Part I
Sovereignty

Error 404: No Sovereignty Analogy Found

Pia Hüsch

Abstract: The debate on the application of state sovereignty in cyberspace is complex and includes a range of issues, such as the governance of cyberspace, exercising jurisdiction in cyberspace, or the question of whether low-intensity cyber operations violate state sovereignty. Next to legal and political questions, technological details further complicate the analysis. Due to this complexity, authors often rely on the use of analogies to conceptualise their arguments. This chapter addresses the use of such analogies by examining two analogies made by legal scholars in the field, one referring to the law of the sea and the other to quantum physics. It argues that the two analogies are exemplary of a wider problem: either the referenced analogy remains superficial without contributing comparative insights to the debate, or the analogy is taken so far that it further complicates the assessment of the original subject matter. Given the difficulties of 'getting the analogy right,' this chapter concludes that the contribution of analogies in the sovereignty in cyberspace debate should not be over-estimated and that in light of the two examples studied, no adequate analogy clarifying the sovereignty in cyberspace debate could be found.

I. Introduction

Following the invention of the internet, more recent trends such as digitalisation, surveillance capitalism, and an increase in malicious cyber operations have all challenged the application of existing public international law to cyberspace. These challenges have not gone unnoticed, and international legal scholarship has covered a range of questions as to how existing rules and principles could be applied to cyberspace and, more generally, how the predominantly territorial understanding of existing international law finds application in cyberspace. To an unprecedented extent, cyberspace even challenges the understanding of what arguably constitutes 'a founding principle of the international legal order':[1] state sovereignty.[2]

The debate on the application of sovereignty in cyberspace is broad and complex and involves many aspects, such as the governance of cyberspace,

1 Samantha Besson, 'Sovereignty' in: Rüdiger Wolfrum (ed.), *MPEPIL* (online edn, Oxford: Oxford University Press 2011), para. 5.

2 Patrick Franceze, 'Sovereignty in Cyberspace: Can It Exist?,' A. F. L. Rev. 64 (2009), 1–42; Pallavi Khanna, 'State Sovereignty and Self-Defence in Cyberspace,' BRICS Law Journal 5 (2018), 139–154; Michael Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace,' Tex L. Rev. 95 (2017), 1639–1676.

exercising jurisdiction in cyberspace, or the question of whether low-intensity cyber operations violate state sovereignty. Next to legal questions, which are closely related to political considerations, quickly developing and complex technological details further complicate the analysis. For these reasons, it is at times difficult to keep up with the sovereignty in cyberspace debate and to analyse the application of sovereignty to cyberspace in terms that are easily understandable to readers. Regularly, authors thus rely on the use of analogies to illustrate their arguments, raising the question of whether the use of analogies actually contributes to the scholarly debate on the application of sovereignty in cyberspace.

The following chapter addresses this question and therefore takes a closer look at what constitutes sovereignty in cyberspace debate. Even though the understanding of state sovereignty continues to vary amongst the discussants, the debate has seen recent trends in the last few years that will be set out in the second part of this chapter. In a third section, this chapter will elaborate on how complex and broad the discussion is and identify a range of key issues in the debate. Such complexity has led many scholars in the cyberspace debate to rely on analogies and metaphors to conceptualise the characteristics of cyberspace. In a fourth section, this chapter will introduce two of such analogies. Firstly, Roguski's 'Layered Approach,' an analogy to the maritime zones in the law of the sea, will be analysed.[3] Secondly, this chapter will consider Cornish's analogy with quantum physics in which he looks at how multiple interpretations of state sovereignty can co-exist.[4] The analogies chosen are considered suitable examples as they illustrate what is often the problem with choosing these analogies: they either remain superficial and do not genuinely provide comparative insights or add more complexity by providing a very detailed analogy without adding clarity to the original subject matter. Given the difficulties of 'getting the analogy right,' this chapter concludes by arguing that the value of analogies in the cyber debate should not be over-estimated. What the sovereignty in cyberspace debates needs instead is clarity, straightforwardness, and precision as opposed to hiding arguments behind unclear metaphors and insufficiently explored analogies.

3 Przemyslaw Roguski, 'Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment,' 11th International Conference on Cyber Conflict, NATO CCD COE Publications (2019), https://ccdcoe.org.

4 Paul Cornish, 'Governing Cyberspace through Constructive Ambiguity,' Survival – Global Politics and Strategy 57 (2015), 153–176.

II. The Application of Sovereignty in Cyberspace

State sovereignty is a concept that is highly relevant to the cyberspace debate as it potentially plays a crucial role in the regulation of many aspects of cyberspace, such as the governance of cyberspace, matters of jurisdiction, or the regulation of low-intensity, inter-governmental cyber operations. Given the widely held consensus that international law applies to cyberspace[5] and the absence of a comprehensive international cyber treaty – and the unlikeliness that there will be one for the foreseeable future[6] – the application of existing public international legal norms has received widespread attention in legal scholarship.[7]

However, it remains far from clear how sovereignty applies in cyberspace exactly. One example of uncertainties with respect to the application of sovereignty in cyberspace is the question of whether disruptive cyber operations[8] falling below the use of force and non-intervention thresholds

---

5 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereafter: UN GGE), 24 June 2013, UN Doc A/68/98, para. 19. This was reconfirmed in 2015, UN GGE, 22 July 2015, A/70/174, para. 28(b).

6 On the topic of a cyber treaty generally and its feasibility in particular see Stephen Moore, 'Cyber Attacks and the Beginning of an International Cyber Treaty,' N.C.J. Int'l L. & Com. Reg. 39 (2013), 223–257, (250 ff.), in reference to Russia and the US he argues that 'it is becoming increasingly less likely that the two states would have interest in negotiating a cyber treaty. […] Any viable cyber treaty will need agreement or at least mutual respect from the two states.,' (252–253). See also more recently, arguing 'that the collapse of the UN GGE process is likely to lead to a shift away from ambitious global initiatives and towards regional agreements between 'like-minded states'.' Anders Henriksen, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace,' Journal of Cybersecurity 5 (2019), 1–9 (1).

7 See e.g. Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Cham: Springer 2017); Harriet Moynihan, 'The Application of International Law to State Cyberattacks – Sovereignty and Non-intervention,' 2 December 2019, https://www.chathamhouse.org; Oona A. Hathaway and others, 'The Law of Cyber-Attack,' Cal. L. Rev. 100 (2012), 817–886 or Nicholas Tsagourias, 'Cyber attacks, self-defence and the problem of attribution,' Journal of Conflict & Security Law 17 (2012), 229–244.

8 Low-intensity cyber operations are operations that fall below the use of force and non-intervention threshold. Examples of operations that alter, disrupt or destroy computer systems are the Sony attack leading to the deletion of one hundred terabytes of Sony's data and furthermore the leak of confidential documents or the attack on the Sands Casino attributed to Iran which has caused significant financial damages and destroyed data as well as computer systems. See e.g. Beatrice A.

are regulated by state sovereignty as a primary rule of international law or whether sovereignty is merely a related principle yet not an alone standing rule.[9] Arguably, these difficulties in the application are rooted in a much older problem, namely that state sovereignty means everything and nothing at the same time, some calling it 'organised hypocrisy'[10], others naming it 'a funny thing' as '(i)t is allegedly the foundation of the Westphalian order, but its exact contours are frustratingly indeterminate.'[11] Indeed, there is no authoritative definition of sovereignty as there is also no common understanding of what constitutes state sovereignty.

Since Bodin first reshaped the idea of sovereignty to reflect no longer its medieval interpretation but a concept separated from a person who acts as the sovereign, the notion of sovereignty has been developed further over the centuries.[12] Nowadays, scholarly attempts to define state sovereignty are manifold, traditionally revolving around the idea of territoriality and exclusive authority. Besson refers to it as 'supreme authority within a territory,'[13] Schrijver notes that '(i)nternally it means that the government of a State is considered the ultimate authority within its borders and jurisdiction,' and adds an external component, i.e. 'that a State is not subject to the legal power of another State of any other higher authority.'[14] Similarly, Oppenheimer defines state sovereignty by stating that 'sovereignty is *independence*… As comprising the power of a state to exercise supreme authority over all persons and things within a territory, sovereignty involves *territorial* authority.'[15]

Many of such definitions could be added, yet all of them remain scholarly attempts to grasp what state sovereignty means as there is no

---

Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law,' Yale L.J. 126 (2017), 1460–1519.

9 Michael Schmitt and Liis Vihul, 'Sovereignty in Cyberspace: Lex Lata vel Non,' AJIL Unbound 11 (2017–2018), 213–218.

10 Stephen D. Krasner, *Sovereignty – Organized Hypocrisy* (Princeton: Princeton University Press 1999).

11 Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?,' Tex L. Rev. 95 (Forthcoming), Cornell Legal Studies Research Paper No. 17–15, (2017) https://papers.ssrn.com, 1.

12 Besson (n. 1), para. 16.

13 Besson (n. 1), para. 1.

14 Nico Schrijver, 'The Changing Nature of State Sovereignty,' BYIL 70 (1999), 65–98 (70–71).

15 Robert Jennings and Arthur Watts (eds), L Oppenheim, *Oppenheim's International Law, Vol 1: Peace* (9th ed, Oxford: Oxford University Press 2008), 382, quoted in Moynihan (n. 7), 11.

universal definition that states agree upon. Despite the fact that many of these definitions share a common core – that perhaps is even agreed upon by some states – the cyberspace debate challenges such definitions yet again, as it becomes evident that the terms territoriality, exclusive authority, and even independence have been challenged by the realities of complex interconnected cyberspace. As Schmitt and Vihul put it: 'On its face, the principle of sovereignty appears to be incompatible with cyberspace. Whereas sovereignty is an inherently territorial concept, cyberspace connects states in ways that seem to dilute territoriality. Nevertheless, the two phenomena have continued to exist in parallel since the emergence of cyber capabilities.'[16] In line with this observation, the following section thus takes a closer look at how the interplay of cyberspace and the principle of sovereignty have been approached so far and what issues have been identified by state practice as well as scholarship. For the purposes of this chapter, sovereignty is used as an umbrella term which, in line with Besson's definition, encompasses different rights and obligations.[17] Some of these rights and obligations are addressed in more detail, e.g., the right to exercise jurisdiction.

III. Different Approaches to the Application of State Sovereignty in Cyberspace

Against this backdrop of different definitions of state sovereignty and the challenge to apply these above-mentioned territorial concepts to cyberspace, it is evident that the issue of state sovereignty in cyberspace is part of an already extremely complex topic. The unique characteristics of cyberspace add yet another layer of difficulty to the challenge of understanding state sovereignty, leaving states in fundamental disagreement as to how to approach sovereignty in cyberspace. The following section will outline some of the approaches taken by key players in the cyber discussion, i.e., the US and like-minded states as well as China and Russia. This section does not aim to provide a comprehensive overview of all positions available but illustrates the broad range of approaches and priorities that can be taken with respect to sovereignty in cyberspace and how many areas and issues of international law and international relations can fall under the broad term of the 'sovereignty in cyberspace debate.'

16 Schmitt and Vihul (n. 9), 218.
17 Besson (n. 1), para. 118 f.

The first area where there are decisive differences is that of the regulation of the use of the internet and the regulation of free speech online. Often seen as a counter-position to the arguably more liberal US approach favouring strong protections of freedom of speech, China and Russia represent a view that strongly favours extending their territorial sovereignty to cyberspace. Despite the previously mentioned difficulties in understanding how territoriality plays out in cyberspace, China, Russia, and some other states push for an increasingly fragmented, territorial approach to the internet over which they can exercise exclusive authority. These positions are based on claims of state sovereignty, used in these instances to influence the interpretation of cyberspace in order to shape it in a way that is in line with the interests of authoritarian regimes. The reliance on state sovereignty has been used as a justification to impose strict regulations on the use of the internet and free speech online and to advance the fragmentation of cyberspace and is based on the idea of stressing the sovereign independence of each state and the principle of non-intervention, prohibiting outside interference in a state's internal affairs. Despite the fact that both China and Russia have at the time of writing not yet published a comprehensive analysis of how international law applies to cyberspace (as, for example, France,[18] Estonia,[19] and more recently, Germany[20] have), a practice already shows that their interpretations are restrictive, especially where the use of the internet is concerned.

In China, the use of the internet has been increasingly limited and controlled under President Xi Jing and is closely monitored by the Communist party. Those who advocated for reform behind what is now widely called 'The Great Firewall' and saw the internet as a tool to bring about political change in the communist state were soon silenced on the basis of what Xi calls 'China's sovereign right to determine what constitutes harmful content.'[21] Khanna notes that 'China's attempts to preserve its

18 French Ministry of Armies, 'International Law Applied to Operations in Cyberspace' (2019), https://www.justsecurity.org. For further analysis see Michael Schmitt, 'France's Major Statement on International Law and Cyber: An Assessment,' 16 September 2019, https://www.justsecurity.org.

19 Statement of the Estonian President at the International Conference on Cyber Conflict 2019 (2019), https://president.ee. For further analysis see Michael Schmitt, 'Estonia Speaks out on Key Rules for Cyberspace,' Just Security (2019), https://www.justsecurity.org.

20 Statement of the German Federal Government, 'On the Application of International Law in Cyberspace' (2021), https://www.auswaertiges-amt.de.

21 Elizabeth C. Economy, describing the Great Chinese Firewall as 'the largest and most sophisticated online censorship operation in the world,' in 'The Great Fire-

informational sovereignty by insulating its internet from Western websites are a clear example of how anxiety over sovereignty has been responsible for restrictions.'[22]

Russia has also tightened its regulation of the use of the internet. In May 2019, it passed a new 'Sovereign Internet Law,' a measure to 'protect Russia in the event of an emergency or foreign threat like a cyber attack.'[23] Behind what some consider the 'Online Iron Curtain,'[24] critics point out that Russia is increasingly aiming to disconnect its internet from global cyberspace, a step that it is allowed to take in case of a self-defined emergency.[25] To this end, Russia now routes its web traffic through state-controlled infrastructure and launched a national system of domain names. These measures might not be technically sufficient to completely isolate the Russian internet from the global internet, yet, allow the Kremlin to enforce online censorship[26] by blocking unwanted content according to 'usefully vague' criteria and without judicial consent.[27] This move has been heavily criticised by human rights advocates.[28]

The approaches followed by Russia and China exemplify practices to disconnect 'their' internet from global cyberspace. In addition to human rights concerns,[29] the fragmented approach advanced by several authoritarian states also fundamentally challenges the idea of global cyberspace. Although some have pointed to the technical difficulty to realise the fragmented approach to cyberspace,[30] Chinese internet policy shows how a large share of the world's population can effectively be put under severe

---

wall of China: Xi Jinping's internet shutdown,' 29 June 2018, https://www.theguardian.com.

22 Pallavi Khanna, 'State Sovereignty and Self-Defence in Cyberspace,' BRICS Law Journal 5 (2018), 139–154 (144).

23 Elizabeth Schulze, 'Russia just brought in a Law to Try to Disconnect its Internet from the Rest of the World,' 1 November 2019, https://www.cnbc.com.

24 Schulze (n. 23).

25 Sarah Rainsford, 'Russia Internet: Law Introducing New Controls Comes Into Force,' 1 November 2019, https://www.bbc.co.uk.

26 Schulze (n. 23).

27 Rainsford (n. 25).

28 Human Rights Watch, 'Russia: New Law Expands Government Control Online,' 31 October 2019, https://www.hrw.org.

29 Kenneth Roth describes China as 'an Orwellian high-tech surveillance state' with a 'sophisticated internet censorship system to monitor and suppress public criticism' in 'China's Global Threat to Human Rights,' Human Rights World Report 2020, https://www.hrw.org.

30 The comments were made in respect to Russia's new sovereign internet law, Schulze (n. 23).

restrictions – a practice that exemplifies how the internet is shaped from a global to a fragmented network – a development which is justified by claims of relying on state sovereignty.

A second related area where there is disagreement on how state sovereignty should play out in cyberspace relates to the question of governance of cyberspace. Whereas China and Russia support a state-centred approach in favour of negotiating a new international cyber treaty by traditional diplomatic means as they perceive them as a sovereign state's prerogative, many other states are of the opinion that existing international law is sufficient to regulate cyberspace and instead of negotiating a new treaty amongst states, they favour a multi-stakeholder approach for the regulation of cyberspace.[31]

These different approaches are also reflected within the UN, which set up two working groups that enjoy similar mandates to work on the regulation of cyberspace. On the one hand, there is the UN Open-Ended Working Group (OEWG), in which Russia enjoys support for its pro-sovereignty efforts, which have previously been backed by countries such as China, Brazil, India, Iran and Nigeria.[32] On the other hand, there is the US led UN Governmental Group of Experts (UN GGE),[33] which is backed by liberal democracies such as Australia, France and the UK.[34]

In these platforms, it becomes evident that the differences between states concern much broader aspects of cyberspace than the exact definition of state sovereignty, and that much depends on how sovereignty is to be applied and the different priorities states follow in their national interests. Some even argue that with the most recent developments in the UN mandates, i.e., the OEWG publishing its final substantive report on 12 March 2021[35] and the UN GGE's 2021 report,[36] the two working groups are, in fact, coming closer to finding similar conclusions.[37]

---

31 Cornish (n. 4), 161.

32 Justin Sherman and Mark Raymond, 'The U.N. Passed a Russian-backed Cybercrime Resolution. That's not Good News for Internet Freedom,' 4 December 2019, https://washingtonpost.com.

33 Samuele De Tomas Colatin, 'A Surprising Turn of Events: UN creates two working groups on cyberspace,' https://ccdcoe.org.

34 Sherman and Raymond (n. 32).

35 UN OEWG, 'Final Substantive Report,' (12 March 2021), UN DOC A/AC.290/2021/CRP.2.

36 Available here as an advanced copy, UN GGE, 'Report of the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security,' (28 May 2021).

The relationship between the two mandates certainly remains subject to further analysis. For the purposes of this chapter, it suffices to say that even where differences remain, the reality is that the differences in interpretation do not necessarily overlap with more traditional lines of geopolitics. Whereas it is true that Western states are generally following similar approaches supporting their interpretation of free speech and advocate for free flow of information online, even France and the UK do not agree when it comes to the third issue concerning sovereignty in cyberspace, i.e., the nature of sovereignty in cyberspace. When the UK put out their statement regarding the interpretation of international law in cyberspace in May 2018,[38] it became evident that its position is not necessarily shared by other Western countries. According to the British interpretation, sovereignty does not amount to a self-standing rule of international law. As sovereignty is merely a principle, an intrusive cyber operation that does not amount to a violation of the non-intervention principle (or the prohibition of the use of force) does not constitute an international wrong.[39] In contrast, the French interpretation of international law in cyberspace argues that 'any cyber attack against French digital systems or any effects produced on French territory by digital means […] constitutes a breach of sovereignty,' implying that sovereignty constitutes a self-standing rule of international law and consequently, all violations thereof amount to a wrongful act.[40] These two statements represent the two positions at the ends of the sliding scale of the principle-vs-rule debate, one of the key discussions in legal scholarship on the topic of sovereignty in cyberspace.[41] In recent years, more and more states have published their interpretation on the matter, many agreeing on sovereignty as a rule assessment. However, differences remain with respect to the exact threshold needed to violate

37 This impression arises given that the UN OEWG confirmed in its final report that it is indeed based on the findings of the UN GGE's previous reports of 2010, 2013 and 2015. However, differences also remain: for example, the OEWG does not explicitly endorse the multistakeholder approach nor does it go into depth on the application of international law to cyberspace. For more, see e.g. Pavlina Ittelson and Vladimir Radunovic, 'What's new with cybersecurity negotiations? UN Cyber OEWG Final Report analysis,' 19 March 2021, https://www.diplomacy.edu.

38 UK Attorney General Jeremy Wright, 'Cyber and International Law in the 21st Century,' 23 May 2018, https://www.gov.uk.

39 Wright (n. 38).

40 French Ministry of Armies (n. 18), 6–7.

41 See e.g. Gary Corn and Robert Taylor, 'Symposium on Sovereignty, Cyberspace, And Tallinn Manual 2.0,' AJIL Unbound 111 (2017), 206–212 or Schmitt and Vihul (n. 9), 213–218.

state sovereignty – a matter that Schmitt calls 'the real task at hand,' which has been addressed more explicitly by the recent German statement.[42]

Finally, a fourth issue that determines the sovereignty in cyberspace debate is that of jurisdiction. Due to the general demand for international law to apply to cyberspace, the internet, to a certain extent, has to match the understanding of existing international law. With respect to the application of the principle of sovereignty and the exercise of jurisdiction, in particular, this means that the importance of territorial or physical aspects of cyberspace is often overstated.[43] Such over-reliance on physical aspects stresses that servers, computers, and other components of communication infrastructure are physically located in a country. On the one hand, such assertion makes a valid point, especially with respect to the establishment of the respective state's jurisdiction.[44] The UN GGE confirmed that states enjoyed jurisdiction with respect to such items of infrastructure in 2013.[45] It also reflects common practice according to which 'states regularly assert jurisdiction, both civil and criminal, over activities within their cyber infrastructure.'[46] On the other hand, overreliance on territorial aspects of activities in cyberspace does not solve the problem that cyber activities often function without a straight-forward territorial connection. This is especially true as offensive cyber operations can 'be mounted from a multitude of globally dispersed locations,'[47] but also affects cloud services and increasingly also applies to state functions conducted via cyberspace.[48] Thus, it has been noticed by Corn and Jensen that cyberspaces have 'at most a tenuous connection to geography.'[49] It follows that 'territorial con-

42 For further analysis see Michael Schmitt, 'Germany's Positions on International Law in Cyberspace Part I,' 9 March 2021, https://www.justsecurity.org.

43 See for example Roguski's criticism of Rule 4 of the Tallinn Manual 2.0, applying an effects-based analysis which 'overemphasizes physical effects on territory' and 'does not sufficiently take into account the technical side of most cyber operations,' Przemyslaw Roguski, 'Violations of Territorial Sovereignty in Cyberspace – an Intrusion-based Approach' in: Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace – Behavior, Power, and Diplomacy* (London: Rowman & Littlefield 2020), 65–84 (74).

44 Khanna (n. 2), 143, referencing Catherine Lotrionte, 'State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights,' Emory Int'. L. Rev. 26 (2012), 825–919 (829).

45 UN GGE A/68/98 (n. 5), para. 19–20.

46 Roguski, 'Violations of Territorial Sovereignty in Cyberspace' (n. 43), 72.

47 Roguski. (n. 43), 68–69, referencing Gary Corn and Eric Jensen, 'The Technicolor Zone of Cyberspace, Part 2,' 8 June 2018, https://www.justsecurity.org.

48 Roguski, 'Layered Sovereignty' (n. 3), 6–9.

49 Corn and Jensen (n. 47).

cepts are not readily transposable to an aterritorial medium by way of simple analogy.'[50]

The four different areas of priorities and the positions established by states, may it be by their practice or set out in statements, as well as scholarly debates show that the internet has clearly challenged the way state sovereignty is understood and that particularly the application of the ultimately territorial principle of sovereignty to largely a-territorial cyberspace remains a decisive challenge which is part of a broader, complex puzzle that plays out in many different ways.

IV. Using Analogies to Analyse the Application of State Sovereignty in Cyberspace

Against this backdrop of a broad and complex debate, scholarship has attempted to grasp the meaning of state sovereignty in cyberspace in a way that better reflects the plurality of interpretations of sovereignty but also one that explains the complexity of the topic by using analogies. In the remaining parts of the chapter, two examples of approaches using an analogy to conceptualise different issues of sovereignty in cyberspace will be examined.

Firstly, Roguski's 'layered approach', which borrows from the law of the sea by establishing several layers of nuancing degrees of state sovereignty in cyberspace, will be analysed.[51] Secondly, Cornish's analogy with quantum physics will be examined, which argues that 'allowing different understandings and expectations of sovereignty to co-exist rather than conflict' could be the solution to the problem of how to regulate state sovereignty in cyberspace.[52]

Whereas these are only two of the analogies used in legal scholarship addressing the sovereignty in cyberspace debate, they are chosen as examples in this chapter as they represent what in the opinion of the current author is a more common problem: the use of analogies does not often make a contribution to the discussion, especially where the analogy remains under-explored or further complicates an already complex analysis.

---

50 Roguski, 'Violations of Territorial Sovereignty in Cyberspace' (n. 43), 68.
51 Roguski, 'Layered Sovereignty' (n. 3).
52 Cornish (n. 4).

1. Roguski and a 'Layered Approach' to State Sovereignty in Cyberspace

In a paper for the 11th International Conference on Cyber Conflict, Roguski proposes a 'Layered Approach' to find a suitable interpretation to the question of how sovereignty can be applied in cyberspace. Roguski suggests a gradual model of three layers.

Firstly, the model envisages a 'Baseline Sovereignty' layer, which constitutes the 'physical layer of cyberspace' in which the 'proximity to the State is absolute through the criterion of territory.'[53] Such the first layer comprises information and communication technologies (ICT) infrastructure, which are widely accepted to fall under the state's sovereignty and jurisdiction in which they are located.[54]

Secondly, he proposes a 'Logical Layer' over which states have limited authority. This essentially a-territorial layer 'consists of the codes and standards that drive physical network components and make communication and exchange of information between possible.'[55] This applies, for example, to the allocation of IP addresses and domain names.[56] As has been seen in reference to Chinese and Russian approaches to cyber sovereignty, the degree of authority states have over these functions depends on whether they are taking an approach similar to the Russian and Chinese model or whether they are following a multi-stakeholder approach – in the first case 'sovereignty over […] the logical layer […] would be restored.'[57]

The third layer of 'Concurrent Sovereignty over Data located on ICT Infrastructure in Another State' foresees that next to the hosting state, concurrent sovereignty would be established 'if the data stored within the ICT infrastructure is sufficiently proximate to the State asserting sovereignty.'[58] It applies a criterion of proximity, a flexible test that 'describes the degree of the link between the data or service stored abroad and the State.'[59]

Roguski's proposal deserves credit as he finds a way to apply existing terms such as the authority to the realities of cyberspace. It is also a practical approach in the sense that it proposes ways to establish jurisdiction

53 Roguski, 'Layered Sovereignty' (n. 3), 10.
54 Ibid. (n. 3), 10–11; UN GGE A/68/98 (n. 5), para. 20; UN GGE A/70/174 (n. 5), para. 27.
55 Roguski, 'Layered Sovereignty' (n. 3), 11, referencing Joint Chiefs of Staff, 'Cyberspace Operations, Joint Publication 3–12,' 8 June 2018.
56 Roguski, 'Layered Sovereignty' (n. 3), 11.
57 Ibid. (n. 3), 12.
58 Ibid. (n. 3),12.
59 Ibid. (n. 3), 10.

and finds compelling examples of application. Roguski further rightly draws attention to the widely used function of cloud services and their potential impact on questions of sovereignty and jurisdiction. He also successfully moves away from territoriality where necessary by replacing it with the proximity criterion, a flexible approach that allows for the degree of connection between state and data to be established. The model applies existing terms and concepts such as authority, the layered approach borrowed from the law of the sea and the proximity criterion, which bears similarities to the 'genuine connection' test to establish extraterritorial jurisdiction.[60] As such, the proposed approach seems plausible, especially as it conveys a sense of familiarity with established terms and approaches.

The analogy layered approach is, therefore, indeed a laudable starting point; however, a deeper analysis of the analogy seems necessary. Roguski's model borrows from the maritime zones established in the Law of the Sea Convention, but there is little engagement with the question of why this analogy was chosen and what the law of the sea approach implies for the sovereignty debate. The value of the United Nations Convention on the Law of the Sea (UNCLOS) arguably lies in the regulation of corresponding rights and obligations and how these are applied in each zone. It seems that Roguski's model only refers to the law of the sea in a superficial manner yet misses the decisive aspect of how and why the layered approach works on the sea and what insights for the application and understanding of sovereignty in cyberspace can be gained from drawing such an analogy to sovereignty at sea. He does not provide a deeper insight or more nuanced analysis on how rights and obligations would be applied in the different zones of cyberspace. The question of jurisdiction is, after all, only one of the aspects of sovereignty and the analogy to 'layered *sovereignty*' leaves room for exploring more rights and obligations that can be regulated by the application of layers.

This relates to a more general point. The fact that Roguski continues to use terms such as authority creates a sense of familiarity and places the proposal within the established lines of the discussion, yet also precludes a deeper discussion of these notions and the conceptual difficulties surrounding them. This is especially true for the term sovereignty, in which respect Roguski's analysis does not provide a conceptual understanding – one that could be compared to the understanding of sovereignty at sea given the use of the analogy in the first place.

---

60 Ibid. (n. 3), 10. For the genuine connection test, see ICJ, *Nottebohm* (Liechtenstein v. Guatemala), judgement of 6 April 1955, ICJ Reports 1955, 4 (para. 4 ff.).

This is reflected in the fact that Roguski's analysis leaves open some questions: despite the fact that his proposal addresses *who* and *when* a state can act when its data stored abroad is targeted (e.g., when a state has 'an overwhelming interest in asserting authority over the data in question'[61]), Roguski does not dig deeper on the question *why* exactly they can act. As he does not explicitly weigh in on the principle-vs-rule debate here, the question of whether the violation of sovereignty in these instances constitutes a wrongful act remains open. Roguski suggests that where a state storing data abroad is affected, 'an attack *might* be qualified as a violation of the sovereignty of the attacked State irrespective of the fact that the territory of the State has not been affected,' adding that it can resort to 'countermeasures or the plea of necessity.'[62] Given that he addresses the availability of countermeasures, one that is only the case where there is a wrongful act[63], his model of sovereignty seems to imply that the violation of state sovereignty constitutes a wrongful act and as such, sovereignty seems to be a rule. Clarification on the question of when such an act exactly constitutes a violation of sovereignty would be useful as it would offer further insights on how he understands the nature of sovereignty.

Interestingly, Roguski has more recently published a chapter in which he explicitly weighs in on the nature of sovereignty and concludes that sovereignty constitutes a self-standing rule.[64] Here, Roguski also elaborates on the threshold of when an offensive cyber operation violates the principle of sovereignty exactly, arguing this is the case not only where physical effects are caused but instead proposes an 'intrusion-based' approach, generally similar to the French model.[65] Despite the fact that Roguski envisages certain thresholds by categorising only those interferences that affect the integrity of data (e.g. by deleting or altering data), and not those that merely access them (e.g., for intended purposes or even by unauthorised access), as a violation of sovereignty, his approach remains broad.[66]

Overall, Roguski's analogy is an interesting starting point, but it would have allowed for more insights if the analogy to the layers of the law of the

61 Ibid. (n. 3), 13.
62 Ibid. (n. 3), 13.
63 ILC, 'Articles on the Responsibility of States for Internationally Wrongful Acts,' (2001) ILCYB, Vol II, Part Two, 31 ff.
64 Roguski, 'Violations of Territorial Sovereignty in Cyberspace' (n. 43), dismissing arguments that sovereignty is not a principle on page 68–69, concluding that 'sovereignty […] forms itself a prohibitive rule of international law.,' 71.
65 Ibid. (n. 43), 73 ff.
66 Roguski, 'Violations of Territorial Sovereignty in Cyberspace' (n. 43), 79.

sea was conducted more explicitly and if the analysis provided more comprehensive assessments of how the different rights and obligations play out in these layers. Whereas the analysis of the layered approach leaves open some questions which are answered in other publications, it would be interesting to see how Roguski's understanding of sovereignty explored in his second publication mentioned here relates to the interpretation of sovereignty at sea alluded to in the first publication.

2. Cornish and the Quantum Physics Analogy

Cornish's approach is of a more conceptual nature, providing the reader with an analysis exploring the different understandings underlying the sovereignty debate. To illustrate the variety of interpretations of sovereignty that co-exist, Cornish applies an analogy to quantum theory's superposition principle by referring to the experiment of Schrödinger's cat in which the pet is located in a box together with radioactive material as well as a radioactive monitor and a bottle of cyanide. The bottle of cyanide will eventually break due to the radioactive material in the box measured by the radioactive monitor, and as a result, the cat will die. The decisive bit is what follows: until someone opens the box to check on the status of the cat, 'the cat is notionally both alive and dead' or perhaps neither of the two options.[67]

Cornish applies this state of superposition to cyberspace by arguing that much of cyberspace is also 'both dead and alive' depending on the perspective you take: one might argue that information is hard as it is sent through cables, yet, on the other hand, it is non-physical, soft as it merely consists of digital code. He adds more examples of such 'dualities we might wish state sovereignty to occupy at once: national and international; procedural and substantive; international and external; intangible and physical; cultural and territorial.'[68]

So far, so convincing. Yet this plurality of interpretations of state sovereignty in cyberspace can only continue to exist if 'no one opens the lid' – and there continues to be a good reason not to do so. This is where the analogy becomes more complex. The aim, so Cornish, must be 'a reasonably unified, international policy for cyberspace as a 'virtual commons,' which can only be achieved if neither of the opposing views triumphs

67 Cornish (n. 4), 166.
68 Ibid. (n. 4), 166.

over the other, 'as the result would be neither unified nor common.'[69] This means that the lid must remain closed, so the reality does not show the incompatibility of the different approaches. Basing his argument on game-theory, Cornish argues that in order for the lid to remain closed, there must be a series of concessions made by the states of opposing position.[70]

Among the concessions listed by Cornish is the acknowledgement by states such as China that 'the multi-stakeholder approach is both more realistic and inclusive […] than intergovernmentalism'[71] and the acceptance that all norms developed 'should be respected both in letter and in spirit.'[72] In return, he sees concessions to be made by those advocating a multi-stakeholder approach, especially with respect to acknowledging that 'territorial sovereignty does bear upon many of the physical aspects of cyberspace,' respect the principle of non-intervention and that 'cyberspace is to provide a neutral medium for communication and cooperation among many different actors, rather than serving as a vehicle for the homogenisation of politics according to Western values, the enforcement of international standards of human rights around the world or the spread of liberal-democratic, rule-of-law-based systems of government,' a concession he accepts as difficult to realise.[73]

In return for these concessions, Cornish expects several benefits to arise out of this trade-off. For 'non-Western' states, it will reconfirm that states are 'at the centre of the norm- and rule-setting processes,' which thus means that these norms can be expected to reflect 'the preferences of all interested parties, rather than a small selection of them.'[74] Cornish also believes that 'by surrendering their insistence on a thin, territorial understanding of sovereignty, governments should also expect a return to a thicker and deeper understanding, in which culture and 'internal sovereignty' are acknowledged and respected.'[75]

As benefits for those supporting a multi-stakeholder approach, Cornish claims that fragmented cyberspace will become unlikely and that 'a more transparent, rules-based system' should emerge, which in turn 'should also see less tolerance for 'plausibly deniable' yet problematic behaviors in cyberspace,' ultimately making cyberspace 'more stable and predictable'

69 Ibid. (n. 4), 167.
70 Ibid. (n. 4), 167.
71 Ibid. (n. 4), 168.
72 Ibid. (n. 4), 168.
73 Ibid. (n. 4), 169.
74 Ibid. (n. 4), 168.
75 Ibid. (n. 4), 168.

which would have positive economic effects.[76] He further argues that such concessions would make it more likely to involve other stakeholders, which eventually could lead to 'the development of a normative, even cosmopolitan, framework.'[77]

Cornish's paper provides international legal scholarship with an out-of-the-box analogy and raises fundamental, highly interesting points, especially with respect to China's understanding of sovereignty. Yet difficulties arise when applying Cornish's analogy to practice. Firstly, it is questionable why it is desirable to find a reason 'not to open a lid.' This seems in clear contradiction with the aim to clarify the application of international legal norms to cyberspace,[78] an action that would – as far as the current author understands – require us to open the lid. Even though some states might prefer the current legal grey zones in cyberspace, Cornish argues that the ultimate benefit of keeping the lid shut is clarity and stability – aims that could arguably be achieved more directly by opening the lid.

Secondly, it seems highly unlikely that either side would start making any concessions. It does not seem likely China and Russia would abandon their restrictive, fragmented approach to cyberspace, nor that the West would support such restrictive interpretation, especially given that access to the internet is increasingly understood as a human right.[79]

In order to explain why states would make concessions, Cornish refers to elementary game theory and a system of cooperation in order to achieve desired benefits.[80] Here, Cornish misses a decisive element of game theory, often best explained by the Prisoner's Dilemma. In an interrogation of two prisoners, each prisoner does not know for sure if the other prisoner is also going to remain silent; a prisoner is more likely to turn on one another, despite the fact that cooperation in the form of mutual silence would be beneficial.[81] They will only remain silent if they trust one another – or

76 Ibid. (n. 4), 171–172.

77 Ibid. (n. 4), 172.

78 Often the aim to clarify norms of state behaviour is equated with leading to more stability, see e.g. Zine Homburger, 'Conceptual Ambiguity of International Norms on State Behaviour in Cyberspace,' 4 April 2019, available at: https://eucyberdirect.eu, 9. On why clarity is desirable in cyberspace, see also Robert McLaughlin and Michael Schmitt, 'The Need for Clarity in International Cyber Law,' 18 September 2017, https://www.policyforum.net.

79 Catherine Howell and Darrell M. West, 'The Internet as a Human Right,' 7 November 2016, available at: https://www.brookings.edu.

80 Cornish (n. 4), 167.

81 For more on the Prisoner's Dilemma, see Steven Kuhn, 'Prisoner's Dilemma' in: Edward Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (online edn, Stanford:

have made an agreement before the interrogation to do so. With respect to Cornish's proposed concessions, the question arises why either party would start making these fundamental concessions.[82] Despite the fact that the long-term outcome might be beneficial, there is no established relationship of trust between the US and China.[83] As long as each state cannot trust the other that their concessions are binding and will be adhered to, the trade-off does not work or as the prisoner's dilemma shows: each prisoner will turn on the other. One way to establish a binding nature could, of course, be in the form of an international treaty – yet Cornish mentions no such step, although it is crucial in order for the reference to game theory to work and to find a rational incentive to keep the lid shut. Without negotiations, transparency or guarantees, these concessions seem to appear 'out of the blue,' making it difficult to see how this analogy could play out in practice.

Thirdly, the current author believes that such concessions are fundamental. Cornish sees them as an enabler to ultimately reach a 'framework for global cyber governance.'[84] It would be interesting to know more about where Cornish sees the benefit of such a model. Is keeping the lid shut merely a temporal solution to establish trust between both frontiers while they make one concession after the other? If one assumes that both sides are ultimately willing to make such fundamental concessions, would it not be more favourable to fully open the lid straight away and find a compromise as a whole? This is in line with the previous arguments, as the current author believes negotiations of a treaty to establish trust and accountability are vital to lead to concessions in the first place. Given the current state of negotiations within the UN working groups, it, of course, does not seem very likely that such negotiations would be fruitful. However, it could be argued that by keeping the lid shut, states like China and Russia will continue to work towards a fragmented model of cyberspace and violate human rights while the West will advance their

---

The Metaphysics Research Lab 2019), 2 April 2019, https://plato.stanford.edu/index.html.

82 Cornish (n. 4) says that 'China, […] would first have to concede that cyberspace should not (and logically cannot) be territorialised,' 168, yet he does not explain whether this is meant as a temporal assessment and if yes, why a first step would be taken by China and if so, on what basis.

83 This was the case when Cornish wrote his analogy (2015) as well as today (2021). For more see Council on Foreign Relations, 'U.S. Relations With China – 1949–2020' (2020), https://www.cfr.org/timeline/us-relations-china.

84 Cornish (n. 4), 172.

global, multi-stakeholder model – a development that is also unlikely to lead to more trust and consequently, will not encourage either party to make concessions.

Fourthly, it does not become clear how the concession that 'China, […] would first have to concede that cyberspace should not (and logically cannot) be territorialised'[85] does not result in the triumph of one side over the other – something, so Cornish earlier, that should be avoided.[86] Despite the fact that both sides have to make concessions that certainly can outweigh one another to some extent, it nevertheless seems that, ultimately, this specific concession would lead to triumph from a Western perspective. This argument in combination with Cornish's claim that cyberspace should not be territorialised[87] might be read as a confirmation that Cornish has indeed chosen a preference of which side should ultimately triumph.

Despite the fact that the current author finds it difficult to see how the model would apply in practice, Cornish ultimately achieves a critical point that Roguski's theoretical model does not explore to the same extent: he successfully shows that there is no agreement on the concept of state sovereignty – neither from a legal nor a cultural perspective – and that sovereignty is many – often contradictory – things according to different perspectives. Instead, Cornish shows that the difficulty in applying state sovereignty to cyberspace is not so much how we can translate 'territoriality' and 'authority' to cyberspace, but that there is no agreement on the concept of state sovereignty in the first place.

V. *Remarks on the Contribution of Analogies to the Sovereignty in Cyberspace Debate*

The work of the two authors examined allows the critical reader to explore key issues relating to the regulation of state sovereignty in cyberspace: the lack of a common understanding of state sovereignty and how to deal with such ambiguity, the concept of territoriality in cyberspace, and the question how current geopolitics can work towards a practical way of governing cyberspace.

85 Ibid. (n. 4), 168.
86 Ibid. (n. 4), 167.
87 Ibid. (n. 4), 168.

Nevertheless, the present analysis also shows the shortcomings of the two models explored. In addition to the content-related arguments raised in the previous analysis, the two analogies allow for reflections on the general contribution such analogies can make when discussing the application of international law to cyberspace as the two examples chosen are representative of two more common problems encountered when using analogies.

Firstly, the interdisciplinary analogy between international cyber law and quantum physics has artificial appeal but, in practice, compounds the complexities of an already immensely complex debate. Whereas the initial analogy between Schrödinger's cat and sovereignty is a thought-provoking comparison indeed, the further the analogy is taken, the less it helps to understand the debates around sovereignty in cyberspace. In order to fully comprehend the value and meaning of the analogies, the reader of Cornish's paper ideally is familiar with basic quantum physics, international law, particularly principles applying to cyberspace, and later game theory. It is easy to see how given the number of references and complexity of each field, respectively, one cannot see the wood for the trees. The nuances that could be conveyed with such analogy are simply hidden away behind ever more metaphors, analogies and references, and it is easy to get lost. The conclusion that must be drawn in this instance is that the interdisciplinary analogy did not contribute to clarifying a complicated matter. On the contrary, the reliance on the quantum physics analogy in combination with additional references to game theory complicated the matter further.

Secondly, almost the opposite can be said for the analogy to the law of the sea made by Roguski. Here, the reference remained of a relatively superficial nature, and the opportunity for a meaningful analogy was at least to some extent missed. The law of the sea analogy could make for a promising legal parallel. However, a deeper analysis of the understanding of sovereignty at sea and in cyberspace as well as of the idea of different zones or layers with varying degrees of rights and obligations, i.e., a closer parallel to the law of the sea analogy, could have made a bigger contribution to the analysis at hand.

This is not to say that analogies generally cannot contribute to the quality of academic debate. On the contrary, they can improve the understanding of an issue, encourage readers to look for approaches and solutions applied in different fields and benefit from the experience made elsewhere. One example of how analogies in the cyberspace debate can contribute to a meaningful analysis is where cyberspace is compared to global commons,

as such analogy can lead 'to some useful comparative insights.'[88] Mueller's analysis of whether cyberspace should be a global commons like the high seas works well as it is a clear yet limited reference with the defined purpose of illustrating the relationship between the two domains.[89]

However, '[t]here are always difficulties' when using (interdisciplinary) analogies.[90] Such assessment also applies to situations where sovereignty in cyberspace is compared to other areas of international law. The challenge of finding an appropriate analogy lies in striking the right balance between mere superficial reference and becoming overwhelmed by complex details. Ultimately, 'it is only possible to analogise so far before analogy fails.'[91] In an area like sovereignty in cyberspace that is already dominated by legal grey zones, uncertainty, and the difficulty of combining legal and technical expertise, what the discourse urgently needs is clarity, comprehensible approaches and sharp analysis that ideally combines technical as well as legal perspectives instead of more analogies and metaphors.

For many years, scholars in the field regularly concluded that what is needed is more insights into state practice.[92] Although such a need remains to some extent, we have recently seen more and more states coming forward with their interpretation of how international law should apply to cyberspace.[93] Especially in the context of the two UN working groups, states have publicly stated their positions, fostering the debate on how sovereignty can be applied to cyberspace. These new statements are important,[94] and some are even of 'normative sophistication.'[95] International legal scholars have waited for such clarity for a long time – and should respond by offering the same clarity in return. To this end, adding to uncertainties by getting lost in analogies that over-complicate the matter or that are not followed through with has to be avoided. The discourse will

88 David Betz and Tim Stevens, 'Analogical Reasoning and Cyber Security,' Sec. Dialogue 44 (2013), 147–164 (151–152).

89 Milton L. Mueller, 'Against Sovereignty in Cyberspace,' International Studies Review 22 (2020), 779–801.

90 Betz and Stevens (n. 88), 156.

91 Betz and Stevens (n. 88), 158.

92 E.g. Eric Talbot Jensen, 'The Tallinn Manual 2.0: Highlights and Insights,' Geo. J. Int' l L. 48 (2017), 735–778 (743).

93 See e.g. n. 18, 19, 20.

94 Przemyslaw Roguski, 'The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States,' 11 May 2020, https://www.justsecurity.org.

95 Michael Schmitt, 'Finland Sets Out Key Positions on International Cyber Law,' 27 October 2020, https://www.justsecurity.org.

only benefit from direct analysis to understand technical and legal aspects of the question of how sovereignty can play out in cyberspace. Therefore, analogies should be used with caution.

VI. Conclusion

The debate surrounding the application of state sovereignty to cyberspace is a complex one. The present analysis has shown that not only is there no authoritative definition of state sovereignty in the first place, but that its application to cyberspace is especially challenging given the discrepancy between the traditional concept of state sovereignty which is often understood to be of a territorial nature and the fact that cyberspace is commonly perceived to be a territorial. In addition, this chapter has illustrated that states approach the sovereignty in cyberspace according to their national interests, e.g. by using the principle of state sovereignty as a justification for political acts or whether they lobby for a distinctive way how to approach governance and administration of cyberspace.

With these complexities in mind, legal scholarship has tried to analyse the subject matter – often with the help of analogies. After all, analogies or references to other or related subject matters are useful to catch the reader's initial attention – hence this chapter's title: 'Error 404: No Sovereignty Analogy Found,' referring to the common error notification many internet users are familiar with. However, the two examples examined in this chapter show how difficult it is to find an analogy that actually contributes to the analysis and clarification of this complex topic. On the contrary, the two analogies examined here have illustrated that instead of striking the right balance, it is likely that a very detailed analogy adds further complexity to the topic and leads to additional confusion and that, in contrast, a superficial analogy does not lead to useful comparative insights either. Therefore, the chapter concludes that where an appropriate balance cannot be struck and an (inter-disciplinary) analogy does not contribute to the analysis at hand, scholars should consider writing their analysis on sovereignty in cyberspace without using analogies and instead, favour clear and straight-forward analysis. In that sense, at least in the light of the two examples studied, no adequate analogy clarifying the sovereignty in cyberspace debate could be found.