Anchoring Digital Sovereignty

Vivek Krishnamurthy*

Abstract

For a quarter-century, a consensus has prevailed that territorial sovereignty applies online as it does offline. Since practically all the Internet's infrastructure and its billions of users reside on the territory of states, conventional wisdom holds that sovereignty must extend to cyberspace. Such accounts ignore how people experience cyberspace as a distinctive place, and how current international law lacks safeguards to prevent states from exercising their sovereignty to splinter the Internet into a set of national networks. Territorial sovereignty is also hard to square with pledges by the world's democracies to keep the Internet free, open, and global; yet it is not the only way that international law knows to define the powers of a state.

Drawing from the law of the sea, this Article argues that we should anchor the nature of state authority in cyberspace in the limited sovereign rights that coastal states possess in the waters off their shores. Unlike the plenary powers that sovereignty vests in states over their entire land territory, a coastal state's sovereign rights weaken the further one goes out to sea, and they are subject to the rights of other states (and of their nationals) to engage in certain peaceful uses of such waters. By redefining state authority over cyberspace in terms of layers of sovereign rights that are subject to the digital rights of others, states can enact legitimate online regulations within international legal constraints that preserve the Internet's free, open, and global character.

* Associate Professor, University of Colorado Law School; Faculty Associate, Berkman Klein Center for Internet & Society, Harvard University. Many thanks to Myka Kollmann and Sebastian Blitt for their outstanding research assistance; to S. James Anaya, Mailyn Fidler, Asaf Lubin, Cymie Paine, Blake Reid, Donald Rothwell, and Peter Swire for their feedback on previous versions of this Article; to participants at the 2022 "Four Societies" Conference, the 2024 Law & Tech Workshop Series, and internal workshops at the Universities of Ottawa and Colorado for their insights; and to Regina Bateson, Anupam Chander, David Sloss, Rich Furman, Pratheepan Gulasekaram, Margot Kaminski, Molly Land, Marina Pavlović, and Penelope Simons for their guidance and support. Any remaining errors of fact or law are mine alone.

Table of Contents

I. INTRODUCTION 3
II. WHAT IS SOVEREIGNTY? 5
A. The Novelty of Sovereignty 6
B. Sovereignty and Jurisdiction 7
III. SCHOLARLY PERSPECTIVES ON SOVEREIGNTY IN CYBERSPACE 8
A. First-Generation Perspectives 9
B. Second-Generation Perspectives 11
C. Third Generation Perspectives 18
IV. GOVERNMENTAL PERSPECTIVES ON SOVEREIGNTY, CYBERSPACE, AND INTERNET FREEDOM 20
A. Government Views on Sovereignty in Cyberspace 21
B. Government Views on Internet Freedom 24
C. Are Territorial Sovereignty and Internet Freedom Reconcilable? 26
V. AN INTRODUCTION TO THE LAW OF THE SEA 28
A. The Concept of Sovereign Rights 30
B. Delineating Sovereign Rights at Sea 32
VI. ANCHORING DIGITAL SOVEREIGNTY IN THE LAW OF THE SEA 47
A. The Emergence of Domains in International Law 48
B. Land-based Technologies and Domains Beyond Land 51
C. Law of the Sea Lessons for International Cyberlaw 52
VII. CONCLUSION 60

I. INTRODUCTION

Early Internet scholarship viewed cyberspace as a separate place, well beyond the regulatory reach of the nation-state.[1] As John Perry Barlow stated in his famous *Declaration of the Independence of Cyberspace:*

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have *no sovereignty* where we gather. . . . Cyberspace does not lie within your borders.[2]

These idealistic notions of cyberspace as a realm beyond state control did not last long. The empire struck back, and states soon began to assert their jurisdiction over cyberspace by applying the territoriality principle (and its extraterritorial exceptions) to online activities. As Anupam Chander and Haochen Sun have recently observed, "[g]overnments have resoundingly answered first-generation Internet law questions of who, if anyone, should regulate the Internet. The answer: they all will. Governments now confront second-generation questions: not whether, but how, to regulate the Internet."[3]

In answering such questions, governments and scholars now treat the application of the traditional, territorial conception of sovereignty to cyberspace as a *fait accompli.* As Dan Svantesson has noted, "[w]hile it has not always been so, today, it is uncontroversial to suggest that sovereignty applies online."[4] Numerous governments have stated that sovereignty is a fundamental rule of international law[5] and that it applies online as it does offline.[6] The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* which represents the acme of legal thinking on the applicability of international law to cyberspace, declares that "the principle of State sovereignty applies in cyberspace" and that states "enjoy

1 The high-water mark of this view is reflected in David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

2 John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996) (emphasis added), https://perma.cc/2EBX-Z4YU.

3 Anupam Chander & Haochen Sun, *Digital Sovereignty as Double-Edged Sword, in* DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE 72, 72–73 (Anupam Chander & Haochen Sun eds., 2023).

4 Dan Svantesson, *A Starting Point for Re-Thinking "Sovereignty" for the Online Environment, in* DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE 49, 50 (Anupam Chander & Haochen Sun eds., 2023).

5 *See infra* Section IV.A.

6 Svantesson, *supra* note 4, at 59–60.

sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."[7]

Much scholarly and governmental effort is currently devoted to answering the "considerably more difficult question of *how* sovereignty applies online."[8] This Article argues, however, that now is the time to reconsider whether sovereignty is the most appropriate legal doctrine for conceptualizing state authority over the Internet, given the difficulty of reconciling the near-plenary nature of the authority sovereignty vests in states with the ambition of the world's democracies to preserve an "open, free, global, interoperable, reliable, and secure" Internet.[9]

While every government will seek to regulate the Internet, and national regulation is often normatively desirable,[10] this Article suggests that we should look to how governments assert their authority over the seas for a better model of how state power should be exercised in the online sphere. It argues that the concept of *sovereign rights*, which is used to describe the limited nature of the authority that states exercise over maritime areas off their shores, offers a better framework for thinking about how states should exercise their regulatory power in cyberspace.

Unlike territorial sovereignty, which vests states with vast and undifferentiated powers to regulate whatever happens on their territory, the law of the sea recognizes different configurations of sovereign rights that are subject to the rights of other states (and their nationals) to make certain peaceful uses of a state's maritime areas. Correspondingly, adapting the regime of sovereign rights to the challenge of governing cyberspace would allow for the nature of state power to be tailored to fit various scenarios while protecting the rights of all humanity to enjoy the benefits of a free and open global Internet.

This Article begins by defining "sovereignty" in the manner that international lawyers use the term before offering scholarly and governmental perspectives on the application of sovereignty to cyberspace. It then explores key aspects of the law of the sea that could be used to help reconceptualize the nature of state authority over the Internet. While the prevailing view is that international law as it is (*lex lata*) requires the application of territorial sovereignty to cyberspace in view of the physicality of its infrastructure, my hope is that this Article will get

7 TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 11 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

8 Svantesson, *supra* note 4, at 50.

9 A DECLARATION FOR THE FUTURE OF THE INTERNET, https://perma.cc/44JF-SXQZ (last visited June 27, 2024).

10 As Anupam Chander and Haochen Sun observe, government regulation of the Internet is "necessary to protect privacy, ensure consumer protection, promote competition, and enable law enforcement." Chander & Sun, *supra* note 3, at 73.

us thinking differently about what directions future law (*lex ferenda*) might take if we are truly serious about preserving the free, open, and global nature of the Internet.

II. WHAT IS SOVEREIGNTY?

Sovereignty is perhaps the most contested of the many "essentially contested concepts" that exist in international law.[11] The term has long been bandied as a political slogan, and its meaning in popular discourse often lies in the eye of the beholder. The word is "widely used—and not always used in the same way—by scholars, journalists, practical politicians, international civil servants, jurists, and others from widely divergent cultural traditions, professions, and intellectual disciplines."[12] Some speak of sovereignty in terms of a state's regulatory power, while others equate sovereignty with strategic autonomy.[13] For example, in deciding to ditch Microsoft Windows in favor of a custom version of the Linux operating system on its government computers, an official of the German *Land* of Schleswig-Holstein spoke of their decision in terms of enhancing their digital sovereignty by reducing their reliance on a foreign technology product.[14]

Sovereignty has been called "a bad word, not only because it has served terrible national mythologies; in international relations, and even in international law, it is often a catchword, a substitute for thinking and precision."[15] Even so, there is a conventional understanding of "sovereignty" in public international law that has informed scholarly and governmental discussions of its application to cyberspace. This is how I use the term in this Article.

According to this conventional understanding, sovereignty is a defining feature of the contemporary international system, which is premised on the existence of numerous states with clearly defined territories. Each state possesses sovereignty over its territory, and each enjoys formal equality under international law. In his authoritative exposition of the principles of public international law,

11 An "essentially contested concept" is one "the proper use of which inevitably involves endless disputes about their proper uses on the part of their users." *See* W. B. Gallie, *IX.—Essentially Contested Concepts*, 56 PROC. ARISTOTELIAN SOC'Y 167, 169 (1956).

12 Winston Nagan & Craig Hammer, *The Changing Character of Sovereignty in International Law and International Relations*, 43 COLUM. J. TRANSNAT'L L. 141, 142–43 (2004).

13 *See, e.g.*, THÉODORE CHRISTAKIS, "EUROPEAN DIGITAL SOVEREIGNTY": SUCCESSFULLY NAVIGATING BETWEEN THE "BRUSSELS EFFECT" AND EUROPE'S QUEST FOR STRATEGIC AUTONOMY 11–12 (2020), https://perma.cc/JQ93-DDUS (chronicling how European officials use the term "sovereignty" to mean both regulatory and strategic autonomy in elaborating the concept of "digital sovereignty").

14 *See Einstieg in den Umstieg* [*Getting Started with the Switch*], SCHLESWIG-HOLSTEIN (Apr. 3, 2024), https://perma.cc/3BX6-HXLT.

15 LOUIS HENKIN, INTERNATIONAL LAW: POLITICS AND VALUES 8 (1995).

James Crawford defines sovereignty as "the collection of rights held by a state, first in its capacity as the entity entitled to exercise control over its territory and, secondly, in its capacity to act on the international plane, representing that territory and its people."[16]

A. The Novelty of Sovereignty

We may now take it for granted, but organizing political authority around formally equal, territorially defined states is a recent development in the long arc of human history. The political scientist Robert Jackson has explained how "[s]overeignty is a historical innovation of certain European political and religious actors who were seeking to escape from their subjection to the papal and imperial authorities of medieval Europe and to establish their independence of all other authorities, including each other."[17]

Conventional accounts trace the origins of sovereignty to the 17th century and credit the writings of international law publicists such as Hugo Grotius, Jean Bodin, and Emer de Vattel in developing the concept, which gave rise to the modern, Westphalian system of states at the end of the Thirty Years' War.[18]

Other scholars have emphasized, however, that the development of a new technology—cartography—was necessary for the creation of the legal concept of territorial sovereignty.[19] These scholars chart how the advancement of modern cartography in the late Middle Ages enabled the conceptualization of space in terms that allowed political authority to be allocated based on bounded and clearly demarcated territories,[20] rather than on ties of kinship, language, and religion.[21]

Even today, the regime of territorial sovereignty is but one of four "spatial" regimes that exist in international law—that is, regimes that are used to organize

16 JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 432 (9th ed. 2019).

17 ROBERT H. JACKSON, SOVEREIGNTY: EVOLUTION OF AN IDEA 6 (2007).

18 *See generally* Daniel Philpott, *Sovereignty: An Introduction and Brief History*, 48 J. INT'L AFFS. 353 (1995). *See also* JACKSON, *supra* note 17. A similar conventional account of the origins of sovereignty can also be found in Sean Watts & Theodore Richard, *Baseline Territorial Sovereignty and Cyberspace*, 22 LEWIS & CLARK L. REV. 771, 827–32 (2018).

19 *See generally* JORDAN BRANCH, THE CARTOGRAPHIC STATE: MAPS, TERRITORY, AND THE ORIGINS OF SOVEREIGNTY (2013); Richard T. Ford, *Law's Territory (A History of Jurisdiction)*, 97 MICH. L. REV. 843 (1999).

20 *See* BRANCH, *supra* note 19. I will return to this theme later in the paper in exploring how technological change often drives the development of new forms of political organization—including the rise of the modern law of the sea. *See infra* Sections V, V.B.4.

21 *See, e.g.*, DAVID E. WILKINS, INDIGENOUS GOVERNANCE: CLANS, CONSTITUTIONS, AND CONSENT 32–33 (2024) (describing the importance of kinship and other ties in defining political community among the Indigenous peoples of North America).

authority over physical spaces on our planet (and beyond).[22] The two most important of these others are *res nullius* and *res communis,* while the last is a *sui generis* residual category comprising "territory not subject to the sovereignty of any state or states and which possesses a status of its own"[23] such as the former United Nations trust territories.[24]

Res nullius refers to areas "legally susceptible to acquisition by states but not as yet placed under territorial sovereignty."[25] Antarctica is a leading example of a *res nullius* today as its territory could be acquired by states but for the provisions of the Antarctic Treaty, which freeze all such claims until 2048.[26]

Res communis, by contrast, refers to spaces and places that are "not capable of being placed under sovereignty."[27] Crawford offers the high seas and outer space as examples of *res communis* as things stand right now,[28] although this is susceptible to change over time.

B. Sovereignty and Jurisdiction

Sovereignty and the sovereign equality of States give rise to three corollaries in international law, according to Crawford: "(1) a jurisdiction, prima facie exclusive, over a territory and the permanent population living there; (2) a duty of nonintervention in the area of exclusive jurisdiction of other states; and (3) the ultimate dependence on consent of obligations arising whether from customary law or from treaties."[29]

Jurisdiction is the "legal mirror image of the principle of sovereignty."[30] The term refers to "a state's competence under international law to regulate the conduct of natural and juridical persons."[31] The starting point of the law of jurisdiction is "the presumption that jurisdiction (in all its forms) is territorial, and may not be exercised extraterritorially without some specific basis in international law."[32]

22 CRAWFORD, *supra* note 16, at 191–92.

23 *Id.*

24 *Id.*

25 *Id.*

26 *See generally* Christy Collis, *Territories Beyond Possession? Antarctica and Outer Space*, 7 POLAR J. 287 (2017).

27 CRAWFORD, *supra* note 16, at 191–92.

28 *See id.*

29 *Id.* at 431.

30 Cedric Ryngaert, *International Jurisdiction Law*, *in* RSCH. HANDBOOK ON EXTRATERRITORIALITY IN INT'L L. 13, 13 (Austen Parrish & Cedric Ryngaert eds., 2023).

31 CRAWFORD, *supra* note 16, at 440.

32 *Id.*

International lawyers distinguish between prescriptive jurisdiction ("the power to make laws, decisions or rules") and enforcement or adjudicative jurisdiction ("the power to take executive or judicial action in pursuance of or consequent on the making of decisions or rules.")[33] Current international law recognizes four bases upon which prescriptive jurisdiction may be exercised by a state outside its territory,[34] but in principle "extraterritorial enforcement jurisdiction is outright prohibited."[35] Exercises of enforcement jurisdiction by the agents of one state on the soil of another—such as arresting someone or seizing evidence—are viewed as grave violations of the second state's sovereignty unless they are preauthorized.[36] However, the rise of the Internet and the growing importance of electronic evidence in both civil and criminal matters has raised questions of whether "remote access to digital data . . . constitute[s] a violation of the prohibition of extraterritorial enforcement jurisdiction."[37] Hence, in our digital age, as Crawford notes, "what amounts to extraterritorial jurisdiction is increasingly a matter of appreciation."[38]

The next two Sections of this Article will explore a wider range of scholarly and governmental perspectives on the application of sovereignty and its corollaries to cyberspace. What will emerge is that applying traditional notions of territorial sovereignty to the Internet is hard to square with its survival as a free, open, and global network.

III. SCHOLARLY PERSPECTIVES ON SOVEREIGNTY IN CYBERSPACE

Over the last three decades, three generations of scholars from the emerging field of cyberlaw and the long-established field of international law have considered the relationship between sovereignty and cyberspace.

First-generation scholarship sought to answer the question of whether traditional notions of territorial sovereignty apply online. Once these questions were answered with a resounding "yes" in the early 2000s, a *second generation* of

33 *Id.*

34 These are (1) the nationality principle, (2) the passive personality principle, (3) the protective principle, and (4) the effects doctrine. The first allows states to exercise jurisdiction extraterritorially over their nationals; the second permits states to punish aliens for acts abroad that cause harm within the state; the third allows states to exercise "jurisdiction over aliens for acts done abroad which affect the internal or external security or other key interests of the state"; and the fourth is a residual category when some act beyond the territory of a state causes a harmful effect that is not cognizable in the first three categories. *Id.* at 446, 443–48.

35 Ryngaert, *supra* note 30, at 27.

36 *See id.*

37 *Id.* These questions are considered in more detail in the discussion of the *Microsoft Ireland* case. *See infra* Section III.B.1.

38 CRAWFORD, *supra* note 16, at 440.

scholars began to tackle the question of how territorial sovereignty applies online. Cyberlaw scholars focused on "vertical" questions of how state power applies to non-state entities—especially those whose activities cross conventional international borders. Meanwhile, international legal scholars focused on "horizontal" questions of the implications of online sovereignty for the relationships between states.

In the second half of the last decade, a *third generation* of literature began to appear that grappled with the growing trend of Internet fragmentation. Whereas second-generation literature, especially from cyberlaw scholars, focused on extraterritorial applications of national law, third-generation literature focuses on the conscious policies of governments to bring the Internet under territorial sovereign control by enacting distinctive national laws to regulate various online phenomena.

A. First-Generation Perspectives

The first generation of scholarship focused on exploring whether cyberspace was a realm beyond the state. In the jargon of international law, one could say that this early generation of scholarship focused on whether cyberspace was a *res communis*—that is, an area that is not capable of being placed under the sovereignty of any state.

Back in the 1990s, a surprising number of scholars answered the question in the affirmative. Writing in 1997, James Boyle summarized what was then a widespread view that "if the king's writ reaches only as far as the king's sword, then much of the content of the Internet might be presumed to be free from the regulation of any particular sovereign."[39] Meanwhile, David Johnson and David Post argued that "[t]he Net . . . radically subverts the system of rule-making based on borders between physical spaces" as in their view, "[c]yberspace has no territorially based boundaries . . . because the cost and speed of message transmission on the Net is almost entirely independent of physical location."[40] Correspondingly, Johnson and Post argued for "conceiving of Cyberspace as a distinct 'place' for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the 'real world.'"[41] In so doing, Johnson and Post were among a number of legal scholars of the era to draw an analogy with the medieval Law Merchant, which they describe as "a distinct set of rules that

39 James Boyle, *Foucault in Cyberspace: Cyberspace, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 179 (1997). Boyle did not subscribe to this view, however.

40 Johnson & Post, *supra* note 1, at 1370.

41 *Id.* at 1378.

developed with the new, rapid boundary-crossing trade of the Middle Ages" that stood apart from the prevailing legal order of the day.[42]

This view was short lived, and by the dawn of the new millennium, scholars had reached a consensus that cyberspace was not a *res communis*. Not only did governments apply and enforce existing laws to online activity, but they also developed new legal doctrines to regulate online activities in a wide range of fields—from special doctrines of immunity for online service providers[43] to new criminal prohibitions on activities such as the non-consensual sharing of intimate imagery.[44] Furthermore, governments asserted their authority over the Internet by modifying its architecture. This is exemplified by China's early efforts to build a "Great Firewall" to keep certain Internet content out of its borders.[45]

Scholars of this generation often applied what Orin Kerr describes as the "external perspective" of the Internet in concluding that sovereignty and its jurisdictional corollaries applied online.[46] Kerr explains that the external perspective "adopts the viewpoint of an outsider concerned with the functioning of the network in the physical world rather than the perceptions of a user. From this external viewpoint, the Internet is simply a network of computers located around the world and connected by wires and cables."[47]

> By contrast, the "internal perspective" of the Internet
>
> adopts the point of view of a user who is logged on to the Internet and chooses to accept the virtual world of cyberspace as a legitimate construct . . . The technical details of what the computers attached to the Internet actually do "behind the scenes" don't particularly matter. What matters is the virtual

42 *Id.* at 1389. Likewise, Joel Reidenberg drew on the Law Merchant (*lex mercatoria*) analogy in developing his concept of *lex informatica*, which he used as a term to describe the governance and regulatory power exercised by technical choices in the design of information technology. *See generally* Joel R Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998).

43 The provision commonly known as Section 230 of the Communications Decency Act, which provides immunity to online platforms from liability for content posted by their users, is an example *par excellence* of this phenomenon. *See* § 230 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996. For an entertaining and informative discussion on how to best cite this provision, *see* Blake E. Reid, *Section 230 of . . . What?*, (Sept. 4, 2020), https://perma.cc/W6J5-P4E6.

44 In the decade ending in 2020, forty-eight of the fifty U.S. states enacted legislation to criminalize the non-consensual sharing of intimate imagery. *See generally* Jonathan S. Sales & Jessica A. Magaldi, *Deconstructing the Statutory Landscape of "Revenge Porn": An Evaluation of the Elements That Make an Effective Nonconsensual Pornography Statute*, 57 AM. CRIM. L. REV. 1499 (2020).

45 *See* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING, 263–71 (Ronald Deibert et al. eds., 2008).

46 Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 360 (2002).

47 *Id.*

> world of cyberspace that the user encounters and interacts with when he or she goes online.[48]

The work of Jack Goldsmith and Tim Wu exemplifies the ascendancy of the external perspective in later first-generation scholarship.[49] In their 2006 book, *Who Controls the Internet?,* Goldsmith and Wu offer the following "simple answer" to the "complex" question of why "theories of globalization and Internet scholarship" had hitherto underestimated the importance of territorial government:

> What we have seen, time and time again, is that physical coercion by government—the hallmark of a traditional legal system remains far more important than anyone expected . . . In almost every chapter of this book, beneath the fog of modern technology, we have seen the effects of coercive governmental force on local persons, firms, and equipment.[50]

Goldsmith and Wu emphasize how the control of local governments over "transport intermediaries"—that is, entities that provide the "ugly physical infrastructure" consisting of "copper wires, fiber-optic cables, and the specialized routers and switches that direct information from place to place"—allows governments to assert control over online activities based on the territoriality principle.[51] Hence the core of Goldsmith and Wu's reasoning as to the application of sovereignty online is that the infrastructure that makes up the Internet—the "series of tubes" in the evocative phrase of the late Senator Ted Stevens[52]—are located on the territory of specific states.[53] Hence while the notion of a borderless cyberspace might be attractive to some, Goldsmith and Wu conclude that cyberspace is necessarily subject to sovereignty because of the physicality of its infrastructure.

B. Second-Generation Perspectives

Second-generation scholars sought to answer the question of *how* traditional doctrines of territorial sovereignty apply online. Cyberlaw scholars of this generation focused on "vertical" questions of how state power applies to the various non-state entities that use the Internet and cause effects in various states.

48 *Id.* at 359–60.

49 *See, e.g.*, JACK L. GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).

50 *Id.* at 180.

51 *Id.* at 73.

52 Evan Dashevsky, *A Remembrance and Defense of Ted Stevens' "Series of Tubes,"* PCMAG (June 5, 2014), https://perma.cc/XL98-W8NP.

53 Unless, of course, those cables lie at the bottom of the sea, in which case they are subject to distinctive provisions of the United Nations Convention on the Law of the Sea. *See* Douglas Guilfoyle et al., *The Final Frontier of Cyberspace: The Seabed Beyond National Jurisdiction and the Protection of Submarine Cables*, 71 INT'L & COMP. L.Q. 657 (2022); s*ee also* discussion *infra* Section V.B.2.

Meanwhile, international law scholars focused on how territorial sovereignty impacts relationships between states—especially when it comes to the legality of the various kinds of "cyber operations" that states may seek to wage against each other.

1. Cyberlaw scholarship and the vertical relationship

Second-generation cyberlaw scholarship focused on the "vertical" assertion by states of their jurisdiction to the online activities of private entities. Most scholars of this generation accepted the premise that territorial sovereignty applied to the online sphere, as evinced by Svantesson's statement that "today it is uncontroversial to suggest that sovereignty applies online."[54] Correspondingly, this generation of scholarship focused on how and when the four widely recognized exceptions to the territoriality principle[55] *can* and *should* be applied to online activities. In other words, this is a literature focused on jurisdictional questions of what constitutes the exercise of territorial jurisdiction in cyberspace, what constitutes extraterritorial exercises of jurisdiction, and when the latter is desirable (or at least justified).

Scholars of this generation grappled with the interconnected nature of the Internet, and the frequent difficulty of applying the territoriality principle as a "baseline"[56] for determining whose law should apply in cyberspace. They considered the question both in terms of the application of national law to the "elephants" and the "mice" that operate in cyberspace, to use Peter Swire's evocative analogy.[57] Whereas "elephants" like Google and Microsoft are large, powerful actors who cannot hide from the local authorities in the jurisdictions where they operate, mice are small, furtive, and rapidly-reproducing creatures that are notoriously hard to catch—which in Swire's analogy represents the spammers, the scam artists, and the cyber-criminals whose activities are so difficult to police online.[58]

Jennifer Daskal's *The Un-Territoriality of Data*[59] and Andrew Keane Woods' *Against Data Exceptionalism*[60] represent the apotheosis of this generation of scholarship in their careful consideration of the application of sovereignty and

54 Svantesson, *supra* note 4, at 50.

55 *See supra* note 34 for a description of these exceptions.

56 *See* Watts & Richard, *Baseline Territorial Sovereignty and Cyberspace*, *supra* note 18.

57 *See generally* Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991 (1998) [hereinafter *Of Elephants, Mice, and Privacy*]; Peter P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, 153 U. PENN. L. REV. 1975 (2005).

58 Swire, *supra* note 57.

59 Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015).

60 Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729 (2016).

territoriality to the problem of law enforcement access to data stored on servers located in different parts of the world for investigative purposes. Many other works of this generation also grappled with when and how the four principal exceptions to territoriality should be applied in the online sphere, and whether certain assertions of jurisdiction should be properly viewed as extraterritorial—or not.[61] This is consistent with Crawford's prescient observation that "what amounts to extraterritorial jurisdiction is increasingly a matter of appreciation."[62]

Scholars of this generation worked in the shadow of several controversial cases in which courts on both sides of the Atlantic were seen by some as exercising their jurisdiction extraterritorially in an inappropriate manner. These include the Court of Justice of the European Union's decision in *Costeja,* which established a "right to be forgotten" under European data protection law;[63] the Supreme Court of Canada's decision in *Equustek v. Google,* in which Google was ordered to remove search results pointing to a pirated product on a worldwide basis;[64] and the *Microsoft Ireland* saga, which grappled with whether an American court could direct Microsoft personnel located in the U.S. to retrieve emails stored on a server in Ireland without violating Irish sovereignty.[65]

Scholars of this generation broadly embraced Kerr's "external perspective" of the Internet in assuming that sovereignty applied online and that the physical location of cyber infrastructure on the soil of given states gave rise to jurisdiction over those phenomena. Consider this statement by Andrew Keane Woods, who argues:

61 *See generally*, DAN SVANTESSON, *The Tyranny of Territoriality*, *in* SOLVING THE INTERNET JURISDICTION PUZZLE (2017).

62 CRAWFORD, *supra* note 16, at 440.

63 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317 (2014), http://perma.cc/ED5L-DZRK [hereinafter Costeja]. The Court later ruled that the geographic scope of the "right to be forgotten" was limited to the European Union; *See* Case C-507/17, Google LLC v. Comm'n nationale de l'informatique et des libertés, ECLI:EU:C:2019:15 (2019).

64 *Google Inc. v. Equustek Solutions Inc.*, [2017] 1 S.C.R 824 (Can.).

65 This saga began when the Southern District of New York denied Microsoft's motion to quash a warrant obtained under the Stored Communications Act ("SCA"), 18 U.S.C. § 2703, requiring the company to provide the FBI with copies of the contents of an email account stored on servers in Ireland. *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014). The Second Circuit quashed the warrant on the basis that it would constitute an unlawful extraterritorial application of the SCA. *Microsoft Corp. v. United States*, 829 F.3d 197, 220 (2d. Cir. 2016). The Supreme Court granted certiorari, but the case was mooted following oral argument by Congress's enactment of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, 132 Stat. 348 (2018), which clarified that SCA warrants could compel a U.S.-based provider like Microsoft to retrieve private customer data from foreign infrastructure. *See United States v. Microsoft Corp.*, 584 U.S. 236 (2018).

> The jurisdictional challenges presented by the global cloud are not conceptually as novel as they seem. Despite the technological wizardry of modern life, the "cloud" is actually a network of storage drives bolted to a particular territory, and there is substantial case law suggesting that courts think of data as a physical object.[66]

Likewise, Paul Rosenzweig notes that in the context of whose law governs stored data, "[w]here the servers are and where the data is stored will, in the end, likely control whose law applies. As they say, 'geography is destiny.'"[67] By contrast, Jennifer Daskal reflects the "internal perspective" in explaining that the way data moves through the Internet "poses a particularly profound test" to the notion of the "sovereign-territoriality link."[68] As Daskal notes:

> Data is, after all, both unterritorial and multiterritorial. It can move across territorial boundaries with the speed of light. It does not travel in obvious or observable ways from point A to B; in fact, it sometimes crosses international borders even if the beginning and end points are within the same territorial borders. It can be copied and held in multiple locations at once.[69]

Some scholars of this generation sought to propose creative ways out of these jurisdictional thickets. Andrew Keane Woods suggests that a renewed emphasis on comity—not only by judges but also by legislators and executive officials—is the key to permitting states to accomplish their regulatory goals in a manner that is "compatible with a global Internet."[70] By contrast, Dan Svantesson proposes a "legitimate interests" and "substantial connection" framework to delimit the appropriate metes and bounds of a given state's jurisdiction online.[71] While Svantesson notes that "orthodox thinking" on such questions "conflate[s] sovereignty and jurisdiction beyond what is reasonable"[72] and that "we quite simply have to reject territorial sovereignty, at least in its strictest forms"[73] to solve the titular "Internet Jurisdiction Puzzle" of his book, scholars of this generation generally did not seek to reconsider the scope and nature of state authority online.

2. International legal scholarship and the horizontal relationship

Much like their cyberlaw colleagues, the second generation of international legal scholarship also considered the implications of applying sovereignty to

66 Woods, *supra* note **Error! Bookmark not defined.**, at 729.

67 Paul Rosenzweig, *The International Governance Framework for Cybersecurity*, 37 CAN.-U.S. L.J. 405, 422 (2012).

68 Jennifer Daskal, *The Overlapping Web of Data, Territoriality, and Sovereignty, in* THE OXFORD HANDBOOK OF GLOB. LEGAL PLURALISM 953, 955 (Paul Schiff Berman ed., 2020).

69 *Id.*

70 Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 359 (2018).

71 SVANTESSON, *supra* note **Error! Bookmark not defined.**, at 62–69.

72 *Id.* at 47.

73 *Id.* at 50.

cyberspace. However, it does so from the "horizontal" perspective of relationships between states, rather than the "vertical" perspective of relationships between states and the non-state entities they govern. This is befitting since the primary concern of international law in the contemporary era is with regulating the relationships between states, who are the key actors in the present-day international system.

The second-generation international legal literature is state- and security-centric. It focuses on evaluating the legality of various kinds of "cyber operations" waged by states against the information infrastructure of other states. While there is broad agreement that certain cyber operations "can qualify as a use of force that violates Article 2(4) of the U.N. Charter or even, depending on its 'scale and effects,' as an armed attack that triggers the territorial state's right of self-defense,"[74] views differ on the legality of "low intensity" cyber operations (including intelligence-gathering) that fall short of a use of force.[75] Indeed, one scholar has described the "uncertainty as to when low-intensity cyber operations violate territorial sovereignty" as the "foremost" area of doubt regarding the "application of international law to cyber activities."[76]

As with the second generation of cyberlaw scholarship, the starting point of this literature is that sovereignty applies online as it does offline in view of the physicality of the Internet's infrastructure. As noted in the Introduction, the *Tallinn Manual 2.0* proclaims that "the principle of State sovereignty applies in cyberspace"[77] and that states "enjoy[] sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."[78] The *Tallinn Manual 2.0* goes so far as to state:

> The fact that cyber infrastructure located in a given State's territory is linked to cyberspace cannot be interpreted as a waiver of its sovereignty. Indeed, States have the right, pursuant to the principle of sovereignty, to disconnect from the Internet, in whole or in part, any cyber infrastructure located on their territory, subject to any treaty or customary international law restrictions, notably in the area of international human rights law.[79]

International legal scholars are divided, however, on whether sovereignty is a "rule" of international law or merely a "principle," and on the implications of the legal status of sovereignty for the legality of "low-intensity" cyber operations. According to Michael Schmitt and Liis Vihul, "overwhelming evidence of State

74 Kevin Jon Heller, *In Defense of Pure Sovereignty in Cyberspace*, 97 INT'L L. STUD. 1432, 1433 (2021).

75 *See* discussion *infra* this Subsection.

76 Luke Chircop, *Territorial Sovereignty in Cyberspace After Tallinn Manual 2.0*, 20 MELBOURNE J. INT'L L. 349, 349–50 (2019).

77 TALLINN MANUAL 2.0, *supra* note 7, at 11 (rule 1).

78 *Id.* at 13 (rule 2).

79 *Id.* at 12–13.

practice and *opinio juris*—the foundational elements of customary international law—supports the assertion that a primary rule not to violate the territorial sovereignty of other states exists."[80] Likewise, Sean Watts and Theodore Richard argue that "the baseline rules of territorial sovereignty should be currently understood as a rule of conduct that generally prohibits States' nonconsensual interference with the integrity of cyber infrastructure on the territory of other States."[81]

By contrast, Gary Corn and Robert Taylor, who have both held senior legal positions in the Department of Defense, take the view that "sovereignty serves as a principle of international law" but is not "a binding rule that dictates results under international law."[82] Correspondingly, Corn and Taylor argue:

> While this principle of sovereignty, including territorial sovereignty, should factor into the conduct of every cyber operation, it does not establish an absolute bar against individual or collective state cyber operations that affect cyberinfrastructure within another state, provided that the effects do not rise to the level of an unlawful use of force or an unlawful intervention.[83]

The "pure sovereignty" view advocated by Kevin Jon Heller argues that sovereignty is a primary rule of international law, and therefore

> any low-intensity cyber operation that involves non-consensually penetrating a computer system located on another State's territory violates the targeted State's sovereignty . . . Indeed, as the definition implies, most pure-sovereigntist States view merely *accessing* a computer system located on another State's territory as a violation of sovereignty.[84]

An intermediate position, which Heller characterizes as the "relative sovereignty" view, holds that "mere penetration of a computer system located on the territory of another state" is insufficient to violate the sovereignty of the targeted state.[85] Rather, "a cyber operation must cause at least some kind of harm to the targeted state to be internationally wrongful."[86]

The difference in views between these camps appears to reflect differences of opinion on the normative desirability of conducting low-intensity cyber operations—particularly against terrorist entities—without the consent of the state on whose territory the relevant cyber-infrastructure resides. Corn and Taylor argue that if sovereignty is a rule of international law, then "states seeking to

80 Michael Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639, 1650 (2017).

81 Watts & Richard, *supra* note 18, at 808.

82 Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207, 208 (2017).

83 *Id.* at 208–09.

84 Heller, *supra* note **Error! Bookmark not defined.**, at 1458.

85 *Id.* at 1461.

86 *Id.*

disrupt distributed terrorist cyber infrastructure would be under an obligation to either seek Security Council authorization or the consent of the state in whose territory the infrastructure resides."[87] Schmitt and Vihul, by contrast, note that giving states wide latitude to engage in low-intensity cyber operations would leave those lacking the cyber-capabilities of great powers like the United States "legally defenseless in the face of most such operations."[88] Likewise, Sean Watts and Theodore Richard argue that "the historical baseline of territorial sovereignty, including a prohibition on territorial interferences, persists as an important guarantor of peaceful relations between States" both in physical space and in cyberspace.[89] As we will see in the next Section, this scholarly debate is mirrored in the views of governments on the very same questions.

Interestingly, this literature does not consider the implications of its views on the relationship between sovereignty and cyberspace to the quotidian use and functioning of the Internet. While noting that "an increasing number of states are resorting to rhetoric and practice that seems to strongly favor sovereignty over a free and open cyberspace," Schmitt and Vihul have nothing further to say about the implications of their views of sovereignty on the "delicate[] balance [between] the notions of a free flow of information in cyberspace with a state's sovereign control over cyber activities occurring within its territory."[90] Nor does this literature cast much light on the questions addressed by second-generation cyberlaw scholars regarding when exercises of online jurisdiction are proper under international law.[91] Rather, this literature focuses on the freedom of states "from interference with territorial sovereignty"[92] under international law, to the exclusion of any serious analysis of the impacts of this position on the freedoms of the natural and legal persons who are subject to their jurisdiction.[93]

87 Corn & Taylor, *supra* note **Error! Bookmark not defined.**, at 211.

88 Schmitt & Vihul, *supra* note **Error! Bookmark not defined.**, at 1669.

89 Watts & Richard, *supra* note 18, at 872.

90 Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace:* Lex Lata Vel Non*?*, 111 AM. J. INT'L L. UNBOUND 213, 218 (2017).

91 The most notable exception is a piece by the General Counsel of Human Rights Watch that critiques the *Tallinn Manual's 2.0* stilted conceptualization of human rights. *See* Dinah PoKempner, *Squinting Through the Pinhole: A Dim View of Human Rights from Tallinn 2.0*, 95 TEX. L. REV. 1598 (2017).

92 Chircop, *supra* note **Error! Bookmark not defined.**, at 369.

93 *See, e.g.,* Phil Spector, *In Defense of Sovereignty, in the Wake of Tallinn 2.0*, 111 AM. J. INT'L L. UNBOUND 219 (2017) (discussing the rights of states under international law to exercise complete authority over their territory and any persons or activities therein, but failing to say anything about international legal protections for individual rights); *accord* Watts & Richard, *supra* note 18; *accord* Heller, *supra* note **Error! Bookmark not defined.** (whose sole mention of human rights is in a footnote).

C. Third Generation Perspectives

A third generation of scholarship emerged in the middle of the last decade that grappled with government actions to bring the Internet under stricter national control. Some of the other defining works of this generation of scholarship include *Data Nationalism* by Anupam Chander and Uyên Lê, which chronicled the various ways that governments were erecting barriers to prevent certain kinds of data from leaving their territory, [94] and Mark Lemley's *The Splinternet*, which chronicled the growing fragmentation of the software, hardware, and networking protocols that give rise to the Internet.[95] More recently, the work of Beth Simmons and Rachel Hulvey, which transcends the disciplinary boundaries between law and political science, documents and contextualizes the rise of borders in cyberspace. Per Simmons and Hulvey, the rise of borders in cyberspace is to be expected because states have long turned to "delimiting, enforcing, and hardening the boundary of their territorial jurisdiction" when they are otherwise unable to effectively regulate "activities, people, and ideas according to social purposes on [their] territory."[96] As they further explain:

> States struggle with sometimes overwhelming "cyber issues," but they are grounded in—and indeed are constituted by—territorial sovereignty. To understand recent trends toward internet fragmentation, we suggest it is important to think like a state. When we do, it becomes clear that state leaders have fairly traditional ideas and values about maintaining sovereign territorial control.[97]

Many scholars of this generation use the terms "digital sovereignty" or "data sovereignty" as a descriptor of the trends they are evaluating. Most such scholars use the term "sovereignty" not as international lawyers do, but in a broader sense. Consider, for example, the introduction to the new edited volume by Anupam Chander and Haochen Sun entitled *Digital Sovereignty*. At first, Chander and Sun define the titular term of their book "to mean the application of traditional state sovereignty over the online domain, or simply 'sovereignty in the digital age," but they go on to clarify that their volume uses the term "in a descriptive way to describe efforts by governments to assert control over online activities." [98]

94 Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677 (2015).

95 Mark Lemley, *The Splinternet*, 70 DUKE L.J. 1397 (2021).

96 Beth A. Simmons & Rachel A. Hulvey, *Cyberborders: Exercising State Sovereignty Online*, 95 TEMPLE L. REV. 617, 619 (2023).

97 *Id.* at 625.

98 Anupam Chander & Haochen Sun, *Introduction: Sovereignty 2.0*, *in* DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE 1, 6 (Anupam Chander & Haochen Sun eds., 2023).

Likewise, Theodore Christakis has explained that in European policy discussions regarding "digital sovereignty," the term is understood not in terms of its meaning in international law, but rather to signify "the power to regulate what is going on in cyberspace and the digital sphere" as well as "the means to achieve strategic autonomy in the digital sphere."[99] Correspondingly, Christakis's study of the emerging phenomenon of "European Digital Sovereignty" examines it from this broader perspective, rather than with reference to the international legal meaning of sovereignty.

One important strand of this generation of scholarship considers the relationship between the international human rights obligations of states and the growing trend toward Internet fragmentation. Such studies often note the "double-edged" character of assertions of digital sovereignty. As Chander and Sun have noted:

> Digital sovereignty is simultaneously a necessary incident of democratic governance and democracy's dreaded antagonist. Governments need to control the Internet's impact on their people. Yet, at the same time, control over the Internet offers governments enormous power over their residents' lives . . . Assertions of digital sovereignty thus carry a double edge—useful both to protect citizens and to control them.[100]

In her study explaining how the free expression protections enshrined in Article 19 of the International Covenant on Civil and Political Rights (ICCPR)[101] could give rise to an international law of the Internet, Molly Land explains how Article 19(2) in particular is "fundamentally committed to a global internet."[102] She explains how the provision creates an "explicit right to seek, receive, and impart information across borders."[103] Yet Land acknowledges that "Article 19(2) does not prevent states from controlling and even filtering content as it crosses their borders, but it does establish a presumption against such limitations and requires that they meet the legality, legitimacy, and proportionality criteria of Article 19(3)."[104]

Correspondingly, in implementing restrictions on expression that otherwise meet the requirements of Article 19(3), states must also "treat foreign content like domestic content" and avoid "disproportionately burdening information and expression from abroad."[105]

99 Christakis, *supra* note 13, at 8, 11.

100 Chander & Sun, *supra* note 3, at 72.

101 International Covenant on Civil and Political Rights art. 19(2), *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) [hereinafter ICCPR].

102 Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L.J. 393, 437 (2013).

103 *Id.* at 438.

104 *Id.*

105 *Id.* at 439.

More recently, Kyung Sin Park has surveyed the rich body of jurisprudence and scholarship assessing the legality of Internet shutdowns under international human rights law and related its lessons to the growing trend toward data localization.[106] As Park demonstrates, there is now a scholarly and judicial consensus that orders blocking the availability of an entire platform in a country, not to mention wholesale Internet shutdowns, are *per se* disproportionate under human rights law.[107] While acknowledging that some data localization laws are intended to ensure that certain data are subject to the heightened safeguards of a particular jurisdiction's privacy and data protection laws, Park explains how the practical effect of many such laws is to prevent the residents of a state from accessing a particular platform for communication—raising similar concerns to those that animate the jurisprudence on Internet shutdowns.[108]

There is also a significant and voluminous third-generation literature on the uses and misuses of international human rights laws by the large platforms that intermediate so much online communication in terms of establishing rules for what can be said online. Proponents of the incorporation of international human rights law into the content moderation rules of behemoths like Meta and Alphabet point to the coherence and protectiveness of international free expression standards as good reasons to support this trend.[109] Others, by contrast, point to the very real limitations of doing so in view of the indeterminacy of international human rights law and the contested nature of its norms, among other limitations.[110]

IV. GOVERNMENTAL PERSPECTIVES ON SOVEREIGNTY, CYBERSPACE, AND INTERNET FREEDOM

While governments generally agree that traditional notions of territorial sovereignty apply in cyberspace, they differ on its implications for the digital realm—especially as to the legality of various kinds of cyber operations. Yet at the same time as governments have been propounding their belief that sovereignty applies online as it does offline, practically all of the world's democracies have also issued statements identifying the preservation of a free, open, and global Internet

106 Kyung Sin Park, *Lessons from Internet Shutdowns Jurisprudence for Data Localization, in* DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE, 332 (Anupam Chander & Haochen Sun eds., 2023).

107 *Id.* at 343–64.

108 *Id.* at 366–69.

109 Evelyn Aswad, *To Protect Freedom of Expression, Why Not Steal Victory from the Jaws of Defeat?*, 77 WASH. & LEE L. REV. 609 (2020).

110 Evelyn Douek, *The Limits of International Law in Content Moderation*, 6 U.C. IRVINE J. INT'L TRANSNAT'L & COMP. L. 37 (2021).

as a first-order policy priority. Scholars have not paid any serious attention to these statements, nor have they attempted to reconcile the views of governments on sovereignty with their views on Internet freedom.

This Section will survey the range of views held by governments regarding the application of sovereignty to cyberspace as well as the importance of preserving a free and open global Internet. In so doing, it will demonstrate the difficulty of reconciling the two sets of views within the current framework of international law—including prevailing understandings of the applicability of international human rights law.

A. Government Views on Sovereignty in Cyberspace

International legal scholars seeking to divine the views of governments on the application of international law to cyberspace (including the principle or rule of sovereignty) often look to the position statements that numerous governments have issued on this question in recent years.[111] The drafting of these statements has been catalyzed by two United Nations initiatives that seek to clarify whether and how international law applies in cyberspace. The first is colloquially known as the U.N. Group of Governmental Experts (GGE) and consisted of six groups of experts who convened intermittently between 2004 and 2021.[112]

The second is widely known as the U.N. Open-Ended Working Group (OEWG) and has a four-year mandate that ends in 2025.[113]

At least 30 national governments and one regional organization have issued statements expressing their views on the application of international law to cyberspace. All but one of them affirm that traditional notions of territorial sovereignty apply in cyberspace.[114] The sole exception appears to be the statement of Kazakhstan,[115] although this may be due to inaccuracies in available machine translations of the Russian language original.

Many national statements cite with approval the declaration of the GGE in its 2013 report that "[s]tate sovereignty and international norms and principles

111 *See, e.g.,* Heller, *supra* note **Error! Bookmark not defined.**, at 1444–50.

112 Michael Schmitt, *The Sixth United Nations GGE and International Law in Cyberspace*, JUST SEC. (June 10, 2021), https://perma.cc/XA64-MVN6.

113 Andrijana Gavrilović, *A New Landmark in Global Cybersecurity Negotiations: UN Cyber OEWG in Numbers*, DIPLOMACY (Mar. 18, 2021), https://perma.cc/XG6H-9GVZ.

114 This conclusion is based on my review of these statements, which have been collected by the Cyber Law Toolkit project and are available at https://perma.cc/9QBY-WNQD.

115 Statement of Kazakhstan, Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts 51, U.N. Doc. A/76/136 (July 13, 2021).

that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory."[116] The GGE reiterated this stance in a 2015 report,[117] which was ultimately adopted by the U.N. General Assembly in December 2015.[118]

In so doing, many states implicitly adopt Orin Kerr's "external perspective" of the Internet in explaining why traditional notions of territorial sovereignty extend to the online sphere.[119] The statement of the Netherlands, for example, declares that "States have exclusive authority over the physical, human and immaterial (logical or software-related) aspects of cyberspace within their territory."[120] Similarly, the French government's submission to the OEWG asserts that governments possess sovereignty over information systems located on their territory.[121] A German government position paper echoes this sentiment, indicating that sovereignty in the digital context implies a right of regulation, enforcement, and adjudication regarding cyber activities and infrastructure within a state's territory.[122]

The views of at least some states on the application of sovereignty to the Internet appear to have evolved over time. In 2010, Canada's Cyber Security Strategy proclaimed that cyberspace "is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship";[123]

116 Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2013), transmitted by Letter dated 7 June 2013 from the Chair of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Established Pursuant to Resolution 66/24 (2012), ¶ 20, U.N. Doc. A/68/98 (June 24, 2013). "ICT" stands for information and communications technology.

117 Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015), transmitted by Letter dated 26 June 2015 from the Chair of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Established Pursuant to Resolution 68/243 (2014), ¶¶ 27-28, U.N. Doc. A/70/174 (July 22, 2015).

118 G.A. Res. 70/237, ¶¶ 1-2 (Dec. 30, 2015).

119 Kerr, *supra* note 46, at 360.

120 Government of the Netherlands, *Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace*, 2 (July 5, 2019), https://perma.cc/S8DX-7926.

121 Government of France, *International Law Applied to Operations in Cyberspace: Paper Shared by France with the Open-Ended Working Group Established by Resolution 75/240 §1.1.1* (2021), https://perma.cc/8CYT-EJF8.

122 Federal Foreign Office et al., *Government of Germany, On the Application of International Law in Cyberspace: Position Paper 2* (Mar. 2021), https://perma.cc/9UJ2-LFQK.

123 Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* at 2 (2010), https://perma.cc/NB65-6PWW

yet a Canadian position paper issued in 2022 held that "[i]t is axiomatic that the principle of sovereignty applies in cyberspace."[124]

What is more, the views of states diverge considerably on the implications of sovereignty for the legality of various kinds of cyber operations. As with the divide in the academic community between those who advocate for "pure" versus "relative" sovereignty, different states take different views on this question. New Zealand's position paper takes the view that cyber operations are unlawful only when they cause significant harms,[125] while Costa Rica[126] and the Czech Republic[127] lay out various factors to be considered in determining if a particular cyber-operation violates territorial sovereignty in their papers.

By contrast, a French Foreign Ministry statement expresses the view that "the unauthorized penetration of French systems or the production of effects in French territory via cyber means by a State entity . . . can constitute a violation of sovereignty."[128] Likewise, a Swiss government position paper on the application of international law to cyberspace states that sovereignty protects ICT infrastructure from "unauthorized intrusion."[129]

The African Union (AU) adopts an even more strident view on this question. In its recently released Common African Position on the application of international law to cyberspace, the AU states that "by virtue of territorial sovereignty, any unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State is unlawful."[130] The AU goes even further in declaring that "the obligation to respect the territorial sovereignty of States, as it applies in cyberspace, does not include a *de minimis* threshold of harmful effects

124 Government of Canada, *International Law Applicable in Cyberspace* ¶ 10 (Apr. 22, 2022), https://perma.cc/54KA-SMXY.

125 Ministry of Foreign Affairs and Trade, Government of New Zealand, *The Application of International Law to State Activity in Cyberspace* ¶ 9 (Dec. 1, 2020), https://perma.cc/Y43C-FC5E.

126 MINISTERIO DE RELACIONES EXTERIOS Y CULTO [MINISTRY OF FOREIGN AFFAIRS AND WORSHIP], Government of Costa Rica, *Costa Rica's Position on the Application of International Law in Cyberspace* ¶ 20 (July 21, 2023), https://perma.cc/6QN7-EK3B.

127 Ministry of Foreign Affairs et al., Government of the Czech Republic, *Position Paper on the Application of International Law in Cyberspace* ¶¶ 5–6 (Feb. 27, 2024), https://perma.cc/M88S-YZU7.

128 Government of France, *France's Response to Resolution 73/27 "Developments in the Field of Information and Telecommunications in the Context of International Security" and Resolution 73/266 "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security"* at 8, https://perma.cc/4H22-H3U8.

129 Directorate of International Law, Federal Department of Foreign Affairs, *Switzerland's Position Paper on the Application of International Law in Cyberspace*, at 2 (May 2021), https://perma.cc/6669-NQAP.

130 Peace and Security Council, African Union Commission, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace* ¶ 16 (Jan. 29, 2024), https://perma.cc/NTE4-RXGR [hereinafter Common African Position].

below which an unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State would not be unlawful."[131]

B. Government Views on Internet Freedom

Notwithstanding its seeming embrace of "pure sovereignty" in cyberspace,[132] the AU statement is among the many that has recognized the "interest of all States" in developing "a global legal architecture" that "guarantees that cyberspace remains open, secure, stable, accessible, and peaceful, protects basic human rights and fundamental freedoms of individuals and peoples, and advances the common interests of humankind."[133]

Indeed, 21 of the 30 national governments that have issued statements on the application of international law to cyberspace expressly acknowledge the importance of protecting a free, open, and global Internet.[134] Moreover, some 70 states signed the Declaration for the Future of the Internet in 2022[135] and pledged to "promote and sustain an Internet that[] is open, free, global, interoperable, reliable, and secure."[136] Thirty-nine governments have joined together to form the Freedom Online Coalition, a multilateral group whose *raison d'être* is to "[a]dvocate for a global, free, open, interoperable, secure and reliable Internet" and "to resist Internet fragmentation."[137]

As part of the ongoing process initiated by the United Nations to negotiate a Global Digital Compact ("Compact"), whose stated aims include "outlin[ing] shared principles for an open, free, and secure digital future for all" and "avoiding fragmentation of the Internet,"[138] numerous states have drafted submissions that affirm their commitment to these principles. For example, a submission by

131 *Id.*

132 Kevin Jon Heller, *The African Union (Rightly) Endorses Pure Sovereignty in Cyberspace*, OPINIO JURIS (Feb. 5, 2024), https://perma.cc/R2FY-PFBU.

133 Common African Position, *supra* note **Error! Bookmark not defined.** ¶ 4.

134 This is based on my review of these statements as described *supra* note **Error! Bookmark not defined.**.

135 Signatories of the Declaration include all 27 member-states of the European Union as well as states ranging from Canada to Costa Rica and New Zealand to Niger. *See* U.S. DEP'T OF STATE, DECLARATION FOR THE FUTURE OF THE INTERNET (Apr. 26, 2022), https://perma.cc/44JF-SXQZ.

136 A DECLARATION FOR THE FUTURE OF THE INTERNET, *supra* note 9, at 1.

137 FREEDOM ONLINE COALITION, THE OTTAWA AGENDA: RECOMMENDATIONS FOR FREEDOM ONLINE (2023), https://perma.cc/EQZ6-SY2T.

138 The United Nations Internet Governance Forum also has a Policy Network on Internet Fragmentation, which is focused on "policy, technical, legal, and regulatory measures that threaten the open, interconnected, and interoperable nature of the Internet." For more details, *see* U.N. Internet Governance Forum, Policy Network on Internet Fragmentation, https://perma.cc/WX23-YEX7.

Switzerland stated its support for the core principles of the Compact, including avoiding Internet fragmentation by working towards a single, open, and interoperable Internet.[139] While recognizing the need for proper regulation of the Internet, France's submission stated that doing so "should not lead to questioning the principles of an open, decentralized and interoperable architecture, net neutrality, and multi-stakeholder and inclusive Internet governance."[140] Japan stated that it "strongly supports promotion of the open, free, global, interoperable, reliable, and secure Internet,"[141] while Singapore echoed this sentiment, indicating that "it is essential that the Internet remains open, secure, and interoperable."[142] Austria stated that it "fully supports an open, stable, [and] free . . . Internet,"[143] as has Poland.[144] The European Union, on behalf of its 27 members, outlined its expectation that the Compact support a free and open Internet, stating that the "EU shares a vision of the Internet that is open, stable, free, inclusive, global, interoperable, reliable, secure, and green."[145]

None of these statements mention the concept of sovereignty or the physicality of the Internet's infrastructure. Rather, many affirm the view of governments that

> the Internet should operate as a single, decentralized network of networks – with global reach and governed through the multistakeholder approach, whereby governments and relevant authorities partner with academics, civil society, the private sector, technical community and others. Digital technologies reliant on the Internet, will yield the greatest dividends when they operate as an open, free, global, interoperable, reliable, and secure system.[146]

139 Government of Switzerland, *Switzerland: Contribution to the Global Digital Compact* at 2–3 (Apr. 30, 2023), https://perma.cc/G7VN-EKAF.

140 Government of France, *Global Digital Compact: Contribution of France* at 5 (Apr. 2023), https://perma.cc/LJU7-NCTX.

141 Government of Japan, C*ontribution of Japan for the Global Digital Compact* at 2 (Apr. 2023), https://perma.cc/NN56-5S75.

142 Permanent Mission of Singapore to the United Nations, *Intervention by First Secretary Matthew Wong of Singapore at the Second Thematic Depp Dive on the Global Digital Compact on the Issue of Internet Governance*, ¶ 2 (Apr. 13, 2023), https://perma.cc/62SH-TSUG.

143 Republic of Austria, *Global Digital Compact -- Contribution by Austria* at 2 (Apr. 2023), https://perma.cc/7JVD-6PC4.

144 Government of Poland, *Input from the Government of the Republic of Poland to the Global Digital Compact* at 3 (Apr. 2023), https://perma.cc/26YS-XC92 ("Poland strongly advocates for an open, undivided, free, global, secure, and resilient Internet.").

145 European Union, *European Union Contribution to the Global Digital Compact* at 6 (Mar. 2023), https://perma.cc/3L59-FJ8Y.

146 A DECLARATION FOR THE FUTURE OF THE INTERNET, *supra* note 9.

Such statements reflect Kerr's internal perspective of the Internet,[147] insofar as they accept cyberspace as a legitimate construct and reflect a commitment to preserving cyberspace as "a single interconnected communications system for all of humanity."[148]

C. Are Territorial Sovereignty and Internet Freedom Reconcilable?

The admirable commitment of so many states to preserving a free, open, and global Internet is difficult to reconcile with their views as to the application of online sovereignty. Consider Norway's national statement, which recognizes sovereignty as a "primary rule of international law" that gives states "the exclusive right to exercise jurisdiction within its territory, including over the information systems located on its territory."[149] While acknowledging that "[i]nternational human rights law applies to cyber activities just as it does to any other activity" and that "[s]tates must comply with their human rights obligations also in cyberspace, as they must in the physical world," Norway qualifies this view by noting:

> Neither the individuals that are subject to a State's jurisdiction, nor the concept of jurisdiction, is altered by the fact that the activity attributed to the State is a cyber activity. In this respect, cyber activity is no different from other means that States may use to violate their human rights obligations towards their citizens.[150]

The challenge, of course, is that conventional views suggest that international human rights law applies only to individuals who are subject to a state's jurisdiction. By and large, this corresponds to those individuals who reside on a state's territory, although there are some exceptional circumstances in which human rights obligations may extend extraterritorially.[151] Neither of these

147 Kerr, *supra* note 46, at 359–60.

148 A DECLARATION FOR THE FUTURE OF THE INTERNET, *supra* note 9.

149 Government of Norway, *Norwegian Positions on Selected Questions of International Law Relating to Cyberspace* at 1 (May 2021), https://perma.cc/V2SV-P3XD.

150 *Id.* at 10.

151 The U.N. Human Rights Committee, in General Comment 31 to the ICCPR, has explained that "a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party." Human Rights Comm., General Comment No. 31: The Nature of the General Legal Obligation Imposed on State Parties to the Covenant, ¶ 10, CCPR/C/21/Rev.1/Add. 13 (May 26, 2004). Human rights bodies have recognized two situations in which this occurs. One is when a state "exercises jurisdictional authority over a territory, even if this is not sovereign territory, as in the case of a military occupation." The other is in situations of extraterritorial abductions or detention, where "by exercising control and authority over an individual, that person is brought within the jurisdiction of the state for the purpose of human rights obligations." NOAM LUBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS 193, 211 (2010).

situations applies, however, when a state decides to exercise its powers as a territorial sovereign to prevent persons who are not subject to its jurisdiction from accessing Internet infrastructure located within its borders—even if such access is harmless. Recall the African Union's view that "the obligation to respect the territorial sovereignty of States, as it applies in cyberspace, does not include a *de minimis* threshold of harmful effects below which an unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State would not be unlawful."[152]

The history of litigation surrounding the Computer Fraud and Abuse Act ("CFAA") in the United States[153] reveals just how much turns on how one interprets the phrase "unauthorized access." Under this law enacted by Congress in 1986, criminal or civil liability can attach when someone "intentionally accesses a computer without authorization or exceeds authorized access."[154]

Prior to the U.S. Supreme Court's 2021 decision in *Van Buren,*[155] there was a great deal of litigation brought by large Internet platforms under the CFAA against companies that engaged in "web scraping" in violation of the former's stated terms of service.[156] "Web scraping" involves the use of an automated tool to extract data from one or more websites. Scraping has many purposes, ranging from academic research[157] to the operation of price comparison websites[158] to the training of artificial intelligence systems for a variety of purposes.[159]

In *hiQ Labs v. LinkedIn,* for example, hiQ used automated bots to scrape information from publicly available LinkedIn profiles.[160] LinkedIn sent hiQ a cease-and-desist letter claiming that hiQ's actions violated LinkedIn's User Agreement and purporting to revoke hiQ's access to its server, yet hiQ continued with its activities.[161] Ultimately, the Ninth Circuit held that because LinkedIn failed to impose access barriers on its public profiles, anyone could access the

152 Common African Position, *supra* note 130, at ¶ 16.

153 18 U.S.C. § 1030.

154 18 U.S.C. § 1030(a)(2).

155 Van Buren v. United States, 593 U.S. 374 (2021).

156 At least 61 such cases resulted in published opinions between 1998 and 2018. *See* Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 378 (2018).

157 *Id.* at 372–73.

158 *See, e.g.*, Judith Hillen, *Web Scraping for Food Price Research*, 121 BRIT. FOOD J. 3350 (2019).

159 John Voorhees, *How We're Trying to Protect MacStories from AI Bots and Web Crawlers – And How You Can, Too*, MACSTORIES (June 17, 2024), https://perma.cc/8DK3-XSJ3 (last visited June 30, 2024).

160 hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1186 (9th Cir. 2022).

161 *Id.* at 1187.

information.[162] Correspondingly, the Court held that LinkedIn's cease-and-desist letter was insufficient to revoke hiQ's access to the social network's publicly available data,[163] and that "the concept of 'without authorization' does not apply to public websites."[164]

The AU position paper does not specify whether it takes the view of hiQ or LinkedIn as to what constitutes "unauthorized access." Yet the notion that territorial sovereignty permits states to block foreigners from accessing ICT infrastructure located on their territory in a harmless manner is hard to square with the continued existence of a free, open, and global Internet. The notion of governments enacting laws to bar foreigners from their information infrastructure without taking technical measures to restrict their access might seem fanciful, yet this does not answer the legal question of whether territorial sovereignty should vest governments with unlimited power to do so. As we have already seen, international human rights law contains few restrictions on the ability of states to prevent those not subject to its jurisdiction from accessing ICT infrastructure located on its territory, even when such access is entirely harmless.

While it is commendable that so many states have expressed their commitment to preserving a free and open global Internet in national policy statements and multilateral declarations, this Article contends that something so important should not be left to the discretion of states. Rather, such rights of access should be protected by international law, and as the rest of this Article explains, the law of the sea can help us chart a path to this outcome.

V. AN INTRODUCTION TO THE LAW OF THE SEA

This Section provides a conceptual orientation to the law of the sea before diving into a description of some of its most important provisions. Since the law of the sea is almost as vast as the oceans, it is not possible to plumb its depths within the bounds of this Article. Even so, my hope is that the surface skim that follows is sufficient to demonstrate why the law of the sea is so helpful to the project of rethinking how states should exercise their authority in the online sphere.

162 *Id.* at 1199.

163 *Id.*

164 *Id. See also* Ryanair DAC v. Booking Holdings Inc., 636 F. Supp. 3d 490, 508 (D. Del. 2022) ("If the information on the website is publicly available without requiring users to authenticate themselves, a violation of the terms of use or the defiance of a cease-and-desist letter will not give rise to liability under the CFAA.").

The law of the sea's origins can be traced back to both Roman law and the classical international law of Asia.[165] Both legal systems recognized that the seas were a commons beyond the authority of any ruler,[166] although it should be noted that political authority in both Rome and classical Asia was based on concepts other than territorial sovereignty.[167]

Starting from this original position of the seas as a commons, the modern law of the sea evolved alongside the doctrine of territorial sovereignty after the end of the Middle Ages. This co-evolution can be seen in the works of Hugo Grotius, a leading international legal scholar of the 17th century, who published *Mare Liberum* ("The Freedom of the Seas")[168] and *De iure belli ac paci*s ("The Rights of War and Peace")[169] in 1609 and 1625, respectively. The former lays out Grotius's arguments for the freedom of the seas, while the latter is widely seen as a foundational work that informed the development of the modern system of sovereign, territorially bounded states following the 1648 Peace of Westphalia.[170]

The cornerstone of Grotius's argument for the freedom of the seas was his view that the oceans cannot be appropriated. In *Mare Liberum,* Grotius reasoned that "that which cannot be occupied, or which has never been occupied, cannot be the property of anyone, because all property has arisen from occupation."[171] By contrast, John Selden—Grotius's contemporary and intellectual rival—argued in a competing volume entitled *Mare Clausum* ("The Closed Seas") that some areas of the sea could be possessed and occupied by a coastal state.[172]

Ultimately, it was the work of Cornelius van Binkershoek, a Dutch jurist of the late 17th century, that charted a middle course between Grotius's and Selden's views.[173] As Philip C. Jessup has explained, Binkershoek

165 Andree Kirchner, *Law of the Sea, History Of, in* MAX PLANCK ENCYCLOPEDIA OF PUB. INT'L L., ¶ 21 (Rüdiger Wolfrum ed., 2007).

166 *Id.*

167 JACKSON, *supra* note 17, at 7.

168 HUGO GROTIUS, THE FREE SEA (David Armitage ed., Richard Hakluyt trans., Liberty Fund, Inc. 2004) (1609).

169 HUGO GROTIUS, THE RIGHTS OF WAR AND PEACE (Richard Tuck ed., Liberty Fund, Inc. 2005) (1625).

170 *See, e.g.,* Hedley Bull, *The Importance of Grotius in the Study of International Relations, in* HUGO GROTIUS AND INT'L RELS. 65 (Hedley Bull et al. eds., 1992).

171 DONALD ROTHWELL & TIM STEPHENS, THE INTERNATIONAL LAW OF THE SEA 2 (3d ed. 2023) (*citing* HUGO GROTIUS ET AL., THE FREEDOM OF THE SEAS, OR THE RIGHT WHICH BELONGS TO DUTCH TO TAKE PART IN THE EAST INDIAN TRADE: A DISSERTATION 27) (James Brown Scott, ed., Ralph van Deman Magoffin, trans., Oxford University Press 1916) (1608).

172 David J. Bederman, *The Sea*, *in* THE OXFORD HANDBOOK OF THE HIST. OF INT'L L., 369 (Bardo Fassbender & Anne Peters eds., 2012).

173 *Id.*

> put his maxim into material terms and declared that the territorial domain of the state extend as far as projectiles could be thrown from cannon on the shore. Thus originated the doctrine of cannon range which is preserved on some statute books to this day, and which may be described as the direct progenitor of the three-mile rule.[174]

The "cannon-shot rule" served as the basis for states to claim a narrow belt of "territorial sea" offshore their coastlines starting in the 17th century. Beyond this narrow belt, however, the Grotian conception of freedom of the seas persisted well into the 20th century, when new technological developments led states to extend their maritime claims further seaward. Since at least the 17th century, the nature of state authority over their maritime domains has always been very different from the nature of the power they exercise over land.

What is more, the role of technological change in driving the evolution of the law of the sea cannot be ignored. Just as the development of modern cartography was a necessary condition for the development of the legal doctrine of territorial sovereignty, advances in artillery in the 17th century gave rise to the notion that a coastal state could exercise authority over a narrow adjoining belt of the sea.[175] Likewise, more recent advances in deep-sea fishing and in technologies to exploit the living and non-living resources found at the bottom of the sea (e.g., lobsters and petroleum) drove the development of the law of the sea in the 20th century.

The presentation of the key features of the contemporary law of the sea in the pages that follow draws heavily from the United Nations Convention on the Law of the Sea (UNCLOS), which was concluded in 1982.[176] Consisting of 17 parts and nine annexes, UNCLOS codifies the customary law of the sea while also introducing innovative new provisions to deal with emerging issues of oceanic governance. UNCLOS has been ratified by 164 of the 193 U.N. member-states—albeit not by the United States, which nonetheless views the provisions of the law of the sea that are discussed in the Sections that follow as reflecting customary international law.[177]

174 PHILIP C. JESSUP, THE LAW OF TERRITORIAL WATERS AND MARITIME JURISDICTION 5–6 (1927).

175 Indeed, it is hard to fathom the idea of states claiming authority over a specified width of salt water adjacent to their coastlines without modern cartography.

176 U.N. Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS].

177 Mark Simonoff, United States Mission to the U.N., Remarks at a UN General Assembly Commemoration of the 40th Anniversary of the Opening for Signature of the 1982 Law of the Sea Convention (Apr. 29, 2022), https://perma.cc/VWC7-6PUH (last visited June 14, 2024) ("Let me end by reiterating U.S. support for the Law of the Sea Convention and our continued regard for much of the Convention as reflective of customary international law.").

A. The Concept of Sovereign Rights

The provisions of the law of the sea that permit states to lay claim to certain maritime areas lying off their coastlines can be understood as creating a regime of "sovereign rights," which stands in contrast to the regime of territorial sovereignty that prevails on the land. While many provisions of UNLCOS recognize coastal states as possessing "sovereignty" over certain maritime areas, the law of the sea has long placed restrictions on the authority of coastal states that are hard to reconcile with conventional understandings of what sovereignty entails.

"Sovereign rights" is a relatively new term in international law. The term appears to have first been used to describe the character of the rights that U.S. states possess in rivers that flow into another state.[178] Its first use in an international treaty appears to be in the 1956 Convention on the Continental Shelf,[179] where it describes the limited nature of the rights that coastal states may claim over this maritime feature (namely, to explore and exploit its natural resources).

Crawford defines "sovereign rights" to mean "various types of rights, indefeasible except by special grant or historic title, in the patrimony of a state."[180] He further notes that "[r]ights which are 'owned' and in this special sense 'sovereign' involve a broader concept, not reducible to territorial sovereignty."[181] In UNCLOS, the term "sovereign rights" is used to describe the nature of the rights that states possess in the continental shelf and the exclusive economic zone (EEZ),[182] in contrast with the "sovereignty" that states are said to possess in the territorial sea.

Although it is unconventional to do so, I believe that it is useful to use the notion of "sovereign rights" to conceptualize the limited nature of the authority that states exercise in *all* maritime zones—including in the territorial sea. Doing so sharpens the contrast between the "sovereignty" that states possess over their land territory, and the rather more limited set of rights that states possess even in the territorial sea. The highly constrained "sovereignty" of states in the territorial sea will be illustrated below, as will how sovereign rights diminish the further one goes out to sea—till one reaches the high seas, the archetypal *res communis* in international law.

178 *See, e.g.*, Ernest C Carman, *Sovereign Rights and Relations in the Control and Use of American Waters*, 3 S. CAL. L. REV. 266 (1930) (using the term "sovereign rights" to describe the rights Colorado claimed in its eponymous river at the time of its statehood).

179 Convention on the Continental Shelf, Apr. 29, 1958, T.I.A.S. No. 5,578, 499 U.N.T.S. 311.

180 CRAWFORD, *supra* note 16, at 194.

181 *Id.*

182 UNCLOS, *supra* note 176, at arts. 56(1)(a), 77(1).

As we will see, the authority of coastal states in the seas is limited by the navigational rights that ships of all states possess in *all* maritime zones. For as long as international law has recognized the "sovereignty" of coastal states in the territorial sea, it has also recognized the right of vessels of other states to enter such waters without the coastal state's authorization in a range of circumstances.[183] Such rights are hard to square with the plenary nature of the powers that sovereignty vests in states to keep foreigners off their territory.

B. Delineating Sovereign Rights at Sea

A good starting point for understanding the nature and extent of the sovereign rights that coastal states possess in maritime areas off their shores is the dictum of the International Court of Justice in the *North Sea Cases* that the "land dominates the sea."[184] This principle holds that states may possess (nominal) sovereignty or sovereign rights in certain maritime areas by virtue of possessing a coastline. In other words, a state's coastline generates maritime projections that, depending on the distance of a maritime area from the coastline, are subject to different varieties of sovereign rights.

1. Baselines

In spatial terms, the starting point for the application of the law of the sea lies in the concept of baselines. Just as land borders demarcate where the territory of one state ends and another begins, baselines establish where the land territory of a coastal state ends and its maritime protections begin. In most cases, the baseline is determined by charting the ordinary low-tide line along a state's coast.[185] Areas seaward of the low-tide line are subject to the legal regime of the sea, while those that are landward are treated as the state's land territory.[186]

UNCLOS recognizes several special geographic circumstances that require other means of determining a baseline. When a coast is jagged or rocky, as in the case of the portion of the Norwegian coast known as the Skjærgård, a coastal state may draw "straight baselines" which may enclose limited areas of salt water and "assimilate" them to the land domain.[187] Such waters are considered "internal

183 *See* discussion *infra* Section V.B.3.

184 North Sea Continental Shelf Cases (Ger. v. Den.; Ger. v. Neth.), Judgement, 1969 I.C.J Rep. 3, ¶ 96 (Feb. 20) [hereinafter *North Sea Cases*].

185 UNCLOS, *supra* note 176, at art. 5.

186 *Id.*

187 *Id.* at art. 7.

waters" and subject to the regime of territorial sovereignty in the same manner as dry land.[188]

2. The high seas

While baselines define where a state's maritime zones begin, the high seas (also known as "international waters") are what lie beyond the limits of national jurisdiction. The contemporary international law that governs the high seas can be found in Part VII of UNCLOS, which codifies customary international law while also introducing some important innovations.[189]

Perhaps the most important provision of Part VII is Article 89, which establishes the default rule that "[n]o State may validly purport to subject any part of the high seas to its sovereignty."[190] Article 87 expands on this default rule by guaranteeing to vessels of all states six fundamental freedoms on the high seas. These are (1) the freedom of navigation, (2) the freedom of overflight, (3) the freedom to lay submarine cables and pipelines, (4) the freedom to construct artificial islands and installations, (5) the freedom to fish, and (6) the freedom to conduct scientific research.[191] The first two freedoms are cast in absolute terms, while the others are subject to restrictions found in other parts of UNCLOS.[192] Meanwhile, Article 94 speaks to the duties of flag states in regulating the conduct of vessels flying their flag in international waters, including regarding maritime safety, environmental protection, and the exercise of civil and criminal jurisdiction aboard such vessels.[193]

Most significant for present purposes is Article 112, which permits all states to lay submarine cables and pipelines on the seafloor of areas considered to be high seas.[194] Douglas Guilfoyle et al. have noted that discussions of "the right of States to exercise jurisdiction over those aspects of the material infrastructure underpinning cyberspace which are located within their territory" disregard "the fundamental fact that the backbone of cyber infrastructure—submarine

188 ROTHWELL & STEPHENS, *supra* note 171, at 53. UNCLOS also permits archipelagic states (i.e., states like Indonesia that are made up entirely of one or more archipelagos) to draw "archipelagic baselines" that connect the outermost islands of their archipelagos and claim the waters enclosed therein as "sovereign." *See* discussion *infra* Section V.B.3.

189 Perhaps its greatest innovation is the creation of a legal regime to regulate the extraction of non-living resources from the seabed and subsoil of areas beyond national jurisdiction, which is considered by UNCLOS to constitute "the common heritage of mankind." *See* UNCLOS, *supra* note 176, Part II.

190 *Id.* at art. 89.

191 *Id.* at art. 87.

192 *Id.*

193 *Id.* at art. 94.

194 *Id.* at art. 112.

telecommunication cables—is not (for the large part) located within sovereign territorial jurisdiction."[195] Even so, Guilfoyle et al. focus not on abstracting principles from the law of the sea germane to the governance of cyberspace, but rather on the narrow yet important issue of the protection of submarine cables in times of peace and war.[196] Other works in this genre—including an entire chapter of the *Tallinn Manual 2.0*[197]—consider the legalities of conducting various kinds of "cyber operations" from different areas of the sea, yet they do not consider what the law of the sea might have to teach us about the governance of cyberspace.[198]

Notwithstanding Section VII's detailed articulation of the legal regime governing the high seas, it bears mention that the extent of the high seas has shrunk enormously over the course of the 20th century. Arvid Pardo has noted that "[p]rior to World War I, the principle of freedom of the sea beyond narrow limits appeared likely to remain the foundation of the law of the sea for the indefinite future."[199] Till the middle of the last century, coastal states could extend their authority only three nautical miles out to sea, yet today some aspects of their writ can run up to 350 nautical miles from their baselines. Despite this shrinkage, the high seas account for two-thirds of the surface of the world's oceans and some 45% of our blue planet's overall surface area.[200]

3. Coastal state "sovereignty" in the territorial sea

Having gone all the way out to the high seas, let us return to the coastal state's baselines. Seaward of this legal fiction which divides the land from the sea lies the first and oldest maritime zone in which states may claim authority: the territorial sea.

The origins of the territorial sea can be found in the "battle of the books" of the early 17th century between Hugo Grotius, John Selden, and their contemporaries, which was ultimately resolved by Cornelius van Binkershoek's proclamation of the "cannon-shot rule" in 1702.[201] For more than two centuries, a consensus existed that a coastal state could exercise authority over a narrow belt of territorial sea extending no more than three nautical miles from a state's

195 Guilfoyle et al., *supra* note 53, at 658.

196 *Id.* at 661.

197 TALLINN MANUAL 2.0, *supra* note 7, at ch. 8 ("The Law of the Sea").

198 *See, e.g.*, Asaf Lubin, *The Dragon-Kings Restraint: Proposing a Compromise for the EEZ Surveillance Conundrum*, 57 WASHBURN L.J. 17 (2017). *See also* James Kraska, *Intelligence Collection and the International Law of the Sea*, 99 INT'L. L. STUD. 602 (2022).

199 Arvid Pardo, *The Law of the Sea: Its Past and Its Future*, 63 OR. L. REV 7, 12 (1984).

200 *The High Seas, an Undisclosed World*, OCÉANS CONNECTÉS (Feb. 2, 2023), https://perma.cc/H8PD-67A7 (last visited June 30, 2024).

201 Bederman, *supra* note 172, at 366–71.

baselines.[202] Today UNCLOS recognizes that coastal states may claim a territorial sea that is twelve nautical miles in breadth.[203]

Turning back to history, David Bederman reports that, at the time of The Hague Codification Conference of 1930, "it was beyond cavil that coastal States exercised sovereignty within their territorial seas," albeit "subject to the right of innocent passage by the commercial vessels of other nations."[204] The contemporaneous work of Jessup suggests that the nature of the coastal state's authority over the territorial sea was not quite so settled. Writing in 1927, Jessup sought to rebut objections to the theory that "the marginal sea[205] . . . is part of the territory of the littoral."[206] Per Jessup's account, the "primary objection advanced by those who deny [the theory] is the right of innocent passage, which they deem inconsistent with complete sovereignty."[207]

The doctrine of innocent passage, whose existence was one of the few things that Grotius and Selden appeared to agree on,[208] recognizes the right of vessels of one state to traverse the territorial sea of another, without the latter's consent or authorization. Jessup explained that innocent passage "seems to be the result of an attempt to reconcile the freedom of ocean navigation with the theory of territorial waters" that arose in the early modern period.[209] While recognizing that the right of innocent passage was "firmly established in international law" when it came to merchant vessels, Jessup noted that a "divergency of opinion" existed as to its application to warships.[210]

Today, UNCLOS Article 2 recognizes that states possess "sovereignty" over the territorial sea,[211] albeit subject to the innocent passage rights that ships of all states enjoy under Article 17.[212] UNCLOS defines "innocent passage" as the right of a ship to "traverse" the territorial sea of one state en route to the ship's

202 Pardo, *supra* note 199, at 11–12.

203 UNCLOS, *supra* note 176, at art. 3.

204 Bederman, *supra* note 172, at 373 (quoting The Barcelona Convention on the Regime of Navigable Waterways of International Concern art. 3, Apr. 20, 1921, 7 L.N.T.S. 27, 35 (entered into force Oct. 31, 1922)).

205 The term "marginal sea" was in widespread use to describe what we now call the territorial sea in the period prior to the Second World War.

206 JESSUP, *supra* note 174, at 119.

207 *Id.*

208 William K. Agyebeng, *Theory in Search of Practice: The Right of Innocent Passage in the Territorial Sea*, 39 CORNELL INT'L L.J. 371, 379–80 (2006).

209 JESSUP, *supra* note 174, at 119.

210 *Id.* at 120.

211 UNCLOS, *supra* note 176, at art. 2.

212 *Id.* at art. 17.

destination, or to proceed to and from a state's "internal waters."[213] Innocent passage does not permit foreign-flagged ships to "anchor" or "loiter"—to use Jessup's colorful terms—in the territorial sea of another state, however.[214] Rather, innocent passage must be "continuous and expeditious,"[215] and it must not be "prejudicial to the peace, good order or security of the coastal State."[216]

UNCLOS Article 21 permits coastal states to "adopt laws and regulations . . . relating to innocent passage through the territorial sea" for a set of enumerated reasons, ranging from "the safety of navigation" to "the preservation of the environment of the coastal State." In so doing, UNCLOS prohibits coastal states from "impos[ing] requirements on foreign ships which have the practical effect of denying or impairing the right of innocent passage," or discriminating against the ships of any state.[217] Since the text of UNCLOS makes no distinction between civilian and military vessels in setting out the right of innocent passage, the prevailing view among international legal scholars today is that this right applies equally to all foreign-flagged vessels.[218]

While Jessup suggested that the long-standing innocent passage regime "is properly denominated a servitude" on the sovereignty of a coastal state,[219] innocent passage so burdens the rights of coastal states that it is hard to square the concept with sovereignty. Indeed, Article 24 of UNCLOS imposes an affirmative duty on coastal states to "not hamper the innocent passage of foreign ships through the territorial sea except in accordance" with its provisions, and to refrain from measures "which have the practical effect of denying or impairing the right of innocent passage."[220] Article 27 of UNCLOS even bars coastal states from asserting their criminal jurisdiction over foreign ships exercising their right of innocent passage through the territorial sea, unless one of a number of specified conditions are met.[221] The contrast with the regime of territorial sovereignty that prevails on land is stark, inasmuch as "the principle that the courts of the place

213 *Id.* at art. 18.

214 JESSUP, *supra* note 174, at 123.

215 UNCLOS, *supra* note 176, at art. 18(2).

216 *Id.* at art. 19(1).

217 *Id.* at art. 26.

218 *See, e.g.*, Hakapää Kari, *Innocent Passage, in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, ¶¶ 29–33 (Rüdiger Wolfrum ed., 2013); ROTHWELL & STEPHENS, *supra* note 171, at 263–64.

219 JESSUP, *supra* note 174, at 119.

220 UNCLOS, *supra* note 176, at art. 24.

221 These conditions are (1) if the consequences of the crime extend to the coastal State; (2) the crime disturbs the peace of the coastal State or the good order of the territorial sea; (3) the ship's captain or the authorities of the flag state have requested the assistance of the coastal state; and (4) to suppress the trafficking of narcotics and psychotropic substances. *Id.* at art. 27.

where the crime is committed may exercise jurisdiction" is both "universally recognized" and "a reflection of the essential territoriality of sovereignty."[222]

Regardless of whether one uses the term "sovereignty" or "sovereign rights," what is clear is that the nature of the coastal state's authority in the territorial sea is far different from what it enjoys over land. Writing in the early 18th century, the Swiss diplomat and international legal publicist Emer de Vattel characterized the rights of the territorial sovereign as follows:

> The sovereign may forbid the entrance of his territory either to foreigners in general, or in particular cases, or to certain persons, or for certain particular purposes, according as he may think it advantageous to the state. There is nothing in all this, that does not flow from the rights of domain and sovereignty: every one is obliged to pay respect to the prohibition; and whoever dares to violate it, incurs the penalty decreed to render it effectual.[223]

Yet in the territorial sea, a coastal state cannot deny innocent passage even to foreign warships, nor can it exercise its criminal jurisdiction unless the requirements of UNCLOS Article 27 are met.

Innocent passage has been an integral part of the territorial sea regime since the very origins of the concept, but today there are two additional doctrines that provide foreign vessels with navigational rights in maritime areas that are otherwise subject to the "sovereignty" of a coastal state. As Rothwell and Stephens explain, "[a]s the international law of the sea came to recognize the territorial sea and new maritime zones extending further seawards, there was a need to provide certainty with respect to the freedom of navigation."[224]

Starting in the 19th century, international law began to develop a distinct legal regime to deal with international straits, which link two bodies of water that are "used for international navigation."[225] The Strait of Gibraltar, which today lie entirely within the territorial seas of Spain and Morocco, and the Bosporus, which might otherwise constitute the internal waters of Turkey, are two examples of straits which connect other significant bodies of water (the Atlantic to the Mediterranean, and the Mediterranean to the Black Sea, respectively) that international law subjects to the special legal regime of "transit passage."[226]

Following the Second World War, newly independent archipelagic states such as Indonesia and the Philippines sought international legal recognition of a

222 CRAWFORD, *supra* note 16, at 442.

223 Watts & Richard, *supra* note 18, at 832 (*quoting* EMER DE VATTEL, THE LAW OF NATIONS 308–09 (Béla Kapossy & Richard Whatmore eds., 2008)).

224 ROTHWELL & STEPHENS, *supra* note 171, at 272.

225 This definition of what constitutes an international strait is from the very first case of the International Court of Justice. Corfu Channel (U.K. v. Alb.), Judgement, 1949 I.C.J Rep. 4, 28 (Apr. 9).

226 *See generally* UNCLOS, *supra* note 176, Part III ("Straits Used for International Navigation").

special status for the waters that lay between the islands that constitute their territory.[227] Correspondingly, UNCLOS Article 47 recognizes the right of such states to draw "archipelagic baselines" that connect the outermost islands of the archipelago.[228] Article 49 states that "the sovereignty of an archipelagic state extends to the waters enclosed by the archipelagic baseline,"[229] yet the "sovereignty" of a state like the Philippines over its archipelagic waters is subject to the rights of passage that ships of all states enjoy in such waters.[230]

Today, many international lawyers fail to recognize that innocent passage has always been an integral part of the legal regime that permits states to exercise some authority over the waters off their shores. They also fail to understand that the legal regime of the territorial sea, including the concept of innocent passage, co-evolved with the regime of territorial sovereignty hundreds of years ago.

Consider the following statement by Watts and Richard, who claim that "[t]he UNCLOS innocent passage rules were agreed upon by States to balance their collective interests in maintaining the oceans as a common resource for transportation and communication with the interests of coastal States in protecting their interests and especially their territorial sovereignty."[231] Or consider the following statement by Schmitt and Vihul, who proclaim that:

> [s]tates have long enjoyed territorial inviolability vis-à-vis their coastal waters. The regimes of innocent, transit, and archipelagic passage developed as customary and treaty-law exceptions to the territorial sea's inviolability; they modify the baseline principle that maritime borders may not be pierced by other States. Territorial inviolability remains intact, subject to the exceptions.[232]

These passages suggest that the "inviolability" of a state's maritime borders is both logically and historically prior to the "exceptions" that later developed, when in fact rights of passage for foreign-flagged vessels have been an integral part of the construction of coastal state authority over adjacent maritime areas. Innocent passage has been a feature of the law of the sea for as long as international law has recognized the concept of the territorial sea, and the same goes for the parallel development of the regimes of archipelagic waters and passage in UNCLOS.

Seen in the context of human history, it is the notion that territorial sovereigns may extend their authority in some fashion over maritime areas that is

227 *See generally* Jorge R. Coquia, *Development of the Archipelagic Doctrine as a Recognized Principle of International Law*, 58 PHIL. L.J. 13 (1983).

228 UNCLOS, *supra* note 176, at art. 47.

229 *Id.* at art. 49.

230 UNCLOS, *supra* note 176, at art. 52.

231 Watts & Richard, *supra* note 18, at 846–47.

232 Schmitt & Vihul, *supra* note **Error! Bookmark not defined.**, at 1645.

exceptional. By contrast, innocent passage and related doctrines preserve the original freedom of the seas that humanity has enjoyed since the ancestors of our species first sailed the oceans blue several hundred thousand years ago.[233]

4. Sovereign rights beyond twelve nautical miles

UNCLOS uses the term "sovereign rights" to describe the nature of the authority that coastal states possess in two kinds of maritime zones that lie more than twelve nautical miles offshore their baselines. The first is the continental shelf, which is the term the law of the sea uses to describe the sovereign rights that states possess in the natural resources that are found on or beneath the seafloor. The second is the EEZ, which refers to the sovereign rights that the coastal state possesses in waters lying between 12 and 200 nautical miles from its baselines.

a) *The continental shelf*

The term "continental shelf" originates not in law but in the natural sciences, where it is used to describe the broad areas of shallow water that lie off the coasts of many of the world's continental landmasses.[234] Continental shelves are built up over geological time by sediments carried by rivers that flow into the sea.[235] These sediments often carry organic material that, under the right conditions, can be transformed into hydrocarbons over millions of years.[236]

By the mid-20th century, it was technologically feasible to drill for oil and gas in the shallow waters of the continental shelves of the Gulf of Mexico and the North Sea.[237] Correspondingly, President Truman issued a famous proclamation in 1945 which laid claim to the "natural resources of the subsoil and seabed of the

233 Archaeological evidence suggests that the capability to navigate oceanic waters "first developed between one million years and 800,000 years ago in Southeast Asia, possibly as a local adaptation to gain access to off-shore marine resources in an ecologically volatile island environment." *See* Robert G. Bednarik, *Seafaring in the Pleistocene*, 13 CAMBRIDGE ARCHAEOLOGICAL J. 41, 46 (2003). Our species (*Homo sapiens*) only evolved some 300,000 years ago, however. *See* Jean-Jacques Hublin et al., *New Fossils from Jebel Irhoud, Morocco and the Pan-African Origin of Homo Sapiens*, 546 NATURE 289 (2017).

234 The coinage of the term is generally attributed to the 19th century British geographer Hugh Robert Mill. *See* M.W. MOUTON, THE CONTINENTAL SHELF 6 (1952).

235 *See, e.g.,* Joseph R. Curray, *The Bengal Depositional System: From Rift to Orogeny*, 352 MARINE GEOLOGY 59 (2014) (describing how sediments carried by the Ganges-Brahmaputra River system from the erosion of the Himalayas by monsoon rains over millions of years has created the world's largest continental shelf in the Bay of Bengal).

236 *See generally* Wallace E. Pratt, *Petroleum on Continental Shelves*, 31 BULL. AM. ASS'N PETROLEUM GEOLOGISTS 657 (1947).

237 *See generally* Quentin Morton, *Beyond Sight of Land*, GEOEXPRO (Dec. 6, 2016), https://perma.cc/B7GT-GSUH (describing the development of deep-sea oil and gas drilling technology in the middle of the last century).

continental shelf beneath the high seas contiguous to the coasts of the United States as pertaining to the United States, subject to its jurisdiction and control."[238] However, what has come to be known as *the* Truman Proclamation hastened to add that "[t]he character as high seas of the waters above the continental shelf and the right to their free and unimpeded navigation are in no way affected."[239]

The Truman Proclamation is significant in the manner it asserts jurisdiction over the continental shelf. While the Proclamation lays claim to the surface of the seafloor (the "seabed") and what lies beneath, everything above the surface of the seafloor is conceded by the United States to be subject to the regime of the high seas—a *res communis*. Correspondingly, we have a jurisdictional claim by the United States that is intelligible not in the two dimensions of a map, but rather in three-dimensional space.

The Truman Proclamation set off an undersea "land rush" as other states sought to stake claims to waters beyond the territorial sea. Work by the International Law Commission in the early 1950s to address the growing state interest and practice of claiming jurisdiction over the continental shelf gave rise to the 1958 Convention on the Continental Shelf ("the Convention"),[240] which defined the continental shelf as constituting

> the seabed and subsoil of the submarine areas adjacent to the coast but outside the area of the territorial sea, to a depth of 200 metres or, beyond that limit, to where the depth of the superjacent waters admits of the exploitation of the natural resources of the said areas.[241]

The Convention goes on to specify that the "coastal State exercises over the continental shelf sovereign rights for the purpose of exploring it and exploiting its natural resources."[242] However, the Convention clarifies that "[t]he rights of the coastal State over the continental shelf do not affect the legal status of the superjacent waters as high seas, or that of the airspace above those waters.[243]

By 1969, the provisions of the Convention on the Continental Shelf had been recognized by the International Court of Justice as having acquired the status of customary international law. In its (second-most) famous dictum in the *North Sea Cases,* the Court noted:

> [T]he rights of the coastal State in respect of the area of continental shelf that constitutes a natural prolongation of its land territory into and under the sea

238 Proclamation No. 2667, Policy of the United States with Respect to the Natural Resources of the Subsoil and Sea Bed of the Continental Shelf, 10 Fed. Reg. 12303 (Sept. 28, 1945) https://perma.cc/2WKW-U3AU [hereinafter Truman Proclamation].

239 *Id.*

240 Convention on the Continental Shelf, *supra* note 179.

241 *Id.* at art. 1(a).

242 *Id.* at art. 2(1).

243 *Id.* at art. 3.

> exist ipso facto and ab initio, by virtue of its sovereignty over the land, and as an extension of it in an exercise of sovereign rights for the purpose of exploring the seabed and exploiting its natural resources.[244]

The passage is notable in the distinction the Court draws between the regime of territorial sovereignty that exists over the land, and the limited "sovereign rights" that a state exercises over its "natural prolongation" in the sea for the specified purposes of "exploring the seabed and exploiting its natural resources."

A more precise formula for determining the outer limits of the continental shelf was developed during the negotiations that led to the adoption of UNCLOS.[245] Article 76(1) redefines the continental shelf of a coastal state as constituting the "seabed and subsoil of the submarine areas" that extend 200 nautical miles beyond a state's baselines, or "throughout the natural prolongation of its land territory to the outer edge of the continental margin."[246]

UNCLOS Part VI establishes a complex, technical procedure by which states can claim sovereign rights over continental shelf areas more than 200 nautical miles beyond their baselines.[247] Such areas are commonly described as the "outer continental shelf" or the "extended continental shelf" (as in the diagram below). To claim such rights, a state must submit detailed geophysical data to an expert body known as the Commission on the Limits of the Continental Shelf ("CLCS").[248] As of July 28, 2024, the CLCS had received 95 submissions from 75 distinct states and issued recommendations as to 34 of them.[249]

In any case, Article 77 of UNCLOS vests in coastal states "sovereign rights" over the continental shelf for the purposes of "exploring it and exploiting its natural resources."[250] However, Article 78(1) is at pains to note that the rights of the coastal state over the continental shelf "do not affect the legal status of the superjacent waters or of the air space above those waters."[251] Moreover, Article 78(2) provides that the exercise by coastal states of their sovereign rights over the continental shelf "must not infringe or result in any unjustifiable interference with

244 *North Sea Cases, supra* note 184, ¶ 19.

245 ROTHWELL & STEPHENS, *supra* note 171, at 109.

246 UNCLOS, *supra* note 176, at art. 76(1).

247 *Id.* at art. 76.

248 *Id.* at art. 76(8).

249 *Submissions, Through the Secretary-General of the United Nations, to the Commission on the Limits of the Continental Shelf, Pursuant to Article 76, Paragraph 8, of the United Nations Convention on the Law of the Sea of 10 December 1982*, UNITED NATIONS DIVISION FOR OCEAN AFFAIRS AND THE LAW OF THE SEA (July 17, 2024), https://perma.cc/5JZB-D5UA (last visited July 28, 2024).

250 UNCLOS, *supra* note 176, at art. 77(1).

251 *Id.* at art. 78(1).

navigation and other rights and freedoms of other States as provided for in this Convention."[252]

b) *The Exclusive Economic Zone*

The Exclusive Economic Zone (EEZ) is a second species of sovereign rights that coastal states possess and enjoy in maritime zones that lie more than twelve nautical miles from their baselines. While the continental shelf regime emerged in the 1940s, the EEZ regime is a product of the negotiations that led to the conclusion of UNCLOS in 1982.[253] Whereas the regime of the continental shelf relates to sovereign rights in the seabed and subsoil of maritime areas beyond the territorial sea, the EEZ regime pertains to exploring, exploiting, conserving, and managing the living and non-living natural resources "of the waters superjacent to the seabed and of the seabed and its subsoil."[254] Furthermore, Article 56 of UNCLOS endows the coastal state with jurisdiction to establish artificial islands and structures (such as oil rigs) within the EEZ, to regulate marine scientific research, and to regulate the protection and preservation of the marine environment within the EEZ.[255]

The EEZ may extend from 12 to 200 nautical miles from a coastal state's baselines.[256] Correspondingly, unless a state is entitled to claim sovereign rights in continental shelf areas lying more than 200 nautical miles from its baselines by virtue of satisfying the criteria established in Part VI of UNCLOS, the EEZ and the continental shelf are co-extensive.[257]

Article 55 of UNCLOS, which establishes the concept of the EEZ, frames the regime in terms of a balance between "the rights and jurisdiction of the coastal State and the rights and freedoms of other States," both of which are governed

252 *Id.* at art. 78(2). There are other fascinating provisions within UNCLOS Part VI that merit mention in passing. Most significant is that States that exploit the non-renewable resources of continental shelf areas located more than 200 nautical miles from their baselines must make contributions to an annual fund from which payments shall be made to member States based on "equitable sharing criteria" that take into account "the interests and needs of developing States, particularly the least developed and landlocked among them." *See* UNCLOS, *supra* note 176, at art. 82(4). Needless to say, the notion that one state's development of resources in areas where it enjoys "sovereign rights" results in financial obligations to other States is anathema to traditional concepts of territorial sovereignty.

253 ROTHWELL & STEPHENS, *supra* note 171, at 83.

254 UNCLOS, *supra* note 176, at art. 56(1)(a).

255 *Id.* at art. 56(1)(b).

256 *Id.* at art. 57.

257 UNCLOS recognizes the first twelve nautical miles of the EEZ as a "contiguous zone" wherein the coastal State may exercise control to prevent and/or punish "infringement of its customs fiscal, immigration or sanitary laws" within its territory or its territorial sea. *Id.* at art. 31.

by the relevant provisions of UNCLOS.[258] Some of the specific freedoms that other states enjoy in the EEZ of a coastal state are specified in UNCLOS Article 58. These include the freedom of navigation and overflight and the right to lay submarine cables and pipelines.[259] In exercising these rights and freedoms, other states must have "due regard" for the rights and duties of the coastal state and abide by its laws and regulations, insofar as they are consistent with UNCLOS and general international law.[260]

Part V of UNCLOS, which establishes the regime of the EEZ, contains detailed provisions on fisheries. Article 61(1) endows the coastal state with the right to determine the allowable catch in its EEZ,[261] while Article 62 details the many ways in which coastal states may regulate the exploitation of the living resources of the EEZ by nationals of foreign states (from requiring licenses to specifying what equipment may be used to catch which fish).[262]

Lastly, Article 73 details the powers of the coastal state to enforce laws it may enact to protect its "exercise of its sovereign rights to explore, exploit, conserve and manage the living resources in the [EEZ]"—so long as such laws are enacted "in conformity" with UNCLOS.[263] Article 73(1) permits the coastal state to take measures including "boarding, inspection, arrest and judicial proceedings" to ensure compliance with its laws.[264] Arrested vessels and their crews must be promptly released upon posting of a reasonable bond or other security, however.[265] Coastal state penalties for violations of EEZ regulations may not include imprisonment absent contrary agreements between the states concerned, and coastal states must promptly inform the flag state of any such actions.[266]

All of the maritime zones described in this Section are depicted schematically in the graphic reproduced below:[267]

258 *Id.* at art. 55.

259 *Id.* at art. 58(1).

260 UNCLOS, *supra* note 176, at art. 58(3).

261 *Id.* at art. 61(1).

262 *Id.* at art. 62.

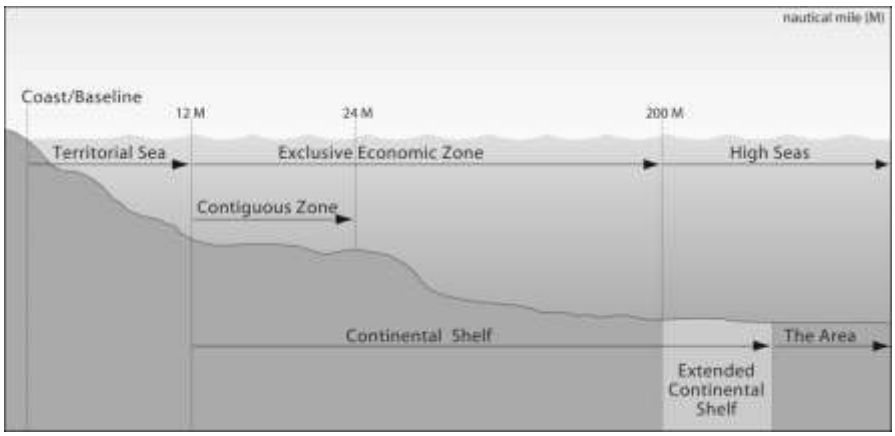
263 *Id.* at art. 73(1).

264 *Id.*

265 *Id.* at art. 73(2).

266 UNCLOS, *supra* note 176, at arts. 73(3)-(4).

267 The graphic was produced by the State Department and is available at https://perma.cc/5QG7-53XM.



5. Multi-layered maritime governance

Starting from the Truman Proclamation, one of the most interesting features of the law of the sea is how it recognizes that different states possess regulatory interests over different kinds of activities occurring at a particular latitude and longitude at sea by factoring the depth at which such activities occur.

Consider the case of a ship sailing through the EEZ. While the coastal state may enforce its laws against the foreign ship as required to protect its right to "explore, exploit, conserve, and manage" the resources of the EEZ under UNCLOS Article 56, for all other matters the law of the flag state prevails.[268]

The notion of multi-dimensional and overlapping national jurisdictions extends beyond the laws that apply to foreign-flagged vessels operating in a coastal state's maritime zones. Consider the result of the cases brought by Bangladesh[269] against its neighbors Myanmar[270] and India[271] to delimit its maritime boundaries in the Bay of Bengal. The tribunals that decided these cases awarded Bangladesh continental shelf rights in areas that lie more than 200 nautical miles from Bangladesh's baselines, yet within 200 nautical miles of its neighbors' baselines. In so doing, the tribunals created two "gray areas" in the Bay of Bengal where Bangladesh possesses sovereign rights over the continental shelf, yet Myanmar and India possess sovereign rights in the resources of the superjacent waters.

268 UNCLOS, *supra* note 176, at art. 94(1).

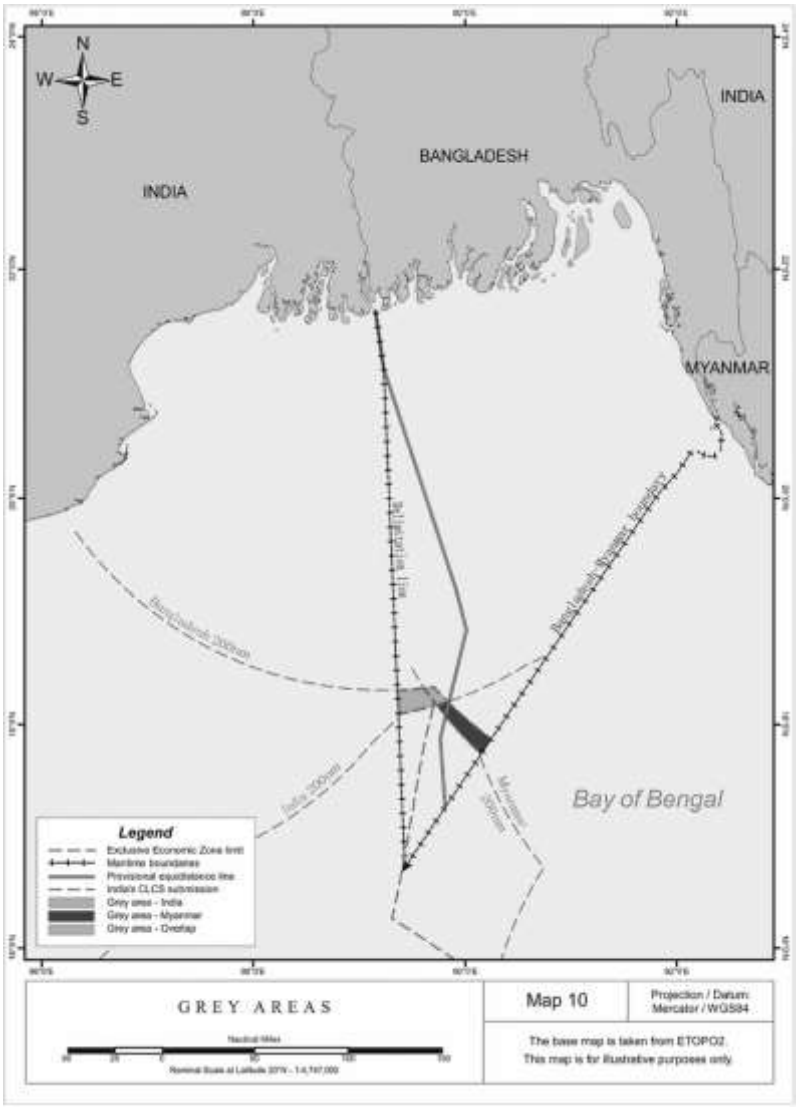
269 Full disclosure: I served as counsel to Bangladesh in both of these cases.

270 Delimitation of the Maritime Boundary in the Bay of Bengal (Bangl./Myan.), Case No. 16, Judgement of Mar. 14, 2012, 2012 ITLOS Rep. 4.

271 Bay of Bengal Maritime Boundary Arbitration (Bangl. v. India), Case No. 2010-16, Award of July 7, 2014, PCA Case Repository (Perm. Ct. Arb.), https://perma.cc/K3M4-3KUR.

These areas are depicted in green and orange respectively on the map reproduced on the next page.[272]

[272] The map is reproduced from *id.* at 159.


N
W
E
S
INDIA
BANGLADESH
INDIA
MYANMAR
Bay of Bengal
Legend
Exclusive Economic Zone limit
Maritime boundaries
Provisional equidistance line
India's CLCS submission
Grey area - India
Grey area - Myanmar
Grey area - Overlap
GREY AREAS
Map 10
Projection / Datum:
Mercator / WGS84
The base map is taken from ETOPO2.
This map is for illustrative purposes only.

A vessel that navigates to coordinates of latitude and longitude within the "gray areas" would find the following jurisdictional layer-cake, depending on their altitude relative to sea level:

The outcome of these cases seems highly anomalous when viewed from the perspective of territorial sovereignty, but it reflects the nuanced, layered approach that the law of the sea takes to jurisdiction at sea. It is consistent with how the law of the sea assigns most jurisdiction over a ship operating in another state's EEZ (or continental shelf beyond 200 nautical miles) to the flag state, while providing the coastal state with limited powers to regulate certain activities (namely the economic exploitation of natural resources).

VI. ANCHORING DIGITAL SOVEREIGNTY IN THE LAW OF THE SEA

This Section explores what the law of the sea can teach us about how we could think about the nature of state authority in the online sphere. Its first Subsection will draw lessons from the history of the law of the sea to show why the physicality of the Internet's infrastructure does not necessitate applying territorial sovereignty to all aspects of its governance. Its second Subsection will show how the key features of the law of the sea explored above—especially the concept of sovereign rights—are better suited than territorial sovereignty to reconcile national regulation of the Internet with preserving its free, open, and global character.

This is not the first work to draw analogies between the governance of the seas and of cyberspace. The *Tallinn Manual 2.0* notes how it "is sometimes suggested that [cyberspace] should be assimilated to the high seas, international airspace, or outer space in the sense of constituting a 'global commons' (a *res communis omnium*)," though it ultimately rejects this notion for "disregard[ing] the

territorial features of cyberspace."[273] Kristen Eichensehr[274] and Sean Kanuck[275] are among the scholars who have canvassed the law governing the high seas for models on how to govern cyberspace, while Corn and Taylor have pointed to "[t]he fact that states have developed vastly different regimes to govern the air, space, and maritime domains" to underscore "the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace."[276]

Yet few are the scholars who have plumbed the law of the sea to find inspiration for some of the most vexing governance challenges we find in cyberspace. One notable exception is Duncan Hollis, who has noted how the law of the sea incorporates a "spectrum" between "sovereignty and res communis" in the way it governs the oceans.[277] Indeed, Hollis explicitly contemplates the possibility of states agreeing

> to certain "sovereign rights" in cyberspace (e.g., a right to actively defend core infrastructure) at the same time as they endorse a right to free and reasonable use of digital electronic telecommunications. In other words, cyberspace might end up occupying a distinct position on the spectrum between sovereignty and stewardship based on the specific content of its accepted standards of behaviour.[278]

Yet Hollis does not further detail what form these sovereign rights might take, or what other features of the law of the sea might be useful in regulating cyberspace. Likewise, Francis Lyall details the historical development of the law of the sea in his study of how the concept of sovereignty in international law has responded to technological change.[279] Yet he does not explore how particular features of the law of the sea can be adapted to address the challenge of governing cyberspace.

A. The Emergence of Domains in International Law

The historical evolution of the law of the sea is informative on whether cyberspace can be treated as a distinct domain in international law. Conventional legal analyses dismiss this possibility in view of the Internet's physicality and the presence of so much Internet infrastructure on the territory of states. This, in turn,

273 TALLINN MANUAL 2.0, *supra* note 7, at 12.

274 Kristen Eichensehr, *The Cyber Law of Nations*, 103 GEO. L.J. 317, 340–41 (2015).

275 Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEX. L. REV. 1571, 1575–77 (2010).

276 Corn & Taylor, *supra* note **Error! Bookmark not defined.**, at 210.

277 DUNCAN B. HOLLIS, STEWARDSHIP VERSUS SOVEREIGNTY? INTERNATIONAL LAW AND THE APPORTIONMENT OF CYBERSPACE 6 (2012).

278 *Id.* at 10.

279 *See generally* FRANCIS LYALL, TECHNOLOGY, SOVEREIGNTY AND INTERNATIONAL LAW ch. 2 (2022).

furnishes a rationale for the mechanical application of territorial sovereignty (and its extraterritorial exceptions) to the digital realm. As Dapo Akande et al. have argued:

> The term 'cyberspace' is *misleading* in that cyber activities, whether carried out by states or non-state entities, do not occur in a new, virtual space. Rather, what we often call 'cyberspace' *is nothing more* than a set of information and communications technologies that enable individuals to exchange and process information more efficiently, such as the Internet and other networks. As much as software, code and data play a significant role in how these technologies operate, they are necessarily made up of physical components or hardware, such as cables, satellites, radio waves, computers and their millions of silicon circuits, as well as the individuals who build, control and use software, hardware and data. Likewise, even if these multifaceted physical components cross national borders to create an *imaginary* 'global information space', as encapsulated in terms such as 'The Cloud', 'World Wide Web', or 'Virtual Reality', these remain very much grounded in tangible physical infrastructure as well as human beings of flesh and bone that are located somewhere in the world.[280]

Akande et al.'s statement reifies the "external perspective" of the Internet that has dominated legal scholarship since the turn of the millennium. Yet in dismissing the "global information space" as "imaginary," Akande et al. disregard the Internet's internal perspective and our everyday experience of cyberspace "as a virtual world that is roughly analogous to the physical world of real space."[281] While Orin Kerr suggests in his article that "modeling the Internet's facts" for the purposes of applying the law to online phenomena "requires a choice between external and internal constructions of those facts, between physical reality and virtual reality,"[282] there's no reason that both conceptions can't be accommodated in international law.

An analogy to human consciousness is instructive here. An external perspective might suggest that our experience of consciousness is "imaginary" as it consists of "nothing more" than the electrical and chemical activity occurring within three pounds of fatty tissue encased in our skulls.[283]

Yet the materiality of consciousness in our biology does not negate the reality of our experience of consciousness. Instead, consciousness is better understood as an *emergent property* of the materiality of our biology and of the processes that

280 Dapo Akande et al., *Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond*, EJIL: TALK! (Jan. 5, 2021) (emphases added), https://perma.cc/YZL4-YHUR (last visited June 4, 2024).

281 Kerr, *supra* note 46, at 359–60.

282 *Id.* at 381.

283 The average adult brain weighs around three pounds and is 60% fat by weight. *Brain Anatomy and How the Brain Works*, JOHNS HOPKINS MED. (July 14, 2021), https://perma.cc/3KXK-4AVL (last visited June 29, 2024).

occur within our brains. In other words, consciousness arises from complex interactions among the tissues of our brains and between the brain and the nervous system that are greater than the sum of their parts.[284] Criminal law acknowledges the reality of both perspectives of consciousness in according importance to whether a person acted with the requisite *mens rea*—a concept that cannot be currently mapped onto our biology[285]—while also recognizing that materially observable phenomena (such as neurological injuries) can absolve individuals of criminal responsibility for their actions.[286] The fact that the criminal law can accommodate internal and external perspectives of our brains suggests that other areas of law—such as the international law that governs the Internet—should be able to do the same as well.

Indeed, cognitive science has much to teach the law about how our subjective experiences of the Internet are a reality that merits respect and legal protection. As Julie Cohen has explained, "[t]he human cognitive apparatus is structured to apprehend the immediate environment as three-dimensional, and to organize object perception and depth perception accordingly."[287] Correspondingly, our cognitive understanding of space "is simultaneously apprehended through embodied perception" of Cartesian space through our senses, but also "produced by our own actions" as we use the spatial metaphors that are deeply embedded into human language to make sense of the world.[288] This leads Cohen to conclude that

> [i]f embodied, experienced spatiality is hardwired, "cyberspace" too is embodied, experienced space; it cannot help but be. This conclusion matches the way Internet users understand and describe their own experiences. Specifically, "cyberspace" is experienced in terms of distances, landmarks, and juxtapositions, exactly as the theory of embodied cognition would predict.[289]

284 *See, e.g.*, Ramón Guevara et al., *Consciousness as an Emergent Phenomenon: A Tale of Different Levels of Description*, 22 ENTROPY 921(2020) (exploring whether consciousness is understandable as an emergent property of classical physical interactions between the grey matter that makes up our brains, or whether they are only fully explainable on a quantum level).

285 *See generally* Uri Maoz & Gideon Yaffe, *What Does Recent Neuroscience Tell Us About Criminal Responsibility?*, 3 J.L. & BIOSCI. 120 (2016) (noting that observational studies that seek to tie mental states to particular patterns of brain activity are correlational, not causal).

286 For a study of how neurophysiological evidence is used in the American criminal justice system to determine if an individual can be held criminally responsible for their actions, *see* Valerie Gray Hardcastle, *My Brain Made Me Do It? Neuroscience and Criminal Responsibility*, *in* THE ROUTLEDGE HANDBOOK OF NEUROETHICS (2017).

287 Julie E. Cohen, *Cyberspace As/And Space*, 107 COLUM. L. REV. 210, 227–28 (2007).

288 *Id.* at 228.

289 *Id.* at 229.

On this view, accepting the validity and the reality of the internal perspective is not to succumb to an illusion, but rather to acknowledge that the reality of most complex phenomena (from consciousness to cyberspace) is almost always a matter of perspective.

B. Land-based Technologies and Domains Beyond Land

There is also a more prosaic response to the notion that the physicality of the Internet's infrastructure on the territory of states necessarily requires the application of territorial sovereignty to its governance. Were it the case that the presence on land of the infrastructure we use to access other domains subjects them to the iron grip of territorial sovereignty, then there could be no distinctive law of the sea. For as creatures that evolved to live on the land, we depend entirely on land-based infrastructure to access the seas. Boats are built of materials we harvest from the land, and practically every maritime voyage begins and ends on the land territory of a state.[290] Yet this has not foreclosed the treatment of the sea as a distinct domain that is governed by a different legal order from that which prevails on land.

Sean Kanuck has suggested that a critical consideration "when comparing and contrasting cyberspace to existing legal commons" such as the oceans and outer space is that "the medium itself, while subject to the natural laws of physics, has in essence been generated by mankind."[291] This is certainly true, yet our ability to exploit domains beyond the land—from the seas to outer space to the electromagnetic spectrum—turns on the technologies we have developed (e.g., boats, rockets, and transmitters) that allow us to transcend the limitations of our bipedal bodies.

Ultimately, all law is socially constructed, and our construction of the sea and of outer space as domains that merit different treatment than the land ultimately arises from a complex mixture of historical contingency and social utility. So even though the land, the sea, outer space, cyberspace, and the electromagnetic spectrum are *nothing more* than different arrangements of the same matter and energy that make up everything in the known universe, we treat them distinctively in the law because we find it useful to do so. Current international law (*lex lata*) may not yet recognize the distinctiveness of cyberspace, yet it is within our power to think differently and place future law (*lex ferenda*) on a different course.

290 The exception, of course, would be voyages that begin and/or end in Antarctica.

291 Kanuck, *supra* note 275, at 1576–77.

C. Law of the Sea Lessons for International Cyberlaw

The law of the sea offers an attractive model for balancing the preservation of the free, open, and global nature of the Internet with the need for national governments to exercise jurisdiction in the online sphere to achieve legitimate policy goals. Analogies drawn from the law of the sea offer the possibility of reconciling the physicality and territoriality of the Internet's architecture—its external perspective—with the "internal perspective" we experience when we go online and feel a sense of freedom as we navigate the limitless expanse of cyberspace.

1. The limited nature of sovereign rights

First and foremost, the limited nature of the sovereign rights that states possess over the maritime areas beyond their shores offers a better framework than territorial sovereignty for conceptualizing the nature of the authority that states should be permitted to exercise in cyberspace. Unlike territorial sovereignty, which gives states near-plenary authority over their land territory, sovereign rights at sea are always subject to the rights of other states (and of vessels flying their flags) to engage in peaceful uses of maritime areas subject to a coastal state's jurisdiction.

As shown in the previous Section, a coastal state may not interfere with the innocent passage rights of foreign-flagged vessels—including warships—in the territorial sea, even though UNCLOS Article 2(1) recognizes the "sovereignty" of coastal states in maritime areas lying within twelve nautical miles of their baselines.[292] Furthermore, in the EEZ, foreign-flagged vessels enjoy significant navigational freedoms so long as they give "due regard to the rights and duties of the coastal State" and comply with those of its laws that may be applicable within the EEZ.[293] By contrast, outside the Schengen Area in Europe,[294] practically the only situation where foreigners possess an international legal right to enter the territory of another state is if they meet the definition of a refugee.[295]

292 *See* discussion *infra* Section V.B.3.

293 *See generally* UNCLOS, *supra* note 176, at art. 58.

294 The European Union's Schengen Convention has practically eliminated border controls between 26 of its 27 members (Ireland being the sole exception) along with Iceland, Norway, and Switzerland. *See* Convention Implementing the Schengen Agreement of June 14, 1985 Between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the Gradual Abolition of Checks at the Common Borders, June 14, 1985, 30 I.L.M. 68.

295 International human rights law prohibits states from arbitrarily interfering with the rights of their nationals to re-enter their country but is silent on the rights of foreigners to enter the territory of a state. *See* ICCPR, *supra* note 101, at art. 12. By contrast, the 1951 Refugee Convention prohibits states from imposing penalties on refugees who unlawfully cross a border to seek refugee status

To be sure, international human rights law also prohibits states from interfering with the rights of individuals subject to its jurisdiction from accessing foreign "expression," "information," and "ideas" unless its restrictions satisfy the three-part test set out in Article 19 of the ICCPR.[296] Yet international human rights law contains no analogous provisions restricting the ability of states to prevent foreign nationals from accessing ICT infrastructure on their territory—even if such access is harmless. The power of states to do so arises from the view that "[s]tates have the right, pursuant to the principle of sovereignty, to disconnect from the Internet, in whole or in part, any cyber infrastructure located on their territory, subject to any treaty or customary international law restrictions, notably in the area of international human rights law."[297]

The *Tallinn Manual 2.0* reflects the current international consensus that states owe human rights obligations only to individuals subject to their "power and effective control."[298] Correspondingly, unless state restrictions on the ability of foreigners to access its ICT infrastructure can be conceptualized as a violation of the human rights of persons subject to its jurisdiction, current international law provides no recourse if a foreign state were to impose measures to keep foreigners out of its patch of cyberspace.[299]

The African Union's view that the "unauthorized access" by foreigners of ICT infrastructure located within a state violates sovereignty, even when such access causes no harm,[300] is even more troubling for the possibility of preserving a free and open global Internet. If international law imposes no limits on the ability of a state to exercise its sovereignty to restrict access, then the ability of foreigners to access ICT infrastructure located on the territory of a foreign state depends entirely on the foreign government's *noblesse oblige*.

(art. 31) and prohibits states from expelling such refugees to territories where their lives would be endangered (art. 33). *See* Convention Relating to the Status of Refugees, July 28, 1951, 198 U.N.T.S. 137.

296 ICCPR, *supra* note 101, at art. 19.

297 TALLINN MANUAL 2.0, *supra* note 7, at 13.

298 *Id.* at 184.

299 In fairness, the expert authors of the *Tallinn Manual 2.0* disagreed on whether one State A owes human rights obligations to a national of State B who hosts a website on a server located in State A. The hypothetical considered by the experts hinges on a cyberattack by State C that prevents access to the website. The majority view was that State A's obligation to protect human rights does not extend to the website in this case, based on the notion that the author of the website is outside the power and effective control of State A. By contrast, "the remaining Experts took the position that the obligation to protect is also triggered if the international human right concerned is being exercised within territory under the State's effective control, irrespective of whether the individual is located within that territory." *Id.* at 198.

300 *See supra* text accompanying notes 131–32.

If the preservation of a free and open global Internet that permits a Canadian to read an Indian newspaper, or an Australian to use Internet telephony to call a friend in Argentina, is something that we wish to preserve, then international law needs to rise to the occasion. Hence just as the concept of sovereign rights at sea recognizes the right of foreign vessels to navigate through a state's maritime zones for various purposes, the application of a sovereign rights framework to cyberspace would recognize that foreigners have some positive rights under international law to access ICT infrastructure located on the territory of another state.

2. The utility of baselines

Yet how precisely are we to tell where the rights of foreigners to access information resources located on the territory of a foreign state apply? And how would we reconcile this principle with the fact that nearly every object in our day and age that operates using electrical power—from cat feeders to pacemakers—is an Internet-connected thing?

Here we can draw inspiration from the concept of baselines in the law of the sea. Baselines demarcate where the application of the law of the sea begins. Baselines often enclose significant areas of salt water that are treated as "internal waters" and subject to the undiluted version of sovereignty that applies on land.[301] Internet law could develop a similar legal doctrine that recognizes that some kinds of Internet infrastructure might constitute the "internal cyberspace" of a state, and hence subject to the full sovereignty of a state, as opposed to a regime of sovereign rights that might apply in other circumstances (wherein foreign users would be endowed with more rights).

The treatment in UNCLOS of port infrastructure offers an informative analogy. Pursuant to Article 11, port infrastructure that extends into the territorial sea (such as a jetty) is considered to form a part of a state's coastline and therefore its land territory, even though such infrastructure is manifestly out at sea.[302] Likewise, while a state might be viewed as exercising territorial sovereignty over the physical infrastructure located in its territory, the Internet traffic that makes use of such infrastructure could be regulated pursuant to a regime of sovereign rights. Another option might be to permit states to declare certain kinds of infrastructure to be subject to its full sovereignty and to a complete right to exclude foreign Internet traffic due to its nature. Such a rule might apply to electronic networks that many states use for national security and civil defense purposes, or to critical infrastructure (such as electrical generation and distribution) that happens to be connected to the Internet. When it comes to such

301 UNCLOS, *supra* note 176, at art. 8.

302 *Id.* at art. 11.

networks, any foreign access—no matter how harmless—might be deemed to be a violation of a state's territorial sovereignty.

3. A sliding scale of sovereign rights

The concept of baselines can be coupled with the variegated nature of sovereign rights that one finds in the law of the sea to tailor precisely how a state exercises its authority over various aspects of cyberspace.

We have seen how a state's sovereign rights diminish as we move toward the high seas, where international law recognizes only the regulatory authority of flag states over their vessels (with exceptions to combat such harms as piracy, slavery, and trafficking). By analogy, we can divide the regions of cyberspace that lie beyond a state's digital baselines into functional zones inspired by the law of the sea.

Certain online phenomena closely linked to a state's land territory could be regulated like the territorial sea, wherein foreigners' rights of access would be limited. This approach could apply to foreigners' access to Internet endpoints on infrastructure within the state. In such cases, similar to the maritime regime of innocent passage, a state could require that access not harm its peace, good order, and security, as outlined in UNCLOS Article 19(1).[303] By contrast, the use of Internet infrastructure within a state to connect endpoints located outside that state might be subject to a more limited set of sovereign rights, such as the regime we find in the EEZ—where the navigational rights of foreign vessels are considerably stronger.

4. Overlapping sovereign rights

The variable configuration of the sovereign rights we find at sea, combined with the ability of maritime zones to overlap in three dimensions, offers some intriguing possibilities for cyberspace governance in view of the layered nature of the Internet. As we saw in the previous Section, the Truman Declaration's assertion of sovereign rights in the seabed and subsoil of the continental shelf was without prejudice to the character of the superjacent waters as high seas.[304] Likewise, in the Bay of Bengal, the sovereign rights of Bangladesh in the resources of the continental shelf coexist with the sovereign rights of India and Myanmar in the resources of the superjacent waters.[305] Hence, by analogy, we might consider assigning different configurations of sovereign rights to different states over the different layers that constitute the Internet.

303 UNCLOS, *supra* note 176, at art. 19(1).

304 *See supra* text accompanying notes 238–39.

305 *See* discussion *supra* Section V.B.5.

Unlike older communications technologies, the Internet has a modular rather than a monolithic design. Consider the conventional telephone network, whose monolithic nature is aptly illustrated by turning the clock back to 1947—the year that the transistor was invented.[306] Back then, the telephone could be used for precisely one application—voice communications[307]—and everything from the handset in your home to the telephone exchange was owned and operated by just one monopoly provider (such as AT&T in the U.S.). Telephone handsets were generally hardwired into a provider's network,[308] and under the prevailing law of the time, one could not attach any equipment to the telephone network without a provider's permission.[309]

By contrast, the Internet has always had a modular architecture that permits many different devices—from laptops to gaming consoles to pacemakers and industrial robots—to interconnect with each other using very different physical media (radio waves, copper cables, fiber optics) to access a vast range of applications (from web access to email to videoconferencing, music streaming, and whatever might constitute the next "killer app"). This is possible due to the Internet's embrace of a design principle known as *protocol layering*, whereby the different tasks associated with moving a communication from origin to destination are divided into "layers" that stack upon one another.[310] This modular approach simplifies networked communications by separating the tasks associated with delivering a communication into manageable parts. Each layer is responsible for a specific aspect of the overall communications process, and it only interacts with the layers that are adjacent to it.[311] The layered approach permits innovation within each layer, so long as the innovations conform with the requirements of making the modular architecture work.[312]

In network engineering, a protocol is a set of standardized rules for formatting and processing data that allows computers to communicate with one another.[313] Network engineers typically conceptualize the protocols that give rise

306 For a fascinating account of the invention of this world-changing device, *see* JON GERTNER, THE IDEA FACTORY: BELL LABS AND THE GREAT AGE OF AMERICAN INNOVATION ch. 5 (2012).

307 GOLDSMITH & WU, *supra* note 49, at 23.

308 Indeed, the modular RJ-11 connector that readers of a certain age may have used to plug telephone handsets into a building's wiring was not invented until the late 1960s. *See RJ Connector*, CRYPTO MUSEUM (Apr. 15, 2024), https://perma.cc/LGZ9-X2HV (last visited June 27, 2024).

309 *See* Hush-A-Phone Corp. v. United States, 238 F.2d 266 (D.C. Cir. 1956) (overruling an FCC decision prohibiting customers from attaching a mechanical device to their telephone handsets to reduce external noise).

310 Christopher S. Yoo, *Protocol Layering and Internet Policy*, 161 U. PA. L. REV. 1707, 1718–20 (2013).

311 *Id.* at 1719–20.

312 *Id.* at 1726.

313 *What Is a Protocol?*, CLOUDFLARE, https://perma.cc/7HBQ-ZTE7 (last visited June 27, 2024).

to the contemporary Internet as a "stack" consisting of five layers of protocols.[314] Engineers refer to this stack as the "Internet protocol suite" or the "TCP/IP protocol stack,"[315] and it is usually visually depicted as follows:

Application
Transport
Network
Data Link
Physical

At the top of the stack is the *application layer,* where one finds the protocols that define the many applications that use the Internet to route communications from origin to destination. For example, the Simple Mail Transfer Protocol (SMTP) defines the operation of email,[316] while the Hypertext Transfer Protocol (HTTP) defines the operation of the World Wide Web.[317] Modern applications such as Zoom leverage multiple open-source and closed-source protocols to achieve their complex functionality.[318]

At the bottom of the stack we find the *physical layer,* which consists of the underlying physical media through which information is transmitted from origin to destination—such as radio waves (as with Wi-Fi and Bluetooth), pulses of light (through fiber optic cables), or electrical impulses (such as through ethernet, telephone, or coaxial cables).[319]

For their part, protocols at the *data link* layer ensure that data moves smoothly between devices on the same physical network (e.g., your home Wi-Fi network, or an office ethernet network) and that multiple devices can use the same

314 *See, e.g.*, *TCP/IP Protocols*, IBM AIX 7.3 DOCUMENTATION (May 22, 2024), https://perma.cc/2N6C-2M8N (last visited June 30, 2024); *see also Introducing the Internet Protocol Suite*, ORACLE SYS. ADMIN. GUIDE, VOLUME 3 (2010), https://perma.cc/V2NS-CXUV (last visited June 30, 2024).

315 *Introducing the Internet Protocol Suite*, *supra* note 314.

316 JONATHAN B. POSTREL, RFC 788: SIMPLE MAIL TRANSFER PROTOCOL 1 (RFC No. 788, 1981), https://perma.cc/YAB2-E7BH (last visited June 27, 2024).

317 TIM BERNERS-LEE ET AL., HYPERTEXT TRANSFER PROTOCOL – HTTP/1.0 1 (RFC No. 1945, 1996), https://perma.cc/GJ5N-8A4Z (last visited June 27, 2024).

318 ZOOM VIDEO COMMC'NS INC., ZOOM CONNECTION PROCESS WHITEPAPER 4 (2020), https://perma.cc/R77F-TPN9 (last visited May 9, 2024) (explaining how Zoom "offers multiple connection paths utilizing various protocols across a geographically distributed infrastructure to ensure a successful connection for all users.").

319 *Introducing the Internet Protocol Suite, supra* note 314.

connection to the wider Internet without collisions or other problems.[320] Meanwhile, protocols at the *transport* layer take information from the application layer and prepare it for transport over the Internet, while also passing along information received from the Internet and routing it to the proper application.[321]

The key to making this modular architecture work is the *network layer* and in particular the Internet Protocol, which was designed by Vint Cerf and Robert Kahn in 1974[322] to solve the then-intractable problem of networking different devices using different physical media for communication.[323] The Internet Protocol defines how every Internet-connected device obtains a unique address, specifies how information to be transmitted over the Internet shall be divided into "packets" containing origin and destination information, and how such packets shall be routed through the Internet to reach their destination.[324]

The layered nature of the Internet opens the possibility of assigning different configurations of sovereign rights to govern each layer. While states might rightfully claim that the physical layer lies within their "digital baselines" and claim territorial sovereignty over the same, a more limited conception of sovereign rights might apply to the transport layer. Such a conception would recognize the inherent right of any two devices connected to the Internet to exchange information with each other, unless doing so threatens the "peace, good order or security" of the state.[325]

Such a legal doctrine is important in view of the underappreciated fact that *all* Internet communications involve the two-way exchange of information. Consider the difference between conventional TV broadcasting and streaming video. In the former, a broadcaster "pushes" content onto the airwaves that is then received by any TV set within range when the viewer tunes in. By contrast, it is the user who chooses what to watch on Netflix when they wish to chill, thereby initiating the flow of data from Netflix's servers to the viewer's device.

Questions often arise at the application layer regarding whether and how national law should apply regulating content—such as whether Pakistan can block access to Wikipedia because it contains articles that the local authorities view as

320 Andrew Froehlich, *What Is the Data Link Layer?*, TECHTARGET (Nov. 2023), https://perma.cc/63Z3-GCMH (last visited July 8, 2024).

321 *Internet Transport-Level Protocols*, IBM AIX 7.3 DOCUMENTATION (May 22, 2024), https://perma.cc/8ZBA-EFL5 (last visited June 30, 2024).

322 Vint Cerf & Robert Kahn, *A Protocol for Packet Network Intercommunication*, 22 IEEE TRANS. ON COMMC'NS. 637 (1974).

323 Yoo, *supra* note 310, at 1735.

324 *Introducing the Internet Protocol Suite*, *supra* note 314. Two additional network-layer protocols (the Internet Control Message Protocol (ICMP) and the Address Resolution Protocol (ARP)) work alongside the Internet Protocol to make Internet communications work. *Id.*

325 UNCLOS, *supra* note 176, at art. 19(1).

"sacrilegious,"[326] or what actions Facebook must take to comply with Thailand's draconian *lèse-majesté* laws.[327] We can debate whether territorial sovereignty or some more limited conception of sovereign rights should apply to national regulation at the application layer, yet there is a strong case for subjecting the transport layer to a more limited conception of sovereign rights—as the ability of any two Internet-connected devices to exchange information with each other is essential to the maintenance of a free and open global Internet.

Likewise, there is a strong case to be made that a concept other than territorial sovereignty should apply to the governance of the Internet's network layer. In recent years, authoritarian regimes such as Russia and China have made moves to have the International Telecommunications Union—an intergovernmental body—take control of the governance of the network layer of the Internet[328] from the multi-stakeholder approach that has prevailed ever since the origins of the commercial Internet in the 1990s.[329] These efforts have not yet been successful,[330] yet the current response of democratic governments to these maneuvers is inadequate. Lofty declarations by governments stating their commitment to Internet freedom are well and good,[331] yet it would be better if such governments turned their commitments into binding international law. The law of the sea offers several possibilities as to how this might be achieved.

Christopher Yoo has cautioned against "using regulation to enshrine any particular [network] architecture into law" and of treating "any particular layered architecture as if it were a natural construct."[332] The existing Internet Protocol suite certainly has its shortcomings—including that it was not designed with security and privacy considerations in mind. Indeed, efforts are under way to revise the operation of key aspects of the Internet protocol suite to achieve a range of design goals, including improved security and privacy.[333]

326 Irfan Sadozai, *PTA Bans Wikipedia in Pakistan Over 'Sacrilegious Content': Spokesperson*, DAWN (Feb. 4, 2023), https://perma.cc/XL9V-2PV6 (last visited June 30, 2024).

327 *Thailand Warns Facebook to Block Content Critical of the Monarchy*, BBC NEWS (May 12, 2017), https://perma.cc/ML4A-KPJQ (last visited June 27, 2024).

328 *See generally* Stacie Hoffmann et al., *Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet*, 5 J. CYBER POL'Y 239 (2020).

329 *See generally* LAURA DENARDIS & MARK RAYMOND, THINKING CLEARLY ABOUT MULTISTAKEHOLDER INTERNET GOVERNANCE (2013), https://perma.cc/3S9A-5FLL (last visited June 30, 2024).

330 Justin Ling, *The Election That Saved the Internet from Russia and China*, WIRED (Oct. 2022), https://perma.cc/YJ87-6P6V (last visited June 30, 2024).

331 *See* discussion *supra* Section IV.B.

332 Yoo, *supra* note 310, at 1769.

333 *See, e.g.*, Vivek Krishnamurthy, *Are Internet Protocols the New Human Rights Protocols? Understanding 'RFC 8280 – Research into Human Rights Protocol Considerations*, 4 BUS. & HUM. RTS. J. 163 (2019).

Even so, modularity and protocol layering are likely to remain fundamental design principles of communications networks for the foreseeable future. As Barbara van Schweick has explained, the complexity of designing communications networks is greatly simplified by decomposing "the functionality required for communicating" into "components and subcomponents by means of modularity and a version of the layering principle."[334] Correspondingly, international law can take cognizance of the broad strokes of these design principles to tailor the nature of state authority to the realities of layered communications architectures.

VII. CONCLUSION

There is much despair in the world today over the state of the Internet. Freedom House reports that global Internet freedom declined for the 13th consecutive year in 2023, and as the rise of artificial intelligence has begun to dominate the global digital policy agenda, there are concerns on how this powerful new technology will be enlisted by the forces of digital authoritarianism to further surveil and censor the Internet.[335] "It's time to let go of the global internet dream" proclaims the headline of a *Financial Times* op-ed that calls on democratic governments to "step up and regulate the online world as it is, rather than how they want it to be."[336]

It may seem odd to suggest that the law of the sea has anything to teach us about how we can preserve and protect global Internet freedom when its ability to govern the oceans faces challenges from forces as diverse as climate change to the outlandish claims of a revisionist China in the South China Sea.[337] The law of the sea has its shortcomings, yet the purpose of this Article is not to suggest that we should apply it hook, line, and sinker to address the global governance challenges we find in cyberspace. Rather, it is to expand our decision space in thinking about such problems by showcasing the richness of the approaches that current international law embodies to govern two-thirds of our planet's surface area.

As for the gloom many feel about the future of a free and open global Internet, we must remember that the sky is often darkest just before the dawn. And it is in those dark moments that the need for new thinking about old problems is especially important. Franklin Delano Roosevelt's *Four Freedoms* may

334 BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION 50 (2010).

335 Allie Funk et al., *The Repressive Power of Artificial Intelligence*, FREEDOM HOUSE, https://perma.cc/HFW5-ZX6L (last visited June 29, 2024).

336 Marietje Schaake, *It's Time to Let Go of the Global Internet Dream*, FIN. TIMES (July 11, 2023), https://perma.cc/Z299-EWWH (last visited July 11, 2024).

337 China's claims and their illegality under international law are detailed in Bernard Oxman, *The South China Sea Arbitration Award*, 24 U. MIAMI INT'L & COMP. L. REV. 235 (2017).

have seemed fanciful when he announced them at the height of the Second World War, yet they formed the moral core of the new international order that arose in the war's aftermath.[338] Hence, accepting today's online world as it is should not discourage us from thinking of how we would like the world to be when the tides of history turn.

338 *See generally* Mark R Shulman, *The Four Freedoms: Good Neighbors Make Good Law and Good Policy in a Time of Insecurity*, 77 FORDHAM L. REV. 555 (2008) (explaining the influence of Roosevelt's Four Freedoms on the foundations of the rules-based postwar international world order).