Tallinn Manual 2.0* points out, that States have the power to regulate ICT infrastructure, persons and activities located in their territory.[41] However, the *Tallinn Manual* underestimates the challenges to a territorial understanding of territoriality brought about by cloud computing, data partitionability and the mobility of ICT devices. The increasing use of cloud computing, understood as the 'storing by users of their infrastructure or content on remote servers',[42] allows companies and governments to move critical functions and services 'to the cloud' and run them from

34 *Tallinn Manual 2.0*, 12.
35 *Ibid*.
36 *Ibid* 12–13.
37 See, for example, for the rule prohibiting violations of territorial sovereignty: ibid 17; Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in Chcosristian Czosseck, Katharina Ziolkowski and Rain Ottis (eds), *4th International Conference on Cyber Conflict* (2012); Michael N Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 Texas Law Review 1639.
38 *Tallinn Manual 2.0*, 25.
39 *Ibid* 16.
40 *Ibid* 23.
41 *Ibid* 14.
42 Primavera De Filippi, Smari McCarthy, 'Cloud Computing: Centralization and Data Sovereignty' *European Journal for Law and Technology*, Vol. 3 No. 2, 2012.

ICT infrastructure usually grouped in large data centres located in a few key points around the globe,[43] often on the territory of another State. Due to a lack of technical restrictions for transborder data flows, data stored in the cloud can be partitioned, held in more than one location and moved between servers to reduce latency and facilitate access for customers. The move to the cloud regularly concerns communications and content data, but increasingly affects whole platforms and services in sectors such as banking[44] and even elements of critical infrastructure, such as remote terminal units, programmable logic controllers[45] or smart grid applications.[46]

If critical infrastructure such as industrial control applications or banking services, or governmental data and services, were to be stored in offshore data centres, the question arises as to the extent of each State's sovereignty. For instance, in case of a cyberattack against these data centres, would only the sovereignty of the State on whose territory the data centre is located be implicated, or would the de-territorialised sovereignty of the other State also be affected? Rather than conceptualising sovereignty in cyberspace exclusively by territoriality (in terms of location of ICT infrastructure), I would submit that there is emerging State practice to suggest that sovereignty in cyberspace may be understood as containing multiple spheres – or layers – of overlapping rights, responsibilities, and political authority.

1) Example 1: Asserting Jurisdiction Over Data Stored Abroad

Recent case law and legislation suggest that States treat remotely stored data and services as falling under their jurisdiction if they have a close connection to the territory of the regulating State. For instance, in *Google Spain*[47] the Court of Justice of the European Union (CJEU) held that the Data Protection Directive 95/46 grants an individual the right to request, under certain circumstances, that his or her personal data be no longer accessible through a search engine,[48] irrespective of the place where the actual data processing takes place, provided that the processing of personal data is carried out in the context of commercial activity on the territory of a Member State.[49]

In *Microsoft Ireland*, federal prosecutors sought and obtained a warrant for the search and seizure of information, including email, stored in a specified account hosted by Microsoft, to disclose the contents of e-mails of a suspect in an investigation related

43 For the location of Amazon's data centres, see Richard Fox and Wei Hao, *Internet Infrastructure. Networking, Web Services and Cloud Computing* (CRC Press 2018) 475.

44 Cary Springfield, 'The Impact of Cloud Computing on the Banking Sector' (*The International Banker*, 2018) <https://internationalbanker.com/banking/the-impact-of-cloud-computing-on-the-banking-sector/> [accessed 11.03.2019].

45 Áine MacDermott and others, 'Hosting Critical Infrastructure Services in the Cloud Environment Considerations' (2015) 11 International Journal of Critical Infrastructures 365, 371.

46 Bhaskar Prasad Rimal and Ian Lumb, 'The Rise of Cloud Computing in the Era of Emerging Networked Society' in Nick Antonopoulos and Lee Gillam (eds), *Cloud Computing. Principles, Systems and Applications* (2nd edn, Springer 2017) 14.

47 CJEU, *Google v. Mario Costeja González*, Case C-131/12, Judgement of 13 May 2014.

48 *Ibid*. para 98.

49 *Ibid*. paras. 55-57.

to drug trafficking.[50] On appeal, the US Court of Appeals for the Second Circuit (CoA) reversed the Magistrate's order,[51] but lower courts in other Circuits did not join with the Court of Appeals for the Second Circuit and granted search warrants in cases relating to, among others, Yahoo and Google e-mail accounts.[52] The issue was resolved by the adoption of the Clarifying Lawful Overseas Use of Data (CLOUD) Act on 22 March 2018, which requires service providers subject to US jurisdiction to produce data under an SCA warrant regardless of the location of the server where the data is stored.[53]

In response to the CLOUD Act, the European Commission proposed a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (EPO Regulation).[54] While in its *amicus curiae* brief in the *Microsoft Ireland* case the Commission argued for an interpretation of domestic law 'mindful of the restrictions of international law and considerations of international comity' by giving due regard to the principle of territoriality,[55] it addressed the issue of transborder access to electronic evidence in much the same way as the United States in the CLOUD Act – by allowing access to data stored in a third State. In its explanatory summary the Commission clearly states that the draft Regulation deliberately 'moves away from data location as a determining factor, as data storage normally does not result in any control by the state on whose territory data is stored'.[56] This is so, because data is no longer stored locally but made available on cloud-based infrastructure that is accessible from anywhere and service providers use decentralised systems to store data in order to optimise load balancing, while also often copying content in several servers distributed globally to speed up content delivery.[57]

2) Example 2: Data Embassies and the De-territorialisation of Governmental Functions

The proliferation of cloud computing not only offers benefits to consumers and the private sector, but also opens opportunities for governments with respect to the performance of State functions. A quick survey shows that many State organs and

50 US District Court (S.D. New York), *In Re Warrant to Search a Certain E-Mail Account*, 15 F.Supp.3d 466 (2014), 468.

51 US Court of Appeals (2d Circuit), *Microsoft Corp. v. USA (In Re Search Warrant)*, 829 F.3d 197 (2016).

52 US District Court, E.D. Pennsylvania, *In re Search Warrant No. 16-1061-M to Google*, 232 F. Supp. 3d 708 (2017); US District Court, E.D. Wisconsin, *In re: Information associated with one Yahoo email address that is stored at premises controlled by Yahoo, In re: Two email accounts stored at Google, Inc*., Case Nos. 17-M-1234, 17-M-1235, 21 Feb. 2017.

53 Jean Galbraith, 'Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data' (2018) 112 American Journal of International Law 486, 487.

54 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, 17 Apr. 2018, Doc. COM(2018) 225 final [hereinafter: Draft EPO-Regulation].

55 US Supreme Court, *United States v. Microsoft Corp*., No. 17-2, Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party, p. 6-7.

56 Draft EPO-Regulation, Explanatory Memorandum, p. 13.

57 *Ibid*. p. 14.

governmental agencies already employ cloud-based web services. For instance, the company Amazon offers hosting solutions and web-based applications to governmental customers which include, *inter alia*, the US Department of State, the Department of Homeland Security, the UK Justice Department, the Government of Singapore and Europol.[58]

An early example where, to increase resilience, certain governmental functions were temporarily performed from ICT infrastructure located in a third State occurred during the Russian attack on Georgia in 2008, when a US internet service provider hosted the website of the Georgian President to better protect it against defacement and DDoS attacks.[59] However, maybe the most prominent example so far of moving certain State functions into the cloud is the Estonian 'data embassy' in Luxembourg.[60] Based on an agreement with the Grand Duchy of Luxembourg, Estonia acquired dedicated data centre space in Luxembourg for the purpose of hosting Estonian data and information systems.[61] Inspired by the Vienna Convention on Diplomatic Relations,[62] the agreement grants data stored in the data centre the status of archives and declares them inviolable, thus exempt from search, requisition, attachment or execution.[63] It further stipulates that assets used for the storage of data and information systems enjoy sovereign immunity.[64] While Estonia and Luxembourg found a treaty solution to the storage of governmental data abroad, even without a treaty one can argue that international law contains mechanisms 'that support the extension of a sovereign's right to inviolability of its data to the internet and cloud storage'.[65] Examples such as these seem to suggest that States might regard governmental data stored abroad as covered by their sovereignty, even though it is not stored on their territory. While no examples of cyberattacks against data embassies are known as of today, I would suggest that a cyberattack crossing the threshold of sufficient harm might indeed be regarded as a violation of the sovereignty of a State, because the State might regard the attack as infringing its exclusive authority.

58 Amazon, *Government, Education, and Nonprofits Case Studies*, <https://aws.amazon.com/solutions/case-studies/government-education/all-government-education-nonprofit/?nc1=f_ls> [accessed 11.03.2019].

59 Jason Healey, 'When "Not My Problem" Isn't Enough: Political Neutrality and National Responsibility in Cyber Conflict' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict. Proceedings* (NATO CCD COE 2012) 24.

60 E-Estonia, 'Estonia to open the world's first data embassy in Luxembourg', < https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/> [accessed 11.03.2019].

61 Loi du 1er décembre 2017 portant approbation du 'Agreement between the Grand Duchy of Luxembourg and the Republic of Estonia on the hosting of data and information systems', signé à Luxembourg, le 20 juin 2017, Annex, Doc. parl. 7185, [hereinafter: Data Embassy Agreement] <http://legilux.public.lu/eli/etat/leg/loi/2017/12/01/a1029/jo> [accessed 11.03.2019].

62 Bartłomiej Sierzputowski, 'The Data Embassy Under Public International Law' (2019) 68 International and Comparative Law Quarterly 225, 234.

63 Art. 6(2) Data Embassy Agreement.

64 Art. 5 Data Embassy Agreement.

65 Estonian Ministry of Economic Affairs and Communications, Microsoft Corp., 'Implementation of the Virtual Data Embassy Solution', <https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf> 14 [accessed 11.03.2019].

B. Layers of Sovereignty and the Criterion of Proximity

In the examples cited above, as well as in similar cases, we see a separation between the territory where the data is stored and the authority over the data. While the host State has jurisdiction over infrastructure and data located in it, the data usually does not affect its territory and therefore, as the EU Commission pointed out, it does not have an interest in regulating it.[66] The interest lies with the State on whose territory the services are offered and/or the users are located. This creates concurrent jurisdictions: one based on the principle of territoriality of the ICT infrastructure storing the data, the other on the territorial availability of the offered services and the nationality or domicile of the data owner. I would therefore argue that, similarly to the Law of the Sea,[67] we might conceptualise cyberspace as consisting of different zones – or layers – of decreasing sovereignty, depending on the proximity to the sphere of exclusive authority, which forms the core of sovereignty.

The criterion of proximity should not be thought of in geographical terms; rather, it is the degree of connectedness of the data to the sphere of exclusive State authority. Similar to the criterion of a 'genuine connection' in *Nottebohm and Barcelona Traction*,[68] used to determine whether a State can assert extraterritorial jurisdiction,[69] it describes the degree of the link between the data or service stored abroad and the State. Proximity therefore does not establish an absolute test, but rather a relative one, depending on the concrete situation and the interests of the States involved. The following criteria established in cases relating to the extraterritorial access to data,[70] factors to determine proximity might include in cases of overlapping sovereignty claims: the degree to which the territory of a particular State is affected, the interests of the affected States, the location and nationality of the data owner, the principal territory the data is accessed from and targeted at, and in case of services the nature and extent of the service provider's ties to the particular State.

C. Mapping Layers of Sovereignty on the Layers of Cyberspace

Based on the criterion of proximity, several layers of sovereignty can be distinguished.

1) Baseline Sovereignty – Exclusive Authority of the Territorial State over ICT Components of the Physical Layer

With regard to the physical layer of cyberspace, the proximity to the State is absolute through the criterion of territory. This reflects the international consensus on the applicability of international law in cyberspace, established by the UN Group of Governmental Experts in its 2013 and 2015 Reports, which found that State

66 Draft EPO-Regulation, Explanatory Memorandum, p. 13.
67 Jon D Carlson and others, 'Scramble for the Arctic: Layered Sovereignty, UNCLOS, and Competing Maritime Territorial Claims' (2013) 33 SAIS Review of International Affairs 21, 23.
68 ICJ, *Nottebohm* (Liechtenstein v Guatemala), Judgment, (1955) ICJ Rep. 4 et seq; ICJ, *Barcelona Traction* (Belgium v Spain), (1970) ICJ Rep. 42.
69 Cedric Ryngaert, *Jurisdiction in International Law* (2nd edn, Oxford University Press 2015) 156.
70 Compare CLOUD Act, 18 U.S.C. §2703(3)(A)-(H).

sovereignty and rules of jurisdiction apply to ICT infrastructure located within State territory.[71] There is agreement on this point between most States, even those with otherwise differing views on cyberspace sovereignty such as the US[72] and China.[73] States regularly assert jurisdiction over components of the physical layer, for instance imposing regulatory standards or security requirements.[74] State authority over the physical layer components located on its territory is exclusive insofar as no other State is permitted under international law to prescribe and enforce rules regarding objects located within the territory of another State.[75] It may, however, be limited by international law if the exercise of exclusive authority over ICT infrastructure would cause harm to other States. If, for instance, States harbouring large Internet Exchange Points such as DE-CIX in Frankfurt or AMS-IX in Amsterdam were to exercise their authority to shut down these exchange points with the effect of disrupting internet traffic in neighbouring States, one might argue that this would violate the obligation not to knowingly harm the rights of other States,[76] as confirmed by the ICJ in *Corfu Channel*.[77]

2) Limited Authority over the Logical Layer

While the physical layer of cyberspace consists of ICT components and can thus be described in territorial terms, the logical layer, which consists of the codes and standards that drive physical network components and make communication and exchange of information between them possible,[78] is fundamentally a-territorial. Nevertheless, it is not free from considerations of sovereignty. The governance and allocation of critical resources making up the public core of the internet[79] – such as the allocation of IP addresses, domain names and the administration of root DNS servers – raises questions as to the extent of State authority over these functions. At present, these functions are being performed by the Internet Corporation for Assigned Names

71 GGE Report 2013, para 20; GGE Report 2015, para 27.

72 See Harold Hongju Koh, 'International Law in Cyberspace' (2012) 54 Harvard International Law Journal 1, 6; Brian Egan, 'Remarks on International Law and Stability in Cyberspace' (*Berkeley Law School, California November 10, 2016*).

73 People's Republic of China, 'International Strategy of Cooperation on Cyberspace', Chapter II Principle 2, <http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_2.htm> [accessed 11.03.2019].

74 Compare e.g. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.

75 '[T]he first and foremost restriction imposed by international law upon a State is that, failing the existence of a permissive rule to the contrary, it may not exercise its power in any form in the territory of another State', PCIJ, *S.S. Lotus* (France v. Turkey.), Judgment, 1927 PCIJ Ser. A No. 10, at p. 18.

76 On the no-harm rule in cyberspace see Katharina Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace* (NATO CCD COE Publications 2013) 165.

77 ICJ, *Corfu Channel Case* (United Kingdom v. Albania), Judgment, 1949 ICJ Rep. 4, 35.

78 Joint Chiefs of Staff, 'Cyberspace Operations, JP 3-12' (2018) <https://fas.org/irp/doddir/dod/jp3_12.pdf> I-3 [accessed 11.03.2019].

79 Dennis Broeders, 'Aligning the International Protection of "the Public Core of the Internet" with State Sovereignty and National Security' (2017) 2 Journal of Cyber Policy 366, 6 <https://doi.org/10.1080/23738871.2017.1403640>.

and Numbers (ICANN)[80] in a multi-stakeholder model of industry self-regulation.[81] Insofar as the US have transitioned control over key IANA functions to the global multi-stakeholder community, the authority of any State over the logical layer is limited to its role as one of the stakeholders. Under the current model, no State alone has sovereignty over the logical layer. However, States such as China and Russia fear that they do not have sufficient authority over core functions of those portions of globally connected networks located on their territory. It is for this reason that both China and Russia have made gaining control over internet governance a key part of their cyberspace strategies and included this principle as a key element of their definition of cyberspace sovereignty.[82] To this end, the Russian parliament has recently passed a bill aimed at creating a domestic Domain Name System, in order to be able to disconnect the Russian internet from the global internet exchange system.[83] Should Chinese and Russian efforts to replace the multi-stakeholder model with a multilateral model under the International Telecommunications Union[84] succeed, or should States choose to take over control over DNS servers and registries serving their territories, sovereignty over the elements of the logical layer necessary to run national networks would be restored.

3) Concurrent Sovereignty over Data Located on ICT Infrastructure in Another State

In cases concerning the sovereignty over data and services stored in the ICT infrastructure located in one State and offered in the territory of another State, it is appropriate to speak of concurrent sovereignty under the proposed model of 'layered sovereignty'. By virtue of the ICT infrastructure's location, the host State has a baseline sovereignty over the ICT infrastructure. However, concurrent sovereignty exists if the data stored within the ICT infrastructure is sufficiently proximate to the State asserting sovereignty. For instance, in the case of governmental data stored in data embassies, the layered model of sovereignty would permit two layers of sovereignty to exist: one of the territorial State over the ICT infrastructure, that is the physical layer, and another of the data holder State over the data, that is the logical (content) layer.

D. Practical Application

What, then, is the practical application of this theoretical model? In my view, there are two areas where a 'layered' conception of sovereignty might be useful. *First*, it would

80 On the role of the Internet Corporation for Assigned Names and Numbers (ICANN) see Scott J Shackelford, 'Defining the Cyber Threat in Internet Governance', *Managing Cyber Attacks in International Law, Business, and Relations* (Cambridge University Press 2014) 20.

81 Kal Raustiala, 'Governing the Internet' (2016) 110 American Journal of International Law 491, 501.

82 Sarah McKune and Shazeda Ahmed, 'The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda' (2018) 12 International Journal of Communication 21, 3839.

83 Katherine Landes, 'The "Iron Curtain" Is Close to Falling over the Russian Internet' (*International Policy Digest*, 2019) <https://intpolicydigest.org/2019/03/02/the-iron-curtain-is-close-to-falling-over-the-russian-internet/> [accessed 11.03.2019].

84 Adam Segal, 'Holding the Multistakeholder Line at the ITU' *Council on Foreign Relations Blog (2014)*, <https://www.cfr.org/report/holding-multistakeholder-line-itu> [accessed 11.03.2019].

allow the allocation of sovereignty over data stored or a service offered from abroad, provided there is sufficient proximity between the data/service and the State asserting jurisdiction. Should this data/service fall victim to a cyberattack, such an attack might be qualified as a violation of sovereignty of the attacked State irrespective of the fact that the territory of that State has not been affected. This is because such a State might have an overwhelming interest in asserting authority over the data in question, for example if it is government data (in the case of data embassies) or if the attacked service is considered as critical infrastructure, is controlling critical infrastructure within the territory of that State or is otherwise of significant importance for essential interests of that State (e.g. banking services). In these cases, the State whose remotely stored data was attacked could resort to countermeasures or the plea of necessity to counter the action in question, irrespective of the rights of the territorial State, whose sovereignty over the ICT infrastructure might also be affected. *Secondly*, the criterion of proximity might be a useful tool to assess the proportionality of countermeasures or the existence of an essential interest of a State which has been affected through the cyberattack. The greater the proximity of the attacked data to the State, the greater its essential interest in protecting it against violations of sovereignty.

4. CONCLUSION

In conclusion, in the post-Westphalian system, geography – 'the physical space of a State' – is at the very core of the concept of sovereignty.[85] However, the advance of modern technology in the 20th and 21st centuries and especially the emergence of cyberspace, with its transboundary, geography-defying quality,[86] have led to a steady decline of the function of territory to exclude the activities of other entities within the boundaries of a State.[87] Therefore a strict application of traditional rules flowing from the principle of sovereignty, especially the rule of territorial sovereignty, would overemphasise the notion of territoriality and disregard the practical challenges to state authority emanating from cyberspace, leading to an imbalance in the rights and obligations of States in favour of the State on whose territory ICT infrastructure is located. A model of layered sovereignty, while at present a proposal *de lege ferenda*, would restore the balance between rights and obligations by adjusting for overlapping rights, responsibilities, and political authority in cyberspace.

85 Bethlehem (n 17) 14.
86 *Ibid.* 18.
87 Shaw (n 12) 64–65.