ON THE POLITICS AND IDEOLOGIES OF THE SOVEREIGNTY DISCOURSE IN CYBERSPACE

HENNING LAHMANN*

This article critically examines the current discourse on the legal status and substance of the international law concept of "sovereignty" in cyberspace against the backdrop of conflicting political-ideological attitudes. It first traces the origins of the interpretation of "respect for sovereignty" as a primary rule of international law, and then discusses two approaches to cyberspace that challenge the emerging consensus: "cyber imperialism," embodied by the US and the other Five Eyes members on the one hand, and "cyber-Westphalia," represented by China, Russia, and Iran on the other. Both groups conceive cyberspace in ways fundamentally irreconcilable with prevailing legal views. A third group of states endorses the "sovereignty-as-rule" understanding but leaves this legal position vulnerable to both authoritarian co-optation and imperialist dismissal.

This article contributes to the discussion on sovereignty by offering an alternative interpretation of state practice and international jurisprudence that constructs sovereignty as a principle with derivative primary rules. It shows that, despite not by itself having the status of a rule, the principle of sovereignty allows for the identification of rules that protect the territorial integrity and political independence of states beyond the traditional notions of the prohibition of intervention and the use of force. It carefully analyzes evidence in existing practice in support of this novel, doctrinally more precise understanding of sovereignty. Based on the argument's legal implications, it concludes with an assessment of the policies of "persistent engagement" and "cyber sovereignty."

* Henning Lahmann is a Hauser Global Postdoctoral Fellow, NYU School of Law; Program Leader International Cyber Law, Digital Society Institute, ESMT Berlin; Associate Research Fellow, Geneva Academy of International Humanitarian Law and Human Rights. The article is based on a paper presentation at the ESIL Karków-Leiden Symposium "Exploring the Frontiers of International Law in Cyberspace" in December 2020. I would like to thank the organizers of the symposium, especially Przemysław Roguski, as well as Isabella Brunner, Talita de Souza Dias, and Antonio Coco.

INTRODUCTION

Given the persistent controversy around the issue both in academia and among states, it is appropriate to once again critically examine the current discourse on "sovereignty" in the context of the application of international law to cyberspace against the backdrop of conflicting political-ideological attitudes. International legal discourse has struggled to apply the existing body of general international law to the growing issue of offensive, state-led cyber conflict. Unlike the traditional rules of the prohibition of the use of force and the principle of non-intervention, the legal status and substance of "sovereignty" remains contentious. Following the influential deliberations of the international group of experts that drafted the text of the Tallinn Manual 2.0, discussions have mostly revolved around the question of whether sovereignty is to be considered a primary *rule* of international law or rather merely a *principle*.

This discourse is surveyed against the backdrop of diverging conceptions of sovereignty among different groups of states that inform and structure the ongoing legal discussions on the application and interpretation of international law in cyberspace in various fora, such as the United Nations

Group of Governmental Experts on Advancing responsible State Behavior in Cyberspace in the Context of International Security (UN GGE) and the UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG). I argue that the common perception of an ideological-political bifurcation between a "Sino-Russian" approach on the one hand and a Western or "likeminded" on the other, supposedly representing "the liberal world order,"[1] falls short. This perception does not appropriately account for the possibility to identify a third approach. Indeed, accepting that the discourse is in fact trifurcated has important implications for the attitudes and trajectory of the "Sino-Russian" camp on the one hand and for the further clarification of the legal status and substance of sovereignty among liberal-democratic states on the other.

After tracing the doctrinal origins of the interpretation of "respect for sovereignty" as a primary rule of international law, the subsequent sections examine three broad trajectories among states' attitudes toward the status of sovereignty in cyberspace under international law. Before addressing the legal opinions of the growing number of states that have endorsed the "sovereignty-as-rule" position, I investigate two categories of states that, for political-ideological reasons, conceive cyberspace in ways fundamentally irreconcilable with this emerging consensus: "cyber imperialism," embodied by the U.S. and its closest allies, and "cyber-Westphalia," as represented by China, Russia, and Iran.

Following that analysis, the article critically scrutinizes the conception of sovereignty as a primary rule from the perspective of both legal policy and doctrine, arguing that this legal position is vulnerable to both authoritarian co-optation and imperialist dismissal. While there can be no doubt that it is possible to understand "respect for sovereignty" as a primary rule of international law, as a legal strategy aimed at defining the limits of permissible state behavior in cyberspace it ultimately obscures more than it clarifies. Moreover, it fails to safeguard essential human rights guarantees online, such as freedom of information and freedom of expression. Crucially, the article shows that even in the absence of a "rule of sovereignty," states are not left without legal protection against adversarial state behavior in cyberspace below the thresholds of coercion and force. A rigorous examination of international practice reveals several applicable primary rules derived from the *principle* of sovereignty that are suitable to fulfill a protective function. In particular, I contend that there is an identifiable argumentative structure in

1. DENNIS BROEDERS, LIISI ADAMSON & ROGIER CREEMERS, HAGUE PROGRAM FOR CYBER NORMS, A COALITION OF THE UNWILLING? CHINESE & RUSSIAN PERSPECTIVES ON CYBERSPACE 1 (2019).

international practice that allows for the identification of primary rules protecting the territorial integrity and political independence of states beyond the traditional notions of the prohibition of intervention and the use of force. Such an interpretation is ultimately better suited to account for the nuances that are needed to adequately assess the international legal implications of the different doctrinal approaches. At its conceptual core, sovereignty is not a rule but a principle, constituting the foundation of, and informing the interpretation of, primary rules that are necessary to decide singular cases of contentious state conduct in cyberspace.

Building on the more precise understanding of sovereignty, this article analyzes the legal implications of the most significant doctrines implemented by the states from the "cyber imperialist" and "cyber-Westphalian" camps. Regarding the former, with "defend forward"— "disrupt[ting] or halt[ing] malicious cyber activity at its source"[2]—and "persistent engagement" as the underlying concepts, "based on the idea that adversaries are in constant contact in cyberspace,"[3] represents the quintessential embodiment of an imperialist conception of cyberspace. Concerning the "Westphalian" approach, "cyber sovereignty," which can be described as "the notion that the government of a sovereign nation should have the right to exercise control over the internet within its own orders, including political, economic, cultural, and technological activities,"[4] actualizes the vision of a Westphalian order in cyberspace.

I. THE EXPERTS HAVE SPOKEN: IDENTIFYING "SOVEREIGNTY AS A RULE"

For anyone tackling the international legal issues surrounding state conduct in cyberspace, there has been no way around the Tallinn Manual 2.0 since it came out in 2017.[5] The Manual aspires to present a comprehensive yet restrained compilation of consolidated opinions reflecting the current state of the law applicable to cyberspace. Despite this rather modest outlook, its impact has been impressive. Although states were initially reluctant to engage with the Manual, they started to refer to it frequently in their official statements[6] while academics readily discussed the Manual's findings from

2. U.S. DEP'T OF DEF., CYBER STRATEGY SUMMARY 1 (2018).

3. CYBERSPACE SOLARIUM COMM'N, FINAL REPORT 137 (2020).

4. Elliot Zaagman, *The Age of Cyber Sovereignty?*, WAR ON THE ROCKS (Aug. 18, 2020), https://warontherocks.com/2020/08/the-age-of-cyber-sovereignty/.

5. NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

6. *See generally* Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583 (2018).

the start.

Alongside a generally rather traditional approach to the relevant rules, one of the most enduringly contentious debates concerns the Manual's treatment of sovereignty. The notion lays the foundation of the entire body of applicable law, emphasized by its preeminent position in the very first rule of the Manual: "The principle of State sovereignty applies in cyberspace."[7] That sovereignty takes effect in this domain had already been confirmed in the 2015 UN GGE report, which stated that "[s]tate sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory."[8] But the Manual took the concept a step further; rather than framing sovereignty as merely a "principle" that serves as the basis for primary rules of international law, it explicitly asserts that sovereignty—or, rather, "respect for sovereignty"—is by itself a primary *rule* whose violation leads to international responsibility absent the breach of a more specific rule that flows from or is otherwise closely linked with the principle of sovereignty, such as the prohibition of the use of force or the principle of non-intervention.[9]

The Manual's framing of sovereignty as a rule suggests that the technical peculiarities of the novel domain of cyberspace prompted the experts to look for legal standards that might be suitable to regulate state conduct below the thresholds of "coercion" and "force" that define the more pertinent prohibitions of intervention and the use of force. Given the fact that the "virtual" environment of globally interconnected networks provides ample opportunity to harm another state's interests, there was a growing need for some rule that could proscribe reckless operations that did not reach the legal thresholds of coercion or force. Without such rule, the international legal order risked remaining without meaningful effect in cyberspace. Accordingly, the experts responsible for the Manual determined that violations of the rule of sovereignty by way of cyber operations could come about either by amounting to a significant "infringement upon the target State's territorial integrity," for example by causing physical damage or the substantial loss of functionality of cyber infrastructures, or by constituting "an interference with or usurpation of inherently government functions."[10]

The Manual's scarce evidence of custom substantiating its assertion of

7. TALLINN MANUAL 2.0, *supra* note 5, at 11.

8. Rep. of the Group of Governmental Experts on Devs. in the Field of Info. and Telecomm. in the Context of Int'l Sec., at 14, UN Doc. A/70/174 (2015).

9. *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, Judgment, 1986 I.C.J. 14, ¶ 212 (June 27).

10. TALLINN MANUAL 2.0, *supra* note 5, at 20.

sovereignty as a primary rule led to initial objections in the academic literature.[11] In subsequent scholarly articles, however, a number of the group's members followed up with more detailed elaborations to support the conclusions.[12] For instance, Michael N. Schmitt and Liis Vihul stated that the International Court of Justice (ICJ) repeatedly referred to "sovereignty" as a primary rule over the course of its existence, which is seen in the decisions in *Corfu Channel*[13] and *Nicaragua.*[14] According to the authors, the UN Security Council likewise invoked a "violation of the sovereignty of a Member State" after Israeli agents had captured the fugitive Holocaust organizer Adolf Eichmann on Argentinian territory in 1960.[15] Since the Manual's publication, the "sovereignty-as-rule" argument has made remarkable inroads. Although endorsement is not unanimous, most international lawyers dealing with cyber issues seem to agree that the prospect of novel forms of state conflict in and through the virtual domain calls for a legal approach that transcends the traditional focus on intervention and the use of force, and they propose sovereignty as the obvious candidate.[16] Today, it is reasonable to conclude that the argument has taken on a mainstream position within the discipline.[17]

At the end of the day, it is of course more important to look at how states position themselves around the question. Overall, the positions seem to be scattered and indeterminate, but some general tendencies have started to crystallize. The following sections will examine three broad trajectories among states' attitudes toward the status of sovereignty in cyberspace under international law. I will first investigate two categories of states whose stance

11. For one of the earliest criticisms, see Gary P. Corn, *Tallinn Manual 2.0 – Advancing the Conversation*, JUST SEC. (Feb. 15, 2017), https:// www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation. For an overview of the early debate in this regard, see Symposium, *Sovereignty, Cyberspace and Tallinn Manual 2.0*, 111 AM. J. INT'L. L. UNBOUND. The discussion on the objections in the literature will be discussed in more detail below, see *infra* Section V.A.

12. *See* Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639 (2017); Phil Spector, *In Defense of Sovereignty, in the Wake of Tallinn 2.0*, 111 AM. J. INT'L L. UNBOUND 219 (2017).

13. *Corfu Channel (U.K. v. Alb.)*, Judgment, 1949 I.C.J. 4, 36 (Apr. 9).

14. *Nicar. v. U.S.*, 1986 I.C.J. ¶ 213.

15. S.C. Res. 138 (June 23, 1960).

16. On this conception of sovereignty as a "fall-back principle," see HARRIET MOYNIHAN, CHATHAM HOUSE, THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS: SOVEREIGNTY AND NON-INTERVENTION 4–5 (2019); FRANÇOIS DELERUE, CYBER OPERATIONS AND INTERNATIONAL LAW 193–232 (2020).

17. For a good summary, see Przemysław Roguski, *Violations of Territorial Sovereignty in Cyberspace – An Intrusion-based Approach*, *in* GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 65, 67–73 (Dennis Broeders & Bibi van den Berg eds., 2020). The author, however, rejects some limitations put forward by the Tallinn Manual regarding the exact legal content of the rule of "territorial sovereignty." *Id.* This issue will be discussed in more detail below.

is, out of political-ideological considerations, more ambiguous toward the Manual's interpretation. For reasons that will become clear, the two categories shall be referred to as "cyber imperialism" and "cyber-Westphalia." Subsequently, I parse the growing number of states that have begun to come out with cautious or even full-throated endorsements of the Tallinn Manual position on sovereignty.

II. CYBER IMPERIALISM

While two of the experts involved in compiling the Tallinn Manual 2.0 could, in 2017, still claim that "[l]ittle criticism of the 'sovereignty-as-rule' position . . . was heard during the nearly four years between publication of the two editions,"[18] this famously changed in 2018 when U.K. Attorney General Jeremy Wright clarified in a speech that it is the "U.K. Government's position . . . that there is no such rule as a matter of international law."[19] In March of 2020, the General Counsel of the U.S. Department of Defense Paul C. Ney, if seemingly more cautiously, concurred. While the department's lawyers would take the principle of sovereignty "into account" when assessing military cyber operations, he acknowledged "similarities with the view expressed by the U.K. Government in 2018" in that "it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law."[20] Both statements caused quite a stir in academic circles, but whereas Wright's position was widely dismissed,[21] Schmitt, for one, found enough nuance in Ney's speech to spot a tacit approximation to the Manual's position.[22] Still, for the time being, it cannot be denied that two of the most active and significant cyber powers have not come out in support the "sovereignty-as-rule" approach.

Apart from the statements' reference to a lack of uniform state practice, might there be a deeper rationale that underlies their standpoint? The conceptual history of "sovereignty" in international legal discourse over the past thirty years might offer an explanation. After the end of the Cold War, liberal international legal scholarship in the West initially declared sovereignty as outdated and mostly unnecessary due to the emergence of a veritable world

18. Schmitt & Vihul, *supra* note 12, at 1649.

19. Jeremy Wright, Att'y Gen., Cyber and International Law in the 21st Century (May 23, 2018) (U.K.).

20. Paul C. Ney, Gen. Counsel, U.S. Dep't of Def., Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020).

21. *See* Roguski, *supra* note 17, at 71.

22. Michael N. Schmitt, *The Defense Department's Measured Take on International Law in Cyberspace*, JUST SEC. (Mar. 11, 2020), https:// www.justsecurity.org/ 69119/ the-defense-departments-measured-take-on-international-law-in-cyberspace/.

society.[23] This branch, however, shifted its stance and began to consider the concept as outright hazardous: adhering to the traditional notion of sovereignty could be dangerous for the populations living under authoritarian or totalitarian regimes. Accordingly, states aimed to substitute sovereignty with a widespread endorsement of the doctrine of humanitarian intervention and what came to be known as the "responsibility to protect."[24] Further, after the terrorist attacks of September 11, 2001, sovereignty came to be seen as inherently dangerous for the civil societies of Western nations who suddenly appeared to be under a constant threat from terrorist groups that had found safe haven in "weak" states, whose sovereignty had thus to be suspended due to their intrinsic unwillingness or inability to act against the transnational peril arising from their territories.[25] Taking into account the additional factor of the rapid development of information technologies on a global scale, the reluctance of the U.S. and the U.K. toward the notion of sovereignty in cyberspace can be read as an outgrowth of all of these narrative arcs.

A. The End of History and the Dream of the Internet

It is hardly a coincidence that the global network of networks that we call the "internet"—originally conceived in the late 1960s as a research project by the U.S. Department of Defense and a few universities mainly based in California—started its triumphant ascent and its commercial breakthrough after the fall of the Communist Bloc. Amplifying and reinforcing America's unipolar moment after the "end of history,"[26] it was almost immediately recognized as the quintessential device to spread the ideals of an Americanized liberal world society built upon freedom of trade and the free exchange of (democratic) ideas. The far-reaching implications of this "cyber-imperialist" trajectory for the global order were soon acknowledged,[27] as succinctly put by Anne-Marie Slaughter in 1997: "If the provision of freedom of information over the Internet creates a *de facto* norm of freedom of information

23. As late as 2014, in the words of the former Legal Adviser to the Foreign and Commonwealth Office of the U.K. Government, Daniel Bethlehem: "On this vision of international society, sovereignty and boundaries are like rocks in a river. They may impede the flow, and even perhaps, on occasion, dam up the water. More usually, however, they simply act as an impediment to the directionality of the flow of the water, which eventually finds a new pathway on its free-flowing gravitational course." *See The End of Geography: The Changing Nature of the International System and the Challenge to International Law*, 25 EUR. J. INT'L L. 9, 15 (2014).

24. *See* Louis Henkin, *That "S" Word: Sovereignty, and Globalization, and Human Rights, Et Cetera*, 68 FORDHAM L. REV. 1, 2–5 (1999).

25. Ntina Tzouvala, *TWAIL and the "Unwilling or Unable" Doctrine: Continuities and Ruptures*, 109 AM. J. INT'L L. UNBOUND 266, 266–67 (2016).

26. FRANCIS FUKUYAMA, THE END OF HISTORY AND THE LAST MAN (1992).

27. *See* Frank Louis Rusciano, *The Three Faces of Cyberimperialism*, *in* CYBERIMPERIALISM?: GLOBAL RELATIONS IN THE NEW ELECTRONIC FRONTIER 9 (Bosah Ebo ed., 2001).

that will change political systems, that's a culture of pluralism and tolerance of freedom of expression. That's one culture, the traditional Western culture. And it will be imposed on non-Western people."[28] Strikingly, amid the decade's prevalent liberal optimism, this did not seem to cause much discomfort among the American class of scholars and policy-makers. Quite the contrary, some went as far as embracing allusions to the British Empire when describing how the possibilities offered by the internet should be seen as an opportunity to expand American "soft power" across the globe. "For the United States," former Deputy Undersecretary of Commerce for International Trade and Development, David Rothkopf, commented in Foreign Policy in the same year as Slaughter, "a central objective of an Information Age foreign policy must be to win the battle of the world's information flows, dominating the airwaves as Great Britain once ruled the seas."[29]

Within these high seas of unrestricted global data flows, the concept of sovereignty had to appear "obsolete and brittle,"[30] and the Anglo-American "imperialism of markets"[31]—which requires the global networks to be free, open, and interoperable[32]—quickly attained quasi-dogmatic status. By 2012, it was considered received wisdom that the internet's primary objective is to "spread prosperity and freedom,"[33] and thus nothing should obstruct the "free flow of information."[34]

B. Technology and Empire: "Home Field Advantage"

U.S. hegemony on the internet is not merely a function of ideological dogma but manifests itself in the organizational and technical foundations of network infrastructures. For one, the setup of internet governance is still dominated by the Internet Corporation for Assigned Names and Numbers

28. Anne-Marie Slaughter et al., *Cultural Imperialism on the Net*, *in* THE INTERNET AND SOCIETY 466, 472 (Jim O'Reilly et al. eds., 1997).

29. David Rothkopf, *In Praise of Cultural Imperialism? Effects of Globalization on Culture*, 107 FOREIGN POL'Y 38, 39 (1997).

30. BENJAMIN H. BRATTON, THE STACK: ON SOFTWARE AND SOVEREIGNTY 6 (2015).

31. HERFRIED MÜNKLER, IMPERIEN: DIE LOGIK DER WELTHERRSCHAFT – VOM ALTEN ROM BIS ZU DEN VEREINIGTEN STAATEN [EMPIRES: THE LOGIC OF WORLD DOMINATION FROM ANCIENT ROME TO THE UNITED STATES] 230 (2005) (Ger.) ("Imperialismus der Märkte").

32. *See* Robert Morgus & Justin Sherman, *The Idealized Internet vs. Internet Realities (Version 1.0)*, NEW AM. (July 26, 2018), https:// www.newamerica.org /cybersecurity-initiative/reports/idealized-internet-vs-internet-realities/.

33. *See International Proposals to Regulate the Internet: Hearing Before the Subcomm. on Commc'ns and Tech. of the H. Comm. on Energy & Com.,* 112th Cong. 145 (2012) (statement of Rep. Greg Walden, Chairman, H. Subcomm. on Commc'ns & Tech.).

34. *Id.* (statement of Philip L. Verveer, Deputy Assistant Secretary of State, U.S. Coordinator for International Communications and Information Policy, Department of State).

(ICANN), a California-based non-profit organization that since its foundation in 1998 has been responsible for maintaining the technical structure of the internet. Even though supervision over its most important subunit—the Internet Assigned Numbers Authority (IANA), which takes care of basic administrative and technical functions—has been transferred from the U.S. Department of Commerce to the private sector, the organization's multi-stakeholder model of governance strives to ensure that the foundational ideals of the "free and open" net remain firmly entrenched.[35]

Even more crucially, the origin story of the internet as having grown out of a modest communications network between a limited number of U.S. institutions into a global cyber superstructure goes a long way toward explaining the enduring competitive edge of the United States and its closest allies, the so-called "Five Eyes" countries,[36] in matters of cybersecurity. Conceiving cyberspace outward from its American core and utilizing transmission routes established in the pre-digital age, the U.S.—in tight cooperation with the U.K. in particular—have natural and near-constant access to many of the essential hubs and cable routes that connect the entire globe, to a degree that results in, in National Security Agency (NSA) parlance, a "home-field advantage" for the conduct of cyber operations.[37] This uniquely privileged position first came to light in the context of the massive and virtually unrestrained global surveillance activity by the NSA and the U.K.'s Government Communications Headquarters (GCHQ) after Edward Snowden's revelations in 2013.[38] The revelations shed light on how the U.S. and U.K. benefitted from the fact that many of the most important internet companies that process and store the world's data streams are subject to U.S. law.[39]

From this historical and conceptual vantage point, globally connected networks may in fact present themselves as one vast open space that transcends conventional ideas of territoriality. Instead of perceiving cyberspace "as just another physical space, like land, air, or sea,"[40] the U.S. security establishment was taught to see an operational environment whose "basic

35. HENNING LAHMANN & JAN ENGELMANN, WHO GOVERNS THE INTERNET? 12 (Anne Lammers et al. eds., 2nd ed. 2020).

36. The "Five Eyes" are the U.S., U.K., Canada, Australia, and New Zealand.

37. BEN BUCHANAN, THE HACKER AND THE STATE 15–16 (2020).

38. *See generally* Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81 (2014) (explaining the legal implications).

39. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps into User Data of Apple, Google, and Others*, GUARDIAN (June 7, 2013, 3:23 PM), https:// www.theguardian.com/ world/ 2013/ jun/06/us-tech-giants-nsa-data.

40. Efrony & Shany, *supra* note 6, at 653.

structure [and] design" are incongruous "with traditional notions of Westphalian geography."[41] The point here is not to pass judgment on this understanding. But there can be no doubt that the described development of cyberspace and the accompanying ideological narrative have had a significant impact, quite literally, on what military and intelligence decision-makers in the U.S. (and the U.K.) *see* when they look at the global network infrastructures. If we want to comprehend the deeper preconceptions and assumptions that have a bearing on the discourse surrounding the legal status of sovereignty in cyberspace, we cannot help but take these conceptual underpinnings seriously.

C. The Legal Construction of Imperial Space: Sovereignty and "Persistent Engagement"

The U.S. approach to sovereignty in cyberspace fundamentally deviates from the stance of all other states, including its closest allies from the Five Eyes group.[42] For the authors of the Tallinn Manual, a state's sovereignty over a part of cyberspace is simply a result of the fact that all ICT infrastructures connected to the global networks have some definite physical location which belongs to the territory of a state.[43] Activities "in cyberspace" occur within determinable ICT systems and thus likewise "on territory . . . over which States may exercise their sovereign prerogatives."[44] While U.S. officials do not deny this basic assumption in principle,[45] they consider a different aspect associated with the notion of sovereignty beyond mere territorial representation ultimately more decisive: *effective control*. Sovereignty as presupposing control over territory is a longstanding idea[46] that is regarded

41. *See* Corn, *supra* note 11.

42. While the other Five Eyes members all articulate the necessity for some form of "active" posture in cyberspace, none have gone as far as the U.S. The U.K.'s "Active Cyber Defence" strategy is primarily understood as "the principle of implementing security measures to strengthen a network or system to make it more robust against attack." U.K. GOV., NATIONAL CYBER STRATEGY 2016–2021 33 (2016). New Zealand's strategy is limited to being "ready to deter and respond to threats" in cyberspace. N.Z. GOV., NEW ZEALAND'S CYBER SECURITY STRATEGY 2019 5 (2019). Australia uses very similar language. *See* AUSTL. GOV., AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY 54 (2017). Only Canada approximates the U.S. approach, postulating, by legislation, a broad mandate to carry out "active cyber operations," defined as "activities *on or through the global information infrastructure* to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security." Communications Security Establishment Act, S.C. 2019, c 13, ¶ 19 (Can.) (emphasis added).

43. TALLINN MANUAL 2.0, *supra* note 5, at 11.

44. *Id.* at 12.

45. *See* Ney, *supra* note 20 ("States have sovereignty over the information and communications technology infrastructure within their territory.").

46. James Crawford, *Sovereignty as a Legal Value*, *in* THE CAMBRIDGE COMPANION TO INTERNATIONAL LAW 117, 131–32 (James Crawford & Martti Koskenniemi eds., 2012).

as the most fundamental aspect of sovereignty.[47] Yet, this notion was mainly relevant for the *establishment*[48] and only in certain limited circumstances as a criterion for the continuity of title.[49] However, as Antony Anghie first argued in his examination of positivist justifications of colonial conquest, the assumed absence of stable control in fact implies that an intruding power is therefore free to act as it pleases,[50] a conception that has regained traction as an implicit component[51] leading to the idea that sovereignty is essentially "contingent" on a state's ability to adequately handle transnational threats emerging from its territory.[52]

With this in mind, it is worth reconsidering certain statements made in this context. Given the fundamental non-territoriality of cyberspace, a result of the inherent interconnectedness as the core structural feature of the domain,[53] actors are "free from the physical constraints of geography and territorial boundaries;"[54] in turn, this means that no actor can have consistent effective control over clearly defined sections of cyberspace. The lack of control over a defined space precludes the assumption of sovereignty in the traditional sense.[55] Unsurprisingly, "sovereignty" makes a single appearance in the Cyberspace Solarium Commission Report, which was published in March 2020 to form the basis for the main strategic approach of the U.S. to threats from the digital domain, and only to emphasize precisely this point.[56] Thus, the U.S. will likely have no issue with acknowledging that every system connected to cyberspace has a physical location within the boundaries

47. Antony Anghie, *Finding the Peripheries: Sovereignty and Colonialism in Nineteenth-Century International Law*, 40 HARV. INT'L L.J. 1, 24 (1999).

48. *See* MALCOLM N. SHAW, INTERNATIONAL LAW 505 (6th ed. 2008).

49. Island of Palmas Case (Neth. v. U.S.), 2 R.I.A.A. 829, 839 (Perm. Ct. Arb. 1928); Sovereignty over Pedra Branca/Pulau Batu Puteh, Middle Rocks and South Ledge (Malay. v. Sing.), Judgment, 2008 I.C.J. 12, ¶ 121 (May 23).

50. *See* Anghie, *supra* note 47, at 3.

51. *See* Ashley S. Deeks, "*Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483 (2011); Daniel Bethlehem, *Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AM. J. INT'L L. 769 (2012); Craig Martin, *Challenging and Refining the "Unwilling or Unable" Doctrine*, 52 VAND. J. TRANSNAT'L L. 387 (2019).

52. *See* Sara Kendall, *Cartographies of the Present: "Contingent Sovereignty" and Territorial Integrity*, 47 NETH. Y.B. INT'L L. 83, 100 (2016).

53. Michael P. Fischerkeller & Richard J. Harknett, *Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation*, 2019 CYBER DEF. REV. 267, 269.

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

55. This viewpoint must have an impact on the question of the application of the principle of due diligence to cyberspace; if a state cannot exercise control over IT infrastructures located on its territory, then, *a fortiori*, it is at least difficult to hold it accountable if non-state actors use them to the detriment of the interests of other states. *See* N.Z. FOREIGN AFFS. & TRADE, THE APPLICATION OF INTERNATIONAL LAW TO STATE ACTIVITY IN CYBERSPACE ¶ 13 (2020).

56. CYBERSPACE SOLARIUM COMM'N, *supra* note 3.

of a state. But in line with this approach, the critical marker of sovereignty is not territoriality by itself, but control. Further, due to the technical features of cyberspace, any assumption of actual, consistent effective control over what happens "within" the interconnected systems is merely theoretical and therefore ultimately legally immaterial.

In such a de-territorialized environment where no one can tell "where the boundaries are,"[57] sovereignty is effectively suspended. It only comes into play once a cyber operation causes effects outside of the virtual domain (assuming a certain threshold is met).[58] "Inside" cyberspace, on the other hand, the global system of sovereign states is replaced with an imperial order that divides the domain into two different zones: the metropole—in U.S. military jargon the "blue cyberspace," "areas in cyberspace protected by the U.S., its mission partners, and other areas DOD may be ordered to protect"[59]—and the periphery, which is considered "red" or "gray space" depending on whether or not an adversarial actor either owns or temporarily assumes control over that part of cyberspace.[60] As an ordering principle, this hierarchical model of metropole and periphery precludes the assumption of sovereign equality[61] and is thus categorically incompatible with the international legal system.[62] Notably, while the Cyber Solarium Commission Report pays lip service to international law, it only does so in passing. Sovereignty may be considered when acting in cyberspace,[63] but the technical features of the operating environment prevent sovereignty from attaining rule-status that could constrain U.S. conduct. The relevant legal order for the permissibility of conduct is instead the domestic law of the metropole.[64] Beyond that, the U.S. mainly supports the proliferation of "norms of responsible state behavior in cyberspace" that align with U.S. "interests and values"[65] and that ideally have a stabilizing effect without necessarily assuming the

57. Declared by a U.S. Cyber Command deputy commander as quoted in Jason Healey, *The Implications of Persistent (and Permanent) Engagement in Cyberspace*, 5 J. CYBERSECURITY 1, 6 (2019).

58. See in this context the official position of N.Z. FOREIGN AFFS. & TRADE, *supra* note 55, ¶ 13, which acknowledges the significance of territorial sovereignty but asserts that the application of the rule "must take into account some critical features that distinguish cyberspace from the physical realm," *inter alia* the fact that "cyberspace contains a virtual element which has no clear territorial link."

59. JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-12, CYBERSPACE OPERATIONS I-4 (2018).

60. *Id.* at I-5.

61. *See* Tzouvala, *supra* note 25, at 267.

62. *See* MÜNKLER, *supra* note 31, at 77; B.S. Chimni et al., *Theme III: Global Governance: Institutions*, 16 LEIDEN J. INT'L L. 897, 902–03 (2003); *see also* MARTTI KOSKENNIEMI, THE GENTLE CIVILIZER OF NATIONS: THE RISE AND FALL OF INTERNATIONAL LAW, 1870–1960 34 (2002) ("An Empire is never an advocate of international law that can seem only an obstacle to its ambitions.").

63. Ney, *supra* note 20.

64. See BUCHANAN, *supra* note 37, at 25–26, for the context of global surveillance.

65. CYBERSPACE SOLARIUM COMM'N, *supra* note 3, at 46–47.

status of legal rules proper.

Michael Schmitt and Liis Vihul have suggested that the attitude toward the rule-status of sovereignty changed sometime after 1999. Up to that point, the U.S. Department of Defense had still held that certain offensive cyber operations may amount to an internationally wrongful act by violating another state's sovereignty.[66] Assuming this interpretation to be correct, there must be an explanation for the altered conception of sovereignty in cyberspace, and it seems unlikely that an epistemic shift concerning the fundamental technical makeup of the global network infrastructures alone can account for it. Instead, the described construction of an imperial space in the cyber domain appears to have coincided with a larger change in threat perception in the aftermath of the terrorist attacks of September 11, 2001, which led to a reframing of security and territory and the adoption of an imperial understanding of the global periphery.[67] In the course of the "War on Terror," the sovereignty of states was redefined, and if necessary suspended, when they proved "unwilling or unable" to act against terrorist groups operating from their territory.[68] As implied by the U.K. Prime Minister, states that tolerate "ungoverned space" within their borders cannot not invoke sovereignty as a defense against foreign intrusion.[69] In this context, it was especially the initiation of drone warfare that had a de-territorializing effect that essentially nullified the sovereignty of target states.[70]

In this vein, Gary Corn and Robert Taylor, serving members of the U.S. Department of Defense, explicitly invoke the threat of terrorists being active in cyberspace for rejecting the rule-status of sovereignty, as that might prevent the U.S. military from conducting effective cyber operations against such non-state actors.[71] Strikingly, the Department's argument follows a

66. Schmitt & Vihul, *supra* note 12, at 1639–40.

67. ANTONY ANGHIE, IMPERIALISM, SOVEREIGNTY AND THE MAKING OF INTERNATIONAL LAW 303–09 (James Crawford et. al. eds., 2005).

68. *See* Deeks, *supra* note 51; Tzouvala, *supra* note 25, at 267.

69. DAVID CAMERON, PRIME MINISTER, RESPONSE TO THE FOREIGN AFFAIRS SELECT COMMITTEE'S SECOND REPORT OF SESSION 2015-16: THE EXTENSION OF OFFENSIVE BRITISH MILITARY OPERATIONS TO SYRIA 2 (2015) (U.K.). To be sure, the invocation of the "unwilling or unable" doctrine is not limited to the U.S. and U.K. *See* Permanent Rep. of Belgium to the U.N., Letter dated June 7, 2016 from the Permanent Rep. of Belgium to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2016/523 (June 9, 2016) (justifying their participation in operations against ISIS on Syrian territory before the U.N. Security Council by explicitly referring to a lack of "effective control" of the Syrian Government); Charge d'affaires of the Permanent Mission of Germany to the U.N., Letter dated December 10, 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Germany to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2015/946 (Dec. 10, 2015) (same).

70. Rebecca Mignot-Mahdavi, *The Institutionalization of Drone Programs, Entering the Normal Functioning of the State* 46 (Eur. Soc'y of Int'l L. Ann. Conf., Paper No. 21/2019, 2019).

71. Corn & Taylor, *supra* note 54, at 211–12.

similar logic for the use of force on the territory of states that turn out to be "unwilling or unable" to prevent terrorists from operating within their boundaries:

> ISIS followers and adherents both inside and outside ISIS-controlled territory operate on servers and infrastructure scattered across the globe, taking advantage of the transparency and permeability of borders that characterize the internet. These states *may have limited or no knowledge* that ISIS is utilizing servers or cyber infrastructure under their sovereign authority. Further, these states *may lack the capability to effectively counter or even discover* ISIS's cyber threat.[72]

In cyberspace, the concept of "unwilling or unable" thus reaches even further than in the "physical" world. Due to the technical peculiarities of cyber infrastructures and their essential non-territoriality, no state is *ever* reliably in control and able to suppress the threat.[73] By implication, the actual location of the periphery in cyberspace is by definition never fixed; it is potentially anywhere outside the "blue space" of U.S. networks. U.S. Cyber Command must thus be able to "maneuver seamlessly across the interconnected battlespace, globally,"[74] as offensive cyber operations aimed at pacifying peripheral spaces may become necessary within the territory of virtually any state. From this vantage point, an apparent paradox emerges: every system that forms part of the "free and open" global network infrastructures is at all times both on the inside of the imperial space, for purposes of commercial activity and the dissemination of liberal ideas, and on the outside where enemies roam free and no state exerts effective sovereign control. In cyberspace, so to speak, the Visigoths are perpetually at the gate.

This approach to transnational cybersecurity has found both its most explicit embodiment and its logical conclusion in the related doctrines of "defend forward" and "persistent engagement," which were officially announced in 2018. Assuming that the historical ability of the U.S. "to protect the homeland by controlling its land, air, space, and maritime domains" has come to an end due to the opportunities cyberspace offers to adversaries,[75] the concepts amount to the strategy to routinely and continuously carry out "clandestine military activity" in cyberspace in order to "deter, safeguard or defend against attacks or malicious cyber activities against the United

72. *Id.* at 211 (emphasis added).

73. *See, e.g.*, Fischerkeller & Harknett, *supra* note 53, at 269 ("Well-defended cyber terrain is attainable but continually at risk.").

74. Paul M. Nakasone, *A Cyber Force for Persistent Operations*, 92 JOINT FORCE Q. 10, 13 (2019).

75. WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 12 (2017), https:// trumpwhitehouse.archives.gov/ wp-content/ uploads/ 2017/ 12/ NSS-Final-12-18-2017-0905.pdf.

States . . . before they reach their target."[76] Although the doctrines are primarily directed at adversarial powers such as China or Russia rather than non-state actors, the fundamental rationale remains constant. With the express objective to "improve the security and stability of cyberspace,"[77] which includes safeguarding the liberal global economic system that relies on cyber infrastructures,[78] U.S. Cyber Command perceives the operational domain as one single imperial space where it maneuvers "*seamlessly* between defense and offense across the interconnected battlespace . . . globally, as close as possible to adversaries and their operations."[79] Fending off perceived threats on faraway shores before they can reach the homeland is a model taken straight out of the playbook of the War on Terror.[80] Viewed from this angle, cyber operations carried out under the framework of "persistent engagement" are not so much expressions of a revived great power competition, as has sometimes been suggested,[81] but rather have adopted the character of campaigns aimed at pacifying the virtual margins of the imperial space.[82]

The implications of this approach is evidenced in November 2018, when U.S. Cyber Command launched a cyber operation against the Internet Research Agency in St. Petersburg, Russia to disrupt the "troll farm's" internet access during the US midterm election,[83] which was widely seen as the

76. Louk Faesen et al., *Case Studies of Norm Development in Hybrid Conflict*, *in* FROM BLURRED LINES TO RED LINES: HOW COUNTERMEASURES AND NORMS SHAPE HYBRID CONFLICT 44, 64 (2020); *see also* James N. Miller & Neal A. Pollard, *Persistent Engagement, Agreed Competition and Deterrence in Cyberspace*, LAWFARE (Apr. 30, 2019, 9:12 AM), https:// www.lawfareblog.com/ persistent-engagement-agreed-competition-and-deterrence-cyberspace.

77. U.S. CYBER COMMAND, ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY: COMMAND VISION FOR US CYBER COMMAND 6 (2018), https:// www.cybercom.mil/ Portals/ 56/ Documents/ USCYBERCOM% 20Vision%20April%202018.pdf.

78. *See* Fischerkeller & Harknett, *supra* note 53, at 268.

79. U.S. CYBER COMMAND, *supra* note 77, at 6 (emphasis added).

80. The U.K. has been more cautious in its official statements regarding an offensive posture in cyberspace, although it recently announced that it considers itself "a world-leader on offensive cyber operations." It is interesting to note that in doing so, it explicitly foregrounded achievements against the terrorist threat posed by ISIS. *See National Cyber Force transforms country's cyber capabilities to protect the UK*, GEN. COMMC'NS. HEADQUARTERS (Nov. 19, 2020), https:// www.gchq.gov.uk/ news/national-cyber-force.

81. Fischerkeller & Harknett, *supra* note 53, at 267, call this conception "agreed competition."

82. This is not to suggest that other actors, such as Russia in particular, do not equally persistently target networks and systems in other states, including the industrial control system. *See, e.g.*, Andy Greenberg, *Hackers Tied to Russia's GRU Targeted the US Grid for Years, Researchers Warn*, WIRED (Feb. 24, 2021, 7:30 AM), https:// www.wired.com/ story/russia-gru-hackers-us-grid/. However, the U.S. approach is unique insofar as it publicly rationalizes its offensive strategy and embeds it in a larger geopolitical approach that, as argued here, is part of a long-term realignment after 9/11.

83. Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST (Feb. 27, 2019), https:// www.washingtonpost.com/ world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

first known application of the strategy of "persistent engagement."[84] For the purpose of this essay, it is less relevant to assess whether the operation's effects reached a severity threshold that would imply a violation of the "rule of sovereignty" in accordance with the Tallinn Manual criteria, or whether it could be justified as a lawful countermeasure. Here, it is significant that despite General Counsel Ney's previous assurance that the U.S. military would "take into account the principle of State sovereignty,"[85] there was no attempt from U.S. Cyber Command to justify the operation under international law. This, at the very least, suggests that Russia's sovereignty was never seriously regarded as posing an impediment. In this light, retrospective attempts to rationalize the conduct within an international legal framework might miss the mark, as it does not appear to constitute an element of the strategic calculus under "persistent engagement."

III. CYBER WESTPHALIA

The possible dawn of a "cybered Westphalian age," which has come to represent a sweeping discursive antipode to the conception of the global networks as principally "free and open," was first observed as early as 2011.[86] A decade later, talk of the (re)emergence of "borders" between states in the cyber domain is now commonplace. Most prominently, Russia, China, and Iran have all engaged in efforts to decouple their domestic parts of cyberspace from the global network superstructure. The development, which has pronounced technological as well as political-legal dimensions, has been framed as part of a broader attempt to "extend authoritarian rule across time and space."[87] While the substance of this contention can hardly be disputed, its liberal perspective sometimes underplays the significance—and persuasive power— of counter-imperialist narratives in the rationalization of "Westphalian" trajectories in cyberspace. With a focus on China as the paradigmatic example of this approach, the following section examines the question of how it informs the discourse surrounding the legal status of sovereignty.

84. Miller & Pollard, *supra* note 76.

85. Ney, *supra* note 20.

86. Chris C. Demchak & Peter Dombrowski, *Rise of a Cybered Westphalian Age*, 5 STRATEGIC STUD. Q. 32 (2011); Chris C. Demchak & Peter Dombrowski, *Cyber Westphalia: Asserting State Prerogatives in Cyberspace*, 2013 GEO. J. INT'L AFFS. 29 ; Chris C. Demchak, *Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age*, 1 CYBER DEF. REV. 49 (2016).

87. Tom Ginsburg, *Authoritarian International Law?*, 114 AM. J. INT'L L. 221, 225 (2020).

A. Echoes of Imperialist Legacies in Transnational Space

Long before the ascent of the notions of "cyber sovereignty" and "cyber-Westphalia," Chinese officials were pushing back against the "free and open" internet that was thought of as dominated by U.S. ideology and technology. In doing so, they consciously invoked the language of anti-imperialism. In 2000, Jiang Mianheng, Vice-President of the Chinese Academy of Sciences, warned that "China's integration into the economy dominated by cyberspace presents the danger of subjugating the country to the fealty of capitalist, neo-imperialist Western powers."[88] This "colonial menace" did not just arrive in the form of "[t]he West's technological domination" but also through the "influence and remote control by ideas and cultures."[89] Already then, the only conceivable response was asserted to be the filtering of internet content and ultimately "the construction of a national network independent of the Internet, the elaboration of new protocols and technologies on which it is to be based."[90] Nearly two decades later, Mianheng's observations were echoed by the high-ranking diplomat He Yafei in his book with the telling title "China's Historical Choice in Global Governance." He noted that "cyber imperialism is on the rise, resulting from *a monopoly of information and internet technology,*" and determined that China was thus compelled to respond with two separate but interconnected strategies: "build up national cyberspace capability to counter such an invasion" and "establish rule of law in cyberspace in global governance."[91] Although the contours of these objectives remain poorly defined, the concept of "internet sovereignty" has become firmly entrenched in contemporary Chinese political discourse.[92]

It is important to recognize this language as more than merely nationalist posturing of a rising power. The line of argumentation is consistent with China's more general perception of the international order since the colonial traumata of the 19th century, when the British Empire forced the Middle Kingdom into the "unequal treaties" as a result of the two Opium Wars, and the aftermath of the shattering of the Boxer Rebellion had led to painful concessions to the Western powers and the Empire of Japan.[93] The emphasis on

88. Daniel Ventre, *Cuba: Towards an Active Cyber-Defense*, *in* CYBER CONFLICT: COMPETING NATIONAL PERSPECTIVES 45, 67 (Daniel Ventre ed., 2012).

89. *Id.*

90. *Id.*

91. HE YAFEI, CHINA'S HISTORICAL CHOICE IN GLOBAL GOVERNANCE (2018) (emphasis added).

92. *See* Jinghan Zeng et al, *China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of Internet Sovereignty*, 45 POL. & POL'Y 432 (2017).

93. Anghie, *supra* note 47, 36–37; *see generally* Phil C.W. Chan, *China's Approaches to International Law Since the Opium War*, 27 LEIDEN J. INT'L L. 859 (2014).

sovereignty must be understood against this historical background.[94] Framing such an approach as "Westphalian," as suggested by Demchak and Dombrowski,[95] is appropriate insofar as the 1648 Treaties of Westphalia are generally perceived as laying the foundations of modern-day sovereignty through an explicit rejection of the formal supremacy of pope and emperor in the Holy Roman Empire,[96] despite the factual issues with this historical interpretation that several scholars have pointed out.[97] More recently, a further reinforcing narrative has formed in Beijing that promotes the idea of China as having emerged from World War II to become the creator and guardian of the post-war international legal order, which today is threatened by the imperial ambitions of the U.S.[98]

Russia—the other state counted among the leading "cyber Westphalian" powers—has developed a similar understanding of sovereignty through a series of markedly different historical events. Unlike China, its historical point of reference is not colonial encroachment and conquest by a European nation because Russia constituted an integral part of the continent's Concert of Powers since after the Congress of Vienna in 1815. The traumatic event that continues to shape its attitudes and politics toward the West and the rest of the world is much more recent and involves not a struggle against a colonial empire, but the loss of one, which came about with the fall of the Soviet Union in 1991.[99] The lessons Russia drew from this outcome of the Cold War are nonetheless similar to China's in that it led to a deep mistrust of "liberal ideology," which, in the Kremlin's narrative, has "outlived its purpose"[100] while at the same time displaying an uncomfortable tendency to lead to "color revolutions."[101] The antidote, quite naturally, is a rejection of the

94. *See* MARIA ADELE CARRAI, SOVEREIGNTY IN CHINA, A GENEALOGY OF A CONCEPT SINCE 1840 82–108 (2019). To be sure, the self-serving performativity of the CCP's more recent rhetoric of anti-imperialism in light of Beijing's global ambitions of late was recently pointed out by literary theorist Nan Z. Da. Nan Z. Da, *Disambiguation, a Tragedy*, N+1, Fall 2020, at 75, 81 (2020).

95. *See* Demchak and Dombrowski, *Rise of a Cybered Westphalian Age, supra* note 86.

96. Martti Koskenniemi & Ville Kari, *Sovereign Equality*, *in* THE UN FRIENDLY RELATIONS DECLARATION AT 50: AN ASSESSMENT OF THE FUNDAMENTAL PRINCIPLES OF INTERNATIONAL LAW 166, 167 (Jorge E. Viñuales ed., 2020).

97. *See generally* Derek Croxton, *The Peace of Westphalia of 1648 and the Origins of Sovereignty*, 21 INT'L HIST. REV. 569 (1999); *see also* Peter M.R. Stirk, *The Westphalian Model and Sovereign Equality*, 38 REV. INT'L STUD. 641 (2011).

98. RANA MITTER, CHINA'S GOOD WAR: HOW WORLD WAR II IS SHAPING A NEW NATIONALISM 248–49 (2020).

99. *See* Lauri Mälksoo, *The Russian Concept of International Law as Imperial Legacy*, *in* EUROPEAN INTERNATIONAL LAW TRADITIONS 261 (Peter Hilpold ed., 2021).

100. Lionel Barber & Henry Foy, *Vladimir Putin: Liberalism Has 'Outlived Its Purpose'*, FIN. TIMES (June 27, 2019), https://www.ft.com/content/2880c762-98c2-11e9-8cfb-30c211dcd229.

101. *See* Krišjānis Bušs, *Russia Stirs Fear of Color Revolutions*, DEMOCRACY SPEAKS (Sept. 9, 2019), https://www.democracyspeaks.org/blog/russia-stirs-fear-color-revolutions.

"free and open" internet which facilitates the spread of liberal ideas and tight control over information flows into and within Russia. This development is in line with a more generally illiberal understanding of the concept of sovereignty in Russian discourse, which is directed against the "dangerous" Western idea of popular sovereignty.[102]

The first subject area in which the Westphalian approach came to the surface on issues concerning cyberspace was the structure of internet governance. In response to the Western preference of maintaining a "multistakeholder" model within the framework of ICANN that acknowledged the legitimate position of private entities alongside state actors with respect to administrative and norm-creating functions, China and Russia early on pushed for extending the mandate of the International Telecommunication Union (ITU).[103] As a multilateral organization based on the principle of "one state, one vote" as an expression of sovereign equality, in the eyes of these states (together with Iran, India, Saudi Arabia, and a few others), the ITU is better suited to advance their cause.

B. Technology and Sovereignty: Asserting Control

If sovereignty presupposes factual, effective control, as was described in section two as the basic assumption underlying the imperial approach to cyberspace, then establishing control by way of technological fixes is not per se an irrational response.[104] In this regard, to perceive the increasing segmentation and decreasing interconnectedness of global network infrastructures as exclusively an "authoritarian attempt" to suppress one's own population is not a sufficiently complex explanation. The fragmentation that results from this process of disconnecting may just as much be aimed at undermining one of the main premises of "persistent engagement" and in this way creating the technical conditions for the realization of sovereignty vis-à-vis imperialist tendencies.[105]

Interestingly, although formulated as a counterstrategy to the U.S. approach,[106] the Chinese variant of cyber sovereignty has so far apparently not taken this path. Instead, it is almost entirely focused on protecting against

102. *See* LAURI MÄLKSOO, RUSSIAN APPROACHES TO INTERNATIONAL LAW 100–04 (2015).

103. Adam Segal, *Holding the Multistakeholder Line at the ITU*, COUNCIL ON FOREIGN RELS. (Oct. 21, 2014), https://www.cfr.org/report/holding-multistakeholder-line-itu.

104. It bears repeating that this does not imply a value judgment.

105. *See* Lennart Maschmeyer, *Persistent Engagement Neglects Secrecy at Its Peril*, LAWFARE (Mar. 4, 2020, 8:00 AM), https:// www.lawfareblog.com/ persistent- engagement- neglects- secrecy- its-peril (discussing the flawed logic behind the argument that persistent engagement relies on the assumption that cyber conflict stems from the "interconnectedness" of modern technology).

106. *See* Yi Shen, *Cyber Sovereignty and the Governance of Global Cyberspace*, 1 CHINESE POL. SCI. REV. 81, 90 (2016) (finding that China's cyber sovereignty was created defensively).

Western values and ideas by targeting the information flows that enter the country on the content layer,[107] that is on top of existing network infrastructures.[108] Its "Golden Shield Project," also known as the Great Firewall, isolates the Chinese part of the internet by extensively filtering incoming data traffic. The inward-looking dimension consists of an invasive surveillance and censorship system aimed at ensuring that nothing from the free and open internet reaches the hearts and minds of Chinese citizens.[109] At the same time, this approach does nothing to shield the People's Republic from offensive cyber operations conducted by the U.S. under its framework of persistent engagement.[110] Some commentators have suggested that China's reluctance to implement a more rigorous physical separation on the network's infrastructure layer might be a reflection of its own long-standing preference for an offensive posture in cyberspace, not unlike that of the U.S.[111] If anything, certain aspects of China's surveillance infrastructure, such as the widespread ban of the HTTPS protocol,[112] seem to have a rather weakening effect on overall cybersecurity.[113]

The same does not hold true for more recent efforts taken by Russia and Iran. In 2019, the State Duma enacted the sovereign internet law which set the stage for an actually physical separation of the Russian networks from the rest of the internet.[114] While the law is expected to be primarily aimed at intensifying domestic censorship and surveillance,[115] the official line is that

107. This paper adopts the three categories of layers introduced by Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L.J. 561, 562 (2000): infrastructure layer, logical layer, and content layer. Several other layer models of global network infrastructures have been proposed in the literature.

108. Justin Sherman, *Russia and Iran Plan to Fundamentally Isolate the Internet*, WIRED (June 6, 2019, 8:00 AM), https:// www.wired.com/ story/ russia-and-iran-plan-to-fundamentally-isolate-the-internet/.

109. Elisabeth C. Economy, *The Great Firewall of China: Xi Jinping's Internet Shutdown*, GUARDIAN (June 29, 2018), https:// www.theguardian.com/ news/ 2018 /jun/ 29 /the-great-firewall-of-china-xi-jinpings-internet-shutdown.

110. *See* Hugo Zylberberg, *Cyber Sovereignty and Online Borders Do Not Improve International Security*, COUNCIL ON FOREIGN RELS. (Oct. 2, 2017, 10:22 AM), https:// www.cfr.org/blog/cyber-sovereignty-and-online-borders-do-not-improve-international-security (discussing the ineffectiveness of using online borders to protect a country's territory).

111. *See* Tianjiao Jiang, *From Offensive Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar*, 1 CHINESE J. INT'L REV. 1 (2019) (discussing how Chinese cyberwar practices look similar to those in the U.S.).

112. *See What is HTTPS?*, CLOUDFARE, https://www.cloudflare.com/learning/ssl/what-is-https/ (explaining that "[HTTPS] is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer").

113. Valentin Weber, *How China's Control of Information Is a Cyber Weakness*, LAWFARE (Nov. 12, 2020, 12:43 PM), https://www.lawfareblog.com/how-chinas-control-information-cyber-weakness.

114. Sherman, *supra* note 108.

115. Zak Doffman, *Putin Signs "Russian Internet Law" to Disconnect Russia from the World Wide*

the law is a direct response to "the aggressive nature of the U.S. National Cyber Security Strategy adopted in September 2018—i.e., "persistent engagement."[116] Russia's official stance represents a significant leap toward cyber sovereignty because it seeks to establish factual control over (virtual) territory. Likewise, Iran initiated steps to physically separate its domestic network from the internet.[117] Iran does not make an explicit nod to U.S. cyber strategy but like Russia stresses a comparable sense of vulnerability to offensive cyber operations.[118] Thus, while the approaches of the main proponents of the Westphalian approach differ, all three states have now taken clear steps to implement some version of "cyber sovereignty."

Despite their differences, the three cases are significant insofar as they all at least tacitly acknowledge the implicit premise that in an interconnected, conceptually de-territorialized space, sovereignty remains fundamentally ephemeral unless actual, sustained control over cyber infrastructure can be established. Given the political history of the internet and the particular counter-narratives of China and Russia, the states' policies should come as no surprise. The subsequent section looks at how these actors have, in addition to these domestic measures, attempted to promote cyber sovereignty within the context of international normative processes.

C. "Westphalian" Approaches to International Law in Cyberspace

The model of cyber sovereignty exemplified by China, Russia, and Iran—although with variations when it comes to the details of implementation—is primarily aimed at regime stabilization,[119] which requires it to be both inward- and outward-looking. The two aspects are necessarily intertwined, and both focus on the content layer of network infrastructures, that is the information transported over the internet. In that sense, these actors frame the implications of the digital transformation as "information-" rather than "cyber security."[120]

Web, FORBES (May 1, 2019), https://www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/.

116. Alena Epifanova, *Deciphering Russia's "Sovereign Internet Law,"* DGAP (Jan. 16, 2020), https:// dgap.org/ en/research/publications/deciphering-russias-sovereign-internet-law.

117. Lily Hay Newman, *How the Iranian Government Shut Off the Internet*, WIRED (Nov. 17, 2019, 3:34 PM), https://www.wired.com/story/iran-internet-shutoff/.

118. *See* Idrees Ali & Phil Stewart, *Exclusive: U.S. Carried Out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials*, REUTERS (Oct. 16, 2019, 1:03 AM), https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK (discussing a secret U.S. cyber strike operation targeting Iran).

119. BROEDERS ET AL., *supra* note 1, at 2.

120. *See* Minister for Foreign Affairs of the Russian Federation, Letter dated Sept. 23, 1998 from the Minister for Foreign Affirs of the Russian Federation addressed to the Secretary-General, U.N. Doc. A/C.1/53/3 (Sept. 30, 1998) (explaining the information revolution and the potential threat of information

This understanding is reflected in the states' individual and joint efforts at norm development and consolidation in international fora. Whereas Russia's 1998 letter to the UN Secretary-General and the accompanying draft resolution did not yet explicitly reference "sovereignty" as threatened by the possibilities of novel global information technologies, it did already observe that they can "be used for purposes incompatible with the objectives of ensuring . . . the observance of the principle of . . . non-interference in internal affairs."[121] Two years later, the Russian Federation declared that the "United Nations . . . shall promote international cooperation for the purpose of limiting threats in the field of international information security and creating, for that purpose, an *international legal basis* to . . . [d]evelop a procedure for the exchange of information on and the *prevention of unauthorized transboundary influence through information.*"[122]

The notion of sovereignty has become front and center in initiatives to regulate state conduct in cyberspace. This has been most emphatically expressed in the two versions of the "International Code of Conduct for Information Security," drafted within the framework of the Shanghai Cooperation Organization (SCO). The second iteration of the International Code of Conduct for Information Security[123] provides in its first operative clause that all states that voluntarily subscribe to the Code pledge to respect the sovereignty, territorial integrity, and political independence of all states. Crucially, this entails the obligation "[n]ot to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability."[124] The statement clarifies that transboundary data streams on the content layer itself, without any intrusion of the underlying cyber infrastructure, potentially qualify as violations of sovereignty if they amount to interfering acts below coercion, the threshold necessary for a violation of the principle of non-intervention. For instance, Russia recently regarded the live broadcasting of anti-government protests via Google's streaming platform YouTube as such an interference in its internal

---

wars).

121. *Id.* at 3.

122. U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, *Reply received from the Russian Federation*, at 6, U.N. Doc. A/55/140 (July 10, 2000) (emphasis added).

123. Permanent Reps. of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the U.N., Letter dated Jan. 9, 2015 from the Permanent Reps. of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the U.N. addressed to the Secretary-General, U.N. Doc. A/69/723, annex (Jan. 13, 2015). The first version had been submitted by China, Russia, Tajikistan and Uzbekistan in September 2011.

124. *Id.* § 2(3).

affairs.[125] China, in particular, has repeatedly underlined that the principle of sovereignty entails the prohibition of such undermining conduct,[126] and has "warned against infringement of its cyber sovereignty *under the pretext of providing free flow of information.*"[127] In 2017, the People's Republic enshrined the duty to respect "cyber sovereignty" as the "cornerstone" of its Strategy for International Cooperation on Cyberspace.[128]

More recently, the armed forces of Iran published a comprehensive statement to weigh in on the question of the status of sovereignty in cyberspace, opining that "[a]ny intentional use of cyber-force with tangible or non-tangible implications which is or can be a threat to the national security or may, due to political, economic, social, and cultural destabilization, result in destabilization of national security constitutes a violation of the sovereignty of the state."[129] Provided the translation is reliable, which is hard to assess, the use of the term "cyber-force" seems to imply that the authors had in mind more traditional offensive cyber operations directed against the logical or physical layers of cyber infrastructures and not so much an attempt at influencing public opinion in Iran by way of conducting an information operation. Still, it is noteworthy that the state considers "non-tangible implications" in the form of "social and cultural destabilization" as falling within the rule's scope, which at least leaves open the possibility that an "interference" on the content layer could be regarded as a violation of Iran's sovereignty as well.

Taken together, the rulemaking and rule-clarifying efforts by China, Russia, and Iran leave no doubt that these "Westphalian" actors are firmly in the same camp as the authors of the Tallinn Manual in regarding sovereignty as a primary rule of international law, and not simply a principle. At the same time, it is clear that when it comes to the substantial scope of the rule, interpretations diverge vastly. While the Manual goes to great lengths to limit the content of the rule of sovereignty to more severe forms of a violation of ter-

125. *See, e.g.*, *Russia Tells Google Not To Advertise "Illegal" Events after Election Protests*, REUTERS (Aug. 11, 2019, 8:20 AM), https:// www.reuters.com /article /us-russia- politics- protests-google/ russia-after-protests-tells-google-not-to-advertise-illegal-events-idUSKCN1V10BY.

126. *See* Li Baodong, Vice Foreign Minister, Ministry of Foreign Affs. of China, Address at the Opening Ceremony of the International Workshop on Information and Cyber Security (June 5, 2014), https://www.fmprc.gov.cn/mfa_eng/wjbxw/t1162458.shtml.

127. *China Supports Free Flow of Information*, GLOB. TIMES (May 31, 2017), https://www.globaltimes.cn/content/1049411.shtml (emphasis added).

128. Press Release, Ministry of Foreign Affs., International Strategy of Cooperation on Cyberspace (Mar. 1, 2017), http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm (China). On this central function of sovereignty for the strategy, see Zhang Xinbao, *China's Strategy for International Cooperation on Cyberspace*, 16 CHINESE J. INT'L L. 377, 379–81 (2017).

129. *Armed Forces Warns of Tough Reaction to Any Cyber Threat – Iran*, ALDIPLOMASY (Aug. 17, 2020), https://www.aldiplomasy.com/en/?p=20901.

ritorial integrity and the interference with "inherent governmental functions,"[130] the principal rationale of the authoritarian actors' emphasis on the inviolability of sovereignty is the anxiety caused by the potentially destabilizing information flows of the "free and open" internet.[131] Only Iran's recent statement seems to be concerned primarily with threats from cyber operations against the logical and physical layers of its domestic cyber infrastructures, which may simply result from the fact that it was prepared by the armed forces. The important differences between these state actors and the Manual, however, have not prevented Western scholars looking for a consolidation of state practice regarding the rule-status of sovereignty from citing the official expressions of the SCO[132] and Iran[133] in support of their arguments.

To be sure, the stated emphasis on mutual respect for sovereignty is not at all free of contradictions and in particular does not imply that the "Westphalian" actors in fact show any such restraint in their dealings with other countries on the international stage.[134] Just as the idea of the "free and open" internet as a facilitator of a liberal world order represents one of the last remnants of the post-Cold War story of inevitable progress, the sovereignty discourse primarily functions as a *metanarrative*—if not in a strictly Lyotardian understanding.[135] It describes the "Westphalian" camp's self-perceived position within the arena of international politics, in particular as it relates to transnational cybersecurity. Consequently, neither of these overarching narratives is set in stone nor invulnerable to shifting political-ideological parameters, as exemplified by the partial rollback of liberalist international policies initiated by the US administration during the Trump presidency.

---

130. TALLINN MANUAL 2.0, *supra* note 5, at 17–27.

131. BROEDERS ET AL., *supra* note 1, at 9.

132. Schmitt & Vihul, *supra* note 12, at 1167–68.

133. Michael N. Schmitt, *Noteworthy Releases of International Cyber Law Positions – Part II: Iran*, ARTICLES WAR (Aug. 27, 2020), https://lieber.westpoint.edu/iran-international-cyber-law-positions/; Przemysław Roguski, *Iran Joins Discussions of Sovereignty and Non-Intervention in Cyberspace*, JUST SEC. (Sept. 3, 2020), https://www.justsecurity.org/72181/iran-joins-discussions-of-sovereignty-and-non-intervention-in-cyberspace/.

134. *See* Jacob Stokes, *Does China Really Respect Sovereignty?*, DIPLOMAT (May 23, 2019), https://thediplomat.com/2019/05/does-china-really-respect-sovereignty/ (demonstrating that China does not show such restraint). Similar observations hold true concerning Russia's interventions in Georgia and Ukraine and Iran's politics towards Iraq, Syria, Lebanon, or Yemen. Peter Dickinson, *The 2008 Russo-Georgian War: Putin's Green Light*, ATLANTIC COUNCIL (Aug. 7, 2021), https:// www.atlanticcouncil.org/ blogs/ ukrainealert/the-2008-russo-georgian-war-putins-green-light/; Kasra Aarabi, Iran's Regional Influence Campaign Is Starting to Flop, FOREIGN POL'Y (Dec. 11, 2019, 6:51 AM), https://foreignpolicy.com/2019/12/11/collapse-iranian-shiism-iraq-lebanon/.

135. JEAN-FRANÇOIS LYOTARD, THE POSTMODERN CONDITION: A REPORT ON KNOWLEDGE xxiii–xxiv (1984).

IV. WHITHER THE THIRD WAY? EMERGING STATE PRACTICE TOWARD SOVEREIGNTY IN CYBERSPACE

So far, we have examined the attitudes of the U.S. and the U.K. on the one hand, and of a couple of non-Western states with authoritarian regimes on the other, with regard to the character and status of sovereignty in cyberspace. This leaves a great number of states from all parts of the globe whose legal opinions may be described as representing a third way between the imperialist and Westphalian ordering principles of cyberspace.

A. The "Free and Open" Net: Affirmation and Pushback

Most Western and other states with liberal-democratic political systems have by and large embraced the U.S. approach in developing an internet that is free, open, and built on interoperable components for frictionless exchange of ideas and commercial goods.[136] This broad consensus usually groups these states together as "likeminded" and distinguishes them from China, Russia, and other actors that opt for tight state control over their citizens' online activities.[137]

At the same time, in this context it is worth noting that in recent years, there has been at least a cautious pushback against American dominance over the internet even among Western actors, on both the technological and legal level. The most outspoken of these actors has been the European Union, which has begun to emphatically promote the idea of "technological" or "digital sovereignty," a policy that accentuates the substantial entanglement of the factual and legal dimensions of sovereignty in a way that echoes the Westphalian approach. If the essence of sovereignty is indeed control, then "digital sovereignty," as "the *ability* of an entity to personally decide the future form of identified dependencies in digitalization and to *possess the necessary powers*"[138] points in this exact direction. Similar to the concept of "cyber sovereignty" described above, "digital sovereignty" can thus be interpreted as an effort to create the preconditions for self-determined agency in the digital domain that the imperialist model has dismissed as factually inconceivable and therefore legally vacuous.[139] This (re)assertion of sovereign prerogatives by way of control has a legal dimension as well, which is

136. *See* Morgus & Sherman, *supra* note 32, at 7.

137. *See* BROEDERS ET AL., *supra* note 1, at 1.

138. FALK STEINER & VIKTORIA GRZYMEK, DIGITAL SOVEREIGNTY IN THE EU 7 (2020), https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Digital_Sovereignty_in_the_EU_Policy_Brief_BSt_EZ_European_Public_Goods_EN.pdf (emphasis added).

139. To be sure, the concept of "digital sovereignty" is not only, and perhaps not even primarily, directed against U.S. hegemony in the tech sector, but just as much against the emergence of Chinese dominance, as could be witnessed in the debate surrounding 5G and Huawei. *See* FRANCES G. BURWELL

best exemplified by the controversial EU General Data Protection Regulation (GDPR).[140] Ironically, the interpretation of the GDPR vis-à-vis data protection standards in the U.S. by the European Court of Justice has even been lambasted as an expression of European "judicial imperialism."[141]

B. In Dialogue with Tallinn: Official Statements on Sovereignty

More importantly for the question of the legal status of sovereignty, a growing number of states have started to issue official statements to lay out their opinion on the matter. After initial reluctance to directly acknowledge the work of the international group of experts,[142] the Tallinn Manual 2.0 has by now become the treatise that most state representatives seem to grapple with when determining their legal positions toward the application of existing international law to cyber operations. In particular, the Manual has exerted considerable influence on the matter concerning the ontological properties and substance of sovereignty. Even though the Manual purports to merely cautiously identify and restate existing customary law, the text's publication has had the effect of prompting subsequent discussions to undertake a doctrinal exegesis of the work as if it were an official legal document. As a result, the Manual's deliberations on sovereignty have assumed an outsized role in the discourse, shaping arguments by *a priori* delimiting their admissible scope.

France, acknowledging the work of the Manual as "the most comprehensive example" of expert treatments of the subject matter, came out with an expansive interpretation of the "rule of sovereignty."[143] Adopting an "intrusion-based approach,"[144] the state assumes a violation whenever an adversarial state conducts an "unauthorised penetration . . . of French systems or any production of effects on French territory via a digital vector."[145] In a

& KENNETH PROPP, ATL. COUNCIL, THE EUROPEAN UNION AND THE SEARCH FOR DIGITAL SOVEREIGNTY: BUILDING "FORTRESS EUROPE" OR PREPARING FOR A NEW WORLD? (2020), https:// www.atlanticcouncil.org/ wp-content/ uploads/ 2020/ 06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf.

140. Enforced since May 2018, the GDPR is the principal data privacy legislation of the European Union. *See* Matt Burgess, *What Is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Mar. 24, 2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

141. Stewart Baker, *How Can the U.S. Respond to Schrems II?*, LAWFARE (July 21, 2020, 8:11 AM), https://www.lawfareblog.com/how-can-us-respond-schrems-ii.

142. *See* Efrony & Shany, *supra* note 6, at 583.

143. MINISTÈRE DES ARMÉES [MINISTRY OF THE ARMIES], INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE 5 (2019), https:// www.defense.gouv.fr/ content/ download/ 567 648/ 9770 527/ file/ international+ law+applied+to+operations+in+cyberspace.pdf (Fr.).

144. *See* Roguski, *supra* note 17, at 65.

145. MINISTRY OF THE ARMIES, *supra* note 143, at 6.

2019 letter to the parliament, the Dutch Ministry of Foreign Affairs dealt extensively with sovereignty, stating that the Netherlands "believes that respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act."[146] Regarding the content of the rule, while cautiously pointing out the "firmly territorial and physical connotations of the traditional concept of sovereignty[,]"[147] the document endorses the work of the Manual by simply quoting its rule 4, which deals with the substance of the rule of sovereignty in detail.

More recently, additional states have publicly endorsed the rule-status of sovereignty in cyberspace. During a session of the UN OEWG in February 2020,[148] both Austria and the Czech Republic approved the stance that sovereignty is a primary rule.[149] Similarly, Germany, likely explicitly citing Tallinn Manual's rule 4, recently declared that "[s]tate sovereignty constitutes a legal norm in its own right and may apply directly as a general norm also in cases in which more specific rules applicable to State behaviour, such as the prohibition of intervention or the use of force, are not applicable."[150] Finland published a very detailed statement on its position in 2020. Similar to the Netherlands, the state not only concurred that sovereignty has the status of a primary rule, it explicitly cited the bifurcated approach taken by the Manual in regard to its substance.[151] Finally, NATO agreed that violations of the rule of sovereignty are possible from a legal perspective in its Allied Joint Doctrine for Cyberspace Operations. Only the U.K. added a reservation to the passage to ensure that AG Wright's 2018 speech would not be mistaken as an accidental aberration.[152] While the U.S. did not join its closest ally in objecting to NATO's official standpoint, it also did not explicitly endorse the "rule" interpretation.

---

146. Letter from Ministry of Foreign Affs. of the Neth. to the Parliament, app at 2 (2019) (discussing government obligations under international law in cyberspace).

147. *Id.*

148. *See Open-Ended Working Group*, U.N. OFF. FOR DISARMAMENT AFFS., https:// www.un.org/disarmament/ open-ended-working-group/ (last visited Nov. 5, 2021).

149. Przemysław Roguski, *The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States*, JUST SEC. (May 11, 2020), https:// www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

150. FED. GOV. OF GER., ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE 3 (2021), https:// www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf. Evidently, Germany understands "norm" to mean "(primary) rule."

151. *See* MINISTRY FOR FOREIGN AFFAIRS, INTERNATIONAL LAW AND CYBERSPACE: FINLAND'S NATIONAL POSITIONS (2020) (Fin.).

152. *See* NATO, ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS v (2020).

A series of sessions in 2020 operating within the framework of the Organization of American States confirms the assessment concerning the U.S. position. These sessions ascertained how its member states understand the application of international law to state-led cyber operations.[153] The U.S. did not deviate from its earlier statements that state practice has not been sufficiently uniform.[154] Most other participating states did not expressly address the matter during the sessions. Only Bolivia, Guatemala, and Guyana supported the "sovereignty-as-rule" standpoint. And while the Tallinn Manual 2.0 appears to have been under consideration, it is unclear how much significance the participants ascribed to it.[155]

Toward the end of 2020, New Zealand and Israel published remarkable statements related to the ongoing debates on sovereignty and hinted at the Manual's contribution. The statements explicitly adopted the Manual's language[156] but deviated from it on one substantial aspect: instead of falling in line with the "sovereignty-as-rule" camp, both states declared the notion to be a mere principle from which primary rules can be derived, among them "territorial sovereignty."[157] The significance of this particular interpretation of existing law will be further examined in section five.

This brief survey of current state practice shows that the question of the legal status of sovereignty is today more firmly on the international agenda than perhaps at any point in the past thirty years. Further, the discussions demonstrate the outsized influence that the Tallinn Manual has had in both academic circles and state policy. The following section further examines the discourse by drawing attention to some of the potential perils of the Tallinn interpretation of sovereignty in view of the politics and ideologies underlying the imperialist and Westphalian approaches to cyberspace. Subsequently, the essay attempts to offer an alternative understanding of the law that might be better suited to avoid these downsides.

153. Organization of American States, *Improving Transparency: International Law and State Cyber Operations – Fourth Report*, CJI/doc. 603/20 rev.1 corr.1, ¶ 55 (Mar. 5, 2020).

154. *Id.*

155. *Id.* ¶¶ 50–54.

156. *See* N.Z. FOREIGN AFFS. & TRADE, *supra* note 55, ¶ 11 (using the language: "inherently governmental functions of another").

157. *Id.* ¶ 11–15; Roy Schöndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INT'L L. STUD. 395, 402 (2021).

V. RECONFIGURING THE DISCOURSE

A. The Pitfalls of Conceiving Sovereignty as a Rule

When Martti Koskenniemi remarked in 2011 that "'sovereignty' has lost much of its normative or descriptive meaning" and indeed its "magic,"[158] he clearly did not anticipate the renaissance the concept would soon enjoy in the context of transnational cybersecurity. The last time talk of "sovereignty" was this popular was perhaps at the height of the Cold War during the process of decolonization when newly independent states seized on the notion to assert their path to self-determination against the dominance of the Global North.[159] But whereas in the 1960s and 70s, socialist and developing states insisted on an understanding of the sovereign equality of states comprising the right to freely choose and develop their political, social, economic, and cultural systems,[160] today it is primarily European and other Western states that push for a revival of sovereignty. The revived focus on the protective dimension of sovereignty[161] is the most visible expression of European and Western states feeling vulnerable to foreign influence and interference in view of the novel possibilities of digital technologies.

The "sovereignty-as-rule" discourse must be understood against this backdrop. What is more, the technical peculiarities of cyberspace as an operative domain cast doubt on the utility of traditional ordering principles of international stability, the most important of which are the prohibition of the use of force and the prohibition of intervention. Associated notions that had always been ambiguous and poorly defined but nonetheless taken for granted, such as "coercion" as a precondition of unlawful intervention, suddenly seemed rather ill-suited to constrain states in cyberspace.[162]

The acknowledgment of this uncertainty appears to have been the main motivating factor for the Tallinn Group of Experts to focus on sovereignty. The group zoomed in on sovereignty as a concept capable of regulating state

158. Martti Koskenniemi, *What Use for Sovereignty Today?*, 1 ASIAN J. INT'L L. 61, 62–63 (2011).

159. *See* Lori Fisler Damrosch, *Politics Across Borders: Nonintervention and Nonforcible Influence Over Domestic Affairs*, 83 AM. J. INT'L L. 1, 10–11 (1989); W. Riphagen (Special Rapporteur), *Rep. of the 1966 Special Committee on Principles of International Law concerning Friendly Relations and Co-operation Among States*, ¶¶ 329–33, U.N. Doc. A/6230 (June 27, 1966) [hereinafter *Rep. of the 1966 Special Committee*].

160. *See* Koskenniemi & Kari, *supra* note 96, at 183.

161. On the distinction between the protective dimension of sovereignty and the principle "as a legitimation of state action" see Wouter G. Werner, *State Sovereignty and International Legal Discourse*, *in* GOVERNANCE AND INTERNATIONAL LEGAL THEORY 125, 147 (Ige F. Dekker & Wouter G. Werner eds., 2004).

162. *See* Ido Kilovaty, *The Elephant in the Room: Coercion*, 113 AM. J. INT'L L. UNBOUND 87, 88–89 (2019).

behavior "below" the thresholds of force and coercion and looked for corroborative practice of states and other international actors as evidence for the rule-status of sovereignty. As Anthony Carty observed thirty years ago, however, one of the pitfalls of the positivist-doctrinal approach of dissecting state practice is that it tends to fall victim to confirmation bias.[163] The problem with this approach in the present context is that the abstract concept of sovereignty means vastly different things to different states by virtue of diverging historical, ideological, and political trajectories,[164] with the consequence that seemingly congruent expressions of legal views may in fact be irreconcilable on a subtextual, substantial level.[165]

The attempt to prove that sovereignty is a rule is therefore not without a cost. Treating "sovereignty" as one uniform, "fallback" *rule*[166] instead of conceiving it as a more abstract principle[167] enables authoritarian states to co-opt the sovereignty discourse in the ongoing processes of norm identification and clarification in cyberspace. These states are also able to promote an overly broad understanding of the legally protected sovereign prerogative. This tactic could recently be witnessed when China submitted statements within the framework of the UN OEWG.[168] In response, democratic states that endorse sovereignty as a primary rule are forced to engage in rear-guard battles in an attempt to limit the rule's substantive scope so that a liberal

163. *See* Anthony Carty, *Critical International Law: Recent Trends in the Theory of International Law*, 2 EUR. J. INT'L L. 1, 1 (1991).

164. *See* Maximilian Bertamini, *United in What? Some Reflections on the Security Council's Sovereignty Rhetoric in the Latest Syria Resolutions*, EJIL:TALK! (Oct. 21, 2020), https:// www.ejiltalk.org/united-in-what-some-reflections-on-the-security-councils-sovereignty-rhetoric-in-the-latest-syria-resolutions/ (discussing various national responses to Syria's claims of sovereignty).

165. *See* Schmitt & Vihul, *supra* note 12, at 1667–68 (approvingly citing the view of the Shanghai Cooperation Organization on sovereignty).

166. According to Nicholas Tsagourias, sovereignty "captures any interference within a state's exclusive internal and external authority which is not captured by other more specific rules such as those on non-intervention or non-use of force." Nicholas Tsagourias, *Law, Borders, and the Territorialisation of Cyberspace*, 15 INDONESIAN J. INT'L L. 523, 544 (2018).

167. In the words of James Crawford, sovereignty contains "the collection of rights held by a state." JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 432 (9th ed. 2019).

168. U.N. Open Ended Working Group, *China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, at 2–3 (2020), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf ("*It is widely endorsed by the international community that the principle of sovereignty applies in cyberspace.* The Group should enrich and elaborate on the specification of the principle, thus laying solid foundation for the order in cyberspace . . . States should refrain from using ICTs to interfere in internal affairs of other states and undermine their political, economic and social stability.") (emphasis added). All OEWG documents are available at <https://www.un.org/disarmament/open-ended-working-group/>. Note that although China speaks of the "principle of sovereignty" here, the context and earlier statements make clear that it implies the notion's rule-status.

interpretation of "sovereignty" may prevail.[169]

At the same time, insisting on sovereignty as one unified, all-encompassing rule makes it easy for proponents of the imperial model of cyberspace to declare any attempts to comprehensively regulate adversarial state behavior in the digital domain to be fundamentally at odds with the idea of the "free and open" internet.[170] If authoritarian regimes are able to "hide behind"[171] "sovereignty" to carry on denying their citizens basic human rights and conducting harmful cyberattacks against other states,[172] then accepting its rule-status can only do more harm than good.[173]

As a result, the content of the ostensible "rule of sovereignty" necessarily remains highly contested and ambiguous. In turn, this might be one factor that explains why states are reluctant to explicitly invoke a violation of the purported rule when calling out adversarial cyber operations that remain below the thresholds of force and coercion as violations of international law even when their unlawfulness seems obvious in a given case.[174] This is not surprising. The analysis suggests that sovereignty might simply be too historically contentious, politically and ideologically malleable, and legally

169. *See* U.N. Open-Ended Working Group, *Pre-Draft Report of the OEWG – ICT: Comments by Austria*, at 3 (Mar. 31, 2020), https:// front.un-arm.org/ wp-content/ uploads/ 2020/04/comments-by-austria.pdf ("[A] violation of the principle of State sovereignty constitutes an internationally wrongful act . . . It is clear, however, that references to State sovereignty must not be abused to justify human rights violations within a State's borders. In other words, State sovereignty must not serve as a pretext for tightening control over a State's citizens, which undermines their basic human rights such as the right to privacy and the freedom of expression.").

170. *See, e.g.*, U.S.-CHINA ECON. & SEC. REV. COMM'N, REPORT TO CONGRESS 95 (2019), https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf ("In contrast to the open and free conception of internet governance championed by the United States, China promotes so-called 'internet sovereignty,' or the idea that governments should be able to control their countries' internets to prevent instability from public access to sensitive information from foreign or domestic sources.").

171. WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 1 (2018), https:// trumpwhitehouse.archives.gov/ wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

172. Less explicitly in this direction, see Wright, *supra* note 19.

173. *See* Oona A. Hathaway & Alasdair Phillips-Robins, *COVID-19 and International Law Series: Vaccine Theft, Disinformation, the Law Governing Cyber Operations*, JUST SEC. (Dec. 4, 2020), https://www.justsecurity.org/73699/covid-19-and-international-law-series-vaccine-theft-disinformation-the-law-governing-cyber-operations/ (making an alternative argument from an academic perspective by claiming that "[i]t is not just States that would find their activities curtailed by a free-standing sovereignty rule prohibiting cross-border cyber operations. Human rights organizations, for example, often seek to influence the politics and law of the countries within which they operate, and these influence campaigns sometimes involve cross-border operations that are resisted by the sovereign State in which they occur. Russia, for instance, has banned foreign non-governmental organizations. A broad rule of sovereignty might help legitimate Russia's actions by giving rise to a claim that these organizations and their sponsors are violating Russia's 'sovereignty'").

174. *See, e.g.*, Przemysław Roguski, *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*, JUST SEC. (Mar. 6, 2020), https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

blunt a concept to be able to meaningfully account for the different understandings that result from conflicting attitudes of states and thus to constrain state behavior in cyberspace. As put by a participant during a discussion on the subject between sixteen representatives of member states of the Organization of American States, "there may be too many meanings for the term 'sovereignty' to ascribe it a rule-like status."[175] In other words, it may be useful as a principle but not as a rule.

B. The Principle of Sovereignty and Its Derivative Primary Rules

That being said, this essay does not contend that absent a "rule of sovereignty," states are left without legal protection against adversarial state behavior in cyberspace. Far from it. But I submit that the "sovereignty-as-rule" discourse, by making this fundamental principle the primary subject of legal analysis, obscures more than it clarifies. The discourse rests on the premise that if sovereignty is not accepted as a rule, only two rules with independent legal status, the use of force and the principle of non-intervention, remain applicable for assessing cyber operations. If the threshold for either rule is not met, we are left in a legal vacuum where basically everything goes.[176] But that is a curious assumption to make. There is another more persuasive interpretation based on the available evidence of international practice. This evidence suggests—as the doctrinal work of the theory's proponents in fact shows—the existence of a number of further primary rules *derived from* the principle of sovereignty.

Trying to determine the status of the principle of sovereignty and identify its primary rules is made somewhat more difficult by the notion's structural ambiguity[177] and the lack of uniformity in the relevant terminology applied in international practice.[178] For instance, official statements from states on international legal matters often use the formula of the "sovereignty, territorial integrity and political independence" of states,[179] even though the common understanding is that the latter two notions are at least also essential

175. Organization of American States, *Improving Transparency: International Law and State Cyber Operations – Fifth Report*, CJI/doc. 615/20 rev.1, ¶ 45 (Aug. 7, 2020).

176. Tsagourias, *supra* note 166, at 541. *See also* Roguski, *supra* note 174.

177. MARTTI KOSKENNIEMI, FROM APOLOGY TO UTOPIA: THE STRUCTURE OF INTERNATIONAL LEGAL ARGUMENT 239 (2005).

178. *See* CRAWFORD, *supra* note 167, at 192, 432 ("The word itself has a lengthy and troubled history, and is susceptible to multiple meanings and justifications"); MICHAEL AKEHURST, A MODERN INTRODUCTION TO INTERNATIONAL LAW 15 (4th ed. 1982) ("It is doubtful whether any single word has caused so much intellectual confusion.").

179. *See* U.N. SCOR, 70th Sess., 7504th mtg. at 4, UN Doc. S/PV.7504 (Aug. 17, 2015) (noting Venezuela's Disassociation from the Presidential Statement Expressing Support for UN Special Envoy Staffan de Mistura); S.C. Res. 2178 (Sept. 24, 2014).

components of the former. In addition, international actors are not always clear about whether they are referring to "sovereignty" or "territorial sovereignty" in a given context, or if they are using the two concepts interchangeably.[180] This lack of clarity is not confined to "sovereignty." Nicholas Tsagourias has pointed out that not even the terminological distinction between the notions of "rules" and "principles" is consistently upheld, not least by the ICJ.[181] With that in mind, the following should be seen as an attempt to make sense of the incoherent picture by structuring the at times overlapping relevant concepts. Due to their inherently blurred edges, this essay can hardly claim to be the be-all and end-all to the discourse. Other interpretations of the available materials, including those subsequently criticized, will remain both possible and reasonable.

Despite this caveat, I submit that the insistence on sovereignty as a primary rule in itself is ultimately not persuasive. Consider the argument, put forth by Michael Schmitt and Liis Vihul, that "[t]he fact that States at times chose to discuss an incident as a breach of their territorial inviolability when the actions might also have crossed the use-of-force or coercive-intervention thresholds demonstrates that States consider the former to be a primary rule distinct from other primary rules that are based in the principle of sovereignty."[182] For example, the authors observe, "[a]lthough drone operations implicate the prohibition on the use of force, States regularly characterize them as sovereignty violations."[183] Importantly, although they explicitly mention the more limited concept of the inviolability of territory, they interpret this as evidence for their argument that the injured state assumed the existence of a "rule of sovereignty."

However, it seems more persuasive to argue that when states invoke a violation of their sovereignty in such a context, they do not imply the breach of a rule with the simple, all-encompassing content "respect for sovereignty" that exists alongside the prohibition of the use of force or another primary rule derived from the principle. Instead, in these statements, "sovereignty" operates as the *legally protected interest* that the prohibition of the use of force aims to protect; the violation of this primary rule necessarily entails a

180. *See Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, Judgment, 1986 I.C.J. 14, ¶ 212–13 (June 27); Rainbow Warrior Affair (N.Z. v. Fr.), 19 R.I.A.A. 199, 201, 209 (1986).

181. Nicholas Tsagourias, *Malicious Cyber Operations against Health Infrastructure during the Covid-19 Pandemic and the Renvoi to Sovereignty in Cyberspace*, 9 ESIL REFLECTIONS 1, 5 (2020) (referencing Delimitation to Maritime Boundary in Gulf of Maine Area (Canada v. U.S.), Judgment, 1984 I.C.J. Rep. 246, ¶ 79 (Oct. 12)).

182. Schmitt & Vihul, *supra* note 12, at 1656.

183. *Id.* at 1657.

violation of sovereignty.[184]

If we accept this interpretation, it becomes apparent that this argumentative structure is common practice. Take as one recent example the assassination, by drone strike, of the head of Iran's Quds force, Major General Qassem Soleimani, by the U.S. military on Iraqi soil in early January 2020. In its letter to the UN Security Council, the Iraqi representative called the operation "an aggression against the State, Government and people of Iraq," a choice of words that clearly implies that Iraq considered the incident an unlawful use of force and in fact even an armed attack.[185] Significantly, the letter went on to state that "these American attacks . . . violate the sovereignty of Iraq."[186] Article 2(4) UN Charter makes clear that it is the purpose of the prohibition of the use of force to protect the "territorial integrity" and "political independence" of all states, which are, as mentioned, considered the two most central elements of the principle of sovereignty.[187] For this reason, it makes little sense to assume that in choosing these particular words, Iraq meant to assert a violation of the "rule of sovereignty" in its manifestation of territorial inviolability, *in addition to* an unlawful use of force by the U.S. Rather, it is more compelling to interpret this phrasing as claiming a violation of its sovereignty *as a consequence of* the breach of the prohibition of the use of force, a rule whose purpose it is to protect the former. The explicit reference to a violation of Iraq's sovereignty here functions merely as a signifier of the legally protected interest that has been harmed through the violation of the primary rule.[188]

---

184. Note that this does not imply that sovereignty is the *only* good that the prohibition of the use of force is meant to protect; further protected goods are at least human life and international peace and stability. *See* Tom Ruys & Felipe Rodríguez Silvestre, *The Nagorno-Karabakh Conflict and the Exercise of "Self-Defense" to Recover Occupied Land*, JUST SEC. (Nov. 10, 2020), https:// www.justsecurity.org/ 73310/ the-nagorno-karabakh-conflict-and-the-exercise-of-self-defense-to-recover-occupied-land/.

185. On the equation of "aggression" and "armed attack," see *Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda)*, Judgment, 2005 I.C.J Rep. 168, ¶ 146 (Dec. 19).

186. Permanent Rep. of Iraq to the U.N., Identical letters dated January 6, 2020 from the Permanent Rep. of Iraq to the United Nations addressed to the President of the Security Council, U.N. Doc. S/2020/15 (Jan. 6, 2020).

187. G.A. Res. 2625 (XXV) (Oct. 24, 1970); Final Act of the Conference on Security and Co-operation in Europe (Helsinki Final Act) art. 1(a)(I), Aug. 1, 1975, 14 I.L.M. 1292; *see* Koskenniemi & Kari, *supra* note 96, 184–86.

188. *But see* Nicholas Tsagourias, *Self-Defence against Non-state Actors: The Interaction between Self-Defence as a Primary Rule and Self-Defence as a Secondary Rule*, 29 LEIDEN J. INT'L L. 801, 803 (2016) (arguing that in the case of military operations by Western states against ISIS on Syrian territory, Syria subsequently merely invoked a violation of its sovereignty but not a violation of the prohibition of the use of force; however, this does not necessarily imply that Syria assumed a violation of the "rule of sovereignty"; its choice of words, "to be present on Syrian territory without the consent of the Syrian government," at least allows for the interpretation that what it invoked was the "rule of territorial inviolability," whose object and purpose it is to protect the state's sovereignty, as will be further explained shortly); *see* Permanent Rep. of the Syrian Arab Republic to the U.N., Identical letters dated September

Once we recognize this argumentative structure,[189] which is based on the distinction between the violation of the primary rule of international law whose purpose it is to protect sovereignty on the one hand and the violation of sovereignty as the protected interest on the other, we can see how it resurfaces in contexts outside of violations of the use of force. These cases suggest the existence of additional primary rules aimed at protecting a state's sovereignty. As in fact pointed out by most of the proponents in the "sovereignty-as-rule" camp, the least controversial rule is the "rule of territorial inviolability." But as opposed to the approach proposed here, these authors do not consider it a primary rule by itself but instead an integral part of the more comprehensive "rule of sovereignty."[190] This may partly result from a lack of conceptual clarity as to the distinction between "territorial sovereignty"— as another term for "territorial inviolability" or "territorial integrity," which often seem to be used synonymously— and "sovereignty," whose substantive scope extends beyond the territorial aspect.[191] "Sovereignty" and "territorial sovereignty" are not congruent. Evidence from international practice supports this interpretation. For example, in *Corfu Channel*, the ICJ asserted a "violation of Albanian sovereignty" *as a consequence* of the U.K.'s failure to respect its "territorial sovereignty."[192] Similarly, in the *Rainbow Warrior* arbitration between New Zealand and France, both parties agreed that the sinking of the vessel in the port of Auckland by French foreign intelligence service DGSE amounted to a "serious violation of New Zealand sovereignty" *as a result of* the "violation of the territorial sovereignty of New Zealand."[193] These cases implicitly recognized that the primary rule breached was the "inviolability" of territory,[194] "territorial integrity," or "territorial sovereignty," while "sovereignty" operated as the protected interest that was

17, 2015 from the Permanent Rep. of the Syrian Arab Republic to the United Nations addressed to the Secretary-General and the President of the Security Council, U.N. Doc. S/2015/719 (Sept. 21, 2015).

189. *See* James Crawford (Special Rapporteur on State Responsibility), *Second Report on State Responsibility*, ¶ 299, U.N. Doc. A/CN.4/498 (1999) (discussing what kinds of rule violations Article 21 of the ILC Articles on the Responsibility of States for Internationally Wrongful Acts might exonerate when a state resorts to self-defense, such as "trespass[ing] on [the aggressor state's] territory" and "interfer[ence] in [the aggressor state's] internal affairs," but not "sovereignty" in and of itself; implying that the Special Rapporteur considers the former two primary rules of international law but not the latter, an understanding in line with the view advocated here).

190. *See* Schmitt & Vihul, *supra* note 12, at 1639; Spector, *supra* note 12, at 219; Roguski, *supra* note 17, at 65; DELERUE, *supra* note 16, at 200–32.

191. *See generally* TALLINN MANUAL 2.0, *supra* note 5, at 20.

192. *Corfu Channel (U.K. v. Alb.)*, Judgment, 1949 I.C.J. 4, 35 (Apr. 9).

193. Rainbow Warrior Affair (N.Z. v. Fr.), 19 R.I.A.A. 199, 201, 209 (1986).

194. *See generally* SHAW, *supra* note 48, at 488 (describing the concept of territory in international law).

violated as a consequence of the breach.[195] In *Military and Paramilitary Activities in and Against Nicaragua*, the ICJ invoked the "duty of every State to respect the territorial sovereignty of others" as the operative primary rule in relation to the minelaying activities in the territorial sea of Nicaragua, while it was the state's sovereignty that was *affected* by virtue of this unlawful conduct.[196] A corresponding construction of "sovereignty" as a principle and "territorial sovereignty" as a primary rule that is consistent with the understanding advocated here can be derived from *Costa Rica v. Nicaragua*.[197]

This argumentative pattern in relation to sovereignty is familiar from other contexts that involve questions of sovereignty beyond its protective dimension. As noted by Martti Koskenniemi, international courts and tribunals frequently deal with cases that prima facie appear to revolve around claims about sovereignty only to reveal themselves as concerning the existence and extent of specific "rights, liberties and competences," but not sovereignty as a rule in itself.[198] For instance, in the *Asylum Case*, while both Peru and Colombia invoked their sovereignty as the basis for their claims, the ICJ did not address this line of argumentation and instead proceeded to identify specific rights derived from the principle, namely the right to grant diplomatic asylum on the one hand and the right to deny safe exit through one's own territory on the other.[199] The same holds true for the *Right of Passage Case*, which ostensibly involved conflicting claims of sovereignty but in the eyes of the Court came down to the question of whether certain specific, customary rights exist that find their basis in the *principle* of sovereignty.[200] Therefore, both cases provide further evidence that "sovereignty"

195. See the recent official statements by New Zealand and Israel: N.Z. FOREIGN AFFS. & TRADE , *supra* note 55, ¶¶ 11–12; Schöndorf, *supra* note 157, at 402.

196. *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, Judgment, 1986 I.C.J. 14, ¶ 213 (June 27). But see *id.* ¶ 251, where the Court speaks of "the principle of respect for territorial sovereignty;" as mentioned above, the terminology is rarely clear-cut. *See also* Schmitt & Vihul, *supra* note 12, at 1653–54 (referring to *territorial sovereignty* in their analysis of the case while still using it as support for the existence of a rule of *sovereignty*).

197. Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicar.) and Construction of a Road in Costa Rica along the San Juan River (Nicar. v. Costa Rica), Judgment, 2015 I.C.J. Rep. 665, ¶ 229 (Dec. 16).

198. KOSKENNIEMI, *supra* note 177, at 247.

199. Asylum (Colom. v. Peru), Judgment, 1950 I.C.J. 266, 278–79 (Nov. 20). This case asks, *inter alia*, "[w]hether a state was required to allow safe passage out of its territory to an individual that had been granted diplomatic asylum in another state." *Asylum, Colombia v Peru, Merits, Judgment, [1950] ICJ Rep 266, ICGJ 14 (ICJ 1950), 20th November 1950, International Court of Justice [ICJ]*, OXFORD PUB. INT'L L., https:// opil.ouplaw.com/ view/ 10.1093/ law:icgj/ 194icj50.case.1/law-icgj-194icj50 (last visited Oct. 25, 2021).

200. Right of Passage Over Indian Territory (Port. v. India), Judgment, 1960 I.C.J. 6, 36–45 (Apr. 12). The case concerned the question, *inter alia*, "[w]hether the right of passage of military personnel and arms should have the same right of passage over Indiana territory as that of private persons and goods." *Right of Passage over Indian Territory, Portugal v India, Merits, Judgment, [1960] ICJ Rep 6, ICGJ 174*

operates as a background principle that allows for the identification and derivation of specific norms that possess the status of rules under positive international law.

The prohibition for a state to exercise its power on the territory of another state is a further primary rule derived from the principle of sovereignty that is distinct from the rule of territorial inviolability.[201] The Tallinn Manual discusses this rule as part of the content of the rule of sovereignty as "usurpation of . . . inherently governmental function[s]."[202] A violation of this rule will often automatically entail a violation of the rule of territorial inviolability. For example, if agents of the responsible state physically enter the victim state's territory to exercise state power, as was the case when Mossad agents abducted Eichmann from Argentinian territory or when British warships conducted enforcement measures in the territorial sea of Albania (*Corfu Channel Case*), both the rule of territorial inviolability and the rule of the prohibition to exercise state power on the territory of another state have been breached. For this reason, the two rules together amount to what state practice and international jurisprudence generally designate as the rule of "territorial sovereignty."[203] However, this does not necessarily need to be the case. For instance, consider the hypothetical example of the Norwegian authorities disseminating stay-at-home orders in the Swedish language via social media because they are dissatisfied with their neighbor's lenient response to COVID-19, micro-targeting Swedish citizens and pretending to act on behalf of the Swedish government. This should be qualified as an exercise of state power on Swedish territory without a simultaneous breach of the rule of territorial inviolability because while the order constitutes an official act that was within the sovereign prerogative of the Swedish government, Norway issued it without entering Swedish territory.[204] Furthermore, as breaches of territorial inviolability will often occur without an additional exercise of state power—for example, by a plane violating a state's airspace—it is analytically more accurate to treat them as two separate primary rules derived from sovereignty.

(ICJ 1960), 12th April 1960, International Court of Justice [ICJ], OXFORD PUB. INT'L L., https://opil.ouplaw.com/view/10.1093/law:icgj/174icj60.case.1/law-icgj-174icj60 (last visited Oct. 25, 2021).

201. *See* DELERUE, *supra* note 16, at 214–15; N.Z. FOREIGN AFFS. & TRADE, *supra* note 55, ¶ 11.

202. *See* TALLINN MANUAL 2.0, *supra* note 5, at 24.

203. The rule of territorial sovereignty has been referenced by New Zealand and Israel in their recent statements on the application of international law to cyberspace. *See* N.Z. FOREIGN AFFS. & TRADE, *supra* note 55, ¶¶ 11–13; Schöndorf, *supra* note 157, at 402.

204. Peter B.M.J. Pijpers & Bart G.L.C. van den Bosch, *The "Virtual Eichmann": On Sovereignty in Cyberspace* 18 (Amsterdam Law School Legal Studies, Research Paper No. 2020-65, 2020) (arguing that the rule of territorial inviolability generally plays a minor rule in cyberspace due to the particular features of the domain as described above; this is disputed here, as will be argued below).

Whereas the authoritative academic literature endorses the assumption that "territorial inviolability" and "prohibition of the exercise of state power on foreign territory" are primary rules derived from the principle of sovereignty,[205] there is no comparable support for the existence of a rule amounting to respect for the right of a state "freely to choose and develop its political, social, economic and cultural systems."[206] Whether states possessed such a right derived from the principle of sovereignty was considered at length during the deliberations of the Special Committee that drafted the text of the Friendly Relations Declaration.[207] The state representatives generally acknowledged the existence of the right but could not reach a definite agreement as to its exact substantive scope. The state representatives mostly discussed the right in the context of the principle of non-intervention as "the negation of sovereign equality,"[208] which implied the obligation to respect the political independence of every state.[209] However, some representatives put forward a broader understanding of "intervention" that included the notion of "interference," described as "acts that were far less serious than armed intervention or subversion."[210] This would have expanded the scope of the prohibition of intervention considerably. At the same time, the U.K. submitted a more limited interpretation that foreshadowed the idea of the "free and open" information ecosystem brought forth by the internet a few decades later: "[I]t should be recognized that in an interdependent world, it is inevitable and desirable that States will be concerned with and will seek to influence the actions and policies of other States, and that the objective of international law is not to prevent such activity but rather to ensure that it is compatible with the sovereign equality of States and self-determination of their peoples."[211] The U.S. endorsed the U.K.'s position.[212] In the end, despite the discomfort of the newly decolonized and socialist states, the view

205. CRAWFORD, *supra* note 167, at 432, speaks of sovereignty as referring to "the rights accruing from the exercise of title [to territory]" and "*[t]he correlative duty of respect for territorial sovereignty*" (emphasis added). *See also* Samantha Besson, *Sovereignty*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 70 (Rüdiger Wolfrum ed., 2012).

206. Milan Sahovic (Special Rapporteur), *Rep. of the Special Committee on Principles of International Law Concerning Friendly Relations and Cooperation among States*, ¶ 409, U.N. Doc. A/6799 (Sept. 26, 1967) [hereinafter *Rep. of the 1967 Special Committee*].

207. *See* Hans Blix (Special Rapporteur), *Rep. of the Special Committee on Principles of International Law Concerning Friendly Relations and Cooperation among States*, ¶¶ 314–315, U.N. Doc. A/5746 (Nov. 16, 1964) [hereinafter *Rep. of the 1964 Special Committee*].

208. *Rep. of the 1967 Special Committee*, *supra* note 206, ¶ 313.

209. *Rep. of the 1966 Special Committee*, *supra* note 159, ¶ 291.

210. *Rep. of the 1967 Special Committee*, *supra* note 208, ¶ 360.

211. *Rep. of the 1964 Special Committee, supra* note 207, ¶ 205.

212. *Id.* at ¶ 207; *see* Robert Rosenstock, *The Declaration of Principles of International Law Concerning Friendly Relations: A Survey*, 65 AM. J. INT'L L. 713, 729 (1971).

prevailed that only coercive interference would henceforth be considered unlawful conduct, with transboundary influencing remaining well below the threshold.

The surge of digital disinformation campaigns by adversarial state actors and other forms of interference in democratic decision-making processes has started to shift a strict application of the coercion requirement toward a new emphasis on other kinds of conduct that infringe on the target state's[213] and its constituent population's freedom of choice.[214] For instance, Australia has begun to call out such adversarial behavior in a way that approximates the argumentative structure laid out above,[215] asserting that "covert foreign influence can cause immense harm to our national sovereignty."[216] The state recently refined this standpoint, which can be understood as suggesting the existence of a (nascent) rule against *covert* influence measures, by making an explicit distinction between "foreign influence" and "foreign interference." Australia describes "foreign interference" as activity that is "coercive, corrupting, deceptive, clandestine [and] *contrary to Australia's sovereignty*, values and national interests."[217] As of August 2021, Australia seems to be the only democratic actor to come out with such a clear statement. Most states remain reluctant to join efforts to clarify or develop customary law in this respect.[218] There appears to be tacit wariness that any hint at determining

213. Kilovaty, *supra* 162, at 87 (discussing New Zealand arguing that cyber disinformation campaigns might meet the coercion requirement); N.Z. FOREIGN AFFS. & TRADE, *supra* note 55, ¶ 10.

214. *See* International Covenant on Civil and Political Rights art. 1, *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171; International Covenant on Economic, Social and Cultural Rights art. 1, *opened for signature* Dec. 16, 1966, 993 U.N.T.S. 14,531 (establishing between a state's right to choose its own political system, its people's right to self-determination, and rules protecting this aspect of sovereignty as the prohibition of intervention has recently been examined by JENS D. OHLIN, ELECTION INTERFERENCE: INTERNATIONAL LAW AND THE FUTURE OF DEMOCRACY (2020)); Nicholas Tsagourias, *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, *in* GOVERNING CYBERSPACE: BEHAVIOUR, POWER AND DIPLOMACY 45 (Dennis Broeders and Bibi van den Berg eds., 2020).

215. *See supra* the text accompanying notes 205–212.

216. *See* Gareth Hutchens, *Brandis Reveals Plans to Curb "Unprecedented" Foreign Influence on Politics*, GUARDIAN (Nov. 14, 2017, 2:37 AM), https:// www.theguardian.com/ australia-news/ 2017 /nov /14/ brandis-reveals-plans-to-curb-unprecedented-foreign-influence-on-politics (noting statement by Australian Attorney General).

217. Dep't of Home Affs., *Countering Foreign Interference*, AUSTL. GOV., https:// www.homeaffairs.gov.au/ about-us/ our-portfolios/national-security/countering-foreign-interference (Feb. 27, 2020) (emphasis added).

218. *See* Henning Lahmann, *Information Operations and the Question of Illegitimate Interference Under International Law*, 53 ISR. L.R. 189, 209–16 (2020) (providing a survey of state practices). *But see* N.Z. FOREIGN AFFS. & TRADE, *supra* note 55, ¶ 10 (declaring "a prolonged and coordinated cyber disinformation operation that significantly undermines a state's public health efforts during a pandemic" as constituting prohibited intervention).

the legal limits of transboundary speech acts would move the discourse further toward the position of China and other adherents of "cyber sovereignty."

To summarize, when "sovereignty" is conceived in the way proposed here, a clearer picture emerges. At its conceptual core, sovereignty is not a rule but a principle; it is indeed "not to be equated with any specific substantive right."[219] Even though it follows that any particular right or duty derived from sovereignty must thus be "grounded in a distinct legal source,"[220] it is important to clarify that I do not claim that the concept of sovereignty by itself is purely descriptive and a mere "abstraction from a number of relevant rules,"[221] devoid of any normative content of its own.[222] The notion does exist as "a normative principle in its own right,"[223] a "general concept which structures legal discourse."[224] Singular cases, however, cannot be decided without recourse to specific rules derived from sovereignty that are accepted as valid under international law.[225] While sovereignty informs the interpretation of existing rules, I contend that it does not act as "a background principle that applies when specific rules do not exist," as recently argued by Nicholas Tsagourias.[226]

Such reliance on the putative direct normative force of the *principle* is also not necessary in the context at hand, as shown by the cases analyzed above. A number of primary rules can be derived, recognized by state practice and international jurisprudence,[227] whose object and purpose it is to protect certain aspects of sovereignty and that are of relevance for the legal qualification of adversarial cyber operations. These include, but are not limited to, the prohibition of the use of force and the principle of non-intervention.[228] As has been argued in this section, we can add "territorial sovereignty" to

219. CRAWFORD, *supra* note 167, at 432.

220. *See* KOSKENNIEMI, *supra* note 177, at 246 (describing what he calls the "legal approach to sovereignty" going back to HANS KELSEN, PRINCIPLES OF INTERNATIONAL LAW (1966), as opposed to the "pure fact approach" put forth by Carl Schmitt. CARL SCHMITT, POLITICAL THEOLOGY: FOUR CHAPTERS ON THE CONCEPT OF SOVEREIGNTY (1985)).

221. GEORG SCHWARZENBERGER & E.D. BROWN, A MANUAL OF INTERNATIONAL LAW 52 (6th ed. 1976).

222. *See* H.L.A. HART, THE CONCEPT OF LAW 218 (Oxford University Press 1961).

223. KOSKENNIEMI, *supra* note 177, at 255; *see* Besson, *supra* note 205, ¶ 116 ("Importantly, the existence of sovereignty rights and duties need not imply that sovereignty is reducible to them and to a bundle of rights.").

224. Werner, *supra* note 161, at 150–51.

225. *Id.*

226. Tsagourias, *supra* note 181; KOSKENNIEMI, *supra* note 177, at 255 (describing it as the "residual rule" of sovereignty).

227. Besson, *supra* note 205, ¶ 88.

228. *Id.* ¶ 126; *see* N.Z. FOREIGN AFFS. & TRADE, *supra* note 55, ¶ 11.

this list.[229] Territorial sovereignty may be broken down into its two main components, the primary rules of inviolability of territory and the prohibition for a state to exercise its power on the territory of another state. Furthermore, there is perhaps a nascent rule against state conduct interfering with another state's right to freely choose and develop its political, social, economic, and cultural systems that falls somewhere between permitted transnational political influence[230] and prohibited coercive intervention.[231] However, available practice does not yet warrant stipulating its precise legal status or content.

A criticism of the argument purported here could be that it is mere semantic nit-picking. Does it matter what we choose to call the rule(s)?[232] What is the actual difference between asserting that sovereignty is a rule and then attempting to determine its substance, as the Tallinn Manual has done and claiming that sovereignty is just a principle from which a number of specific primary rules follow that in combination cover a more or less identical protective scope? The difference is, first, that the conception proposed in this essay is doctrinally more precise by taking seriously the status of sovereignty as a state's "collection of rights,"[233] with corresponding duties for other states,[234] rather than one uniform rule. Second, this article has shown that sovereignty as an abstract general concept is politically and ideologically charged to a degree that renders it woefully inadequate to serve as a workable rule that is not constantly vulnerable to both authoritarian co-optation[235] and imperialist dismissal. That being said, to reiterate, it is certainly possible to frame "respect for sovereignty" as a primary rule of international law. Emerging state practice, catalyzed by the Tallinn Manual's pivotal contribution, suggests that a growing number of (European) states have taken this route. But it is questionable whether it is wise to do so. As a legal strategy aimed at clarifying the application of international law to cyberspace while safeguarding human rights guarantees online, such as freedom of information and freedom of expression, it might ultimately turn out to be a trap.

229. *See* Schöndorf, *supra* note 157, at 402; N.Z. FOREIGN AFFS. & TRADE, *supra* note 55, ¶¶ 11–12.

230. Damrosch, *supra* note 159, at 48–49.

231. N.Z. FOREIGN AFFS. & TRADE, *supra* note 55, ¶ 10 (advocating for reconceiving the understanding of "coercion" that captures a "prolonged and coordinated cyber disinformation operation").

232. *See* Spector, *supra* note 12, at 222.

233. CRAWFORD, *supra* note 167, at 431.

234. *See* Besson, *supra* note 205, ¶ 117.

235. *See* MOYNIHAN, *supra* note 16, ¶ 157.

C. Legal Implications I: "Persistent Engagement" and "Defend Forward"

Focusing on specific primary rules rather than a general "rule of sovereignty" allows us to better assess the international legal implications of national policies pursued under the imperialist and Westphalian approaches to cyberspace.

It was pointed out above that the strategy of "persistent engagement," with its related concept of "defend forward," proceeds from the assumption that cyber operations carried out under its umbrella do not breach the inviolability of another state's territory because the interconnectedness of cyberspace casts doubt on the entire notion of territoriality.[236] The rule could only come into play if the consequences of the operation cause considerable tangible effects on the target state's territory, such as physical damage or loss of functionality of infrastructure connected to cyberspace.[237] According to this view, it is implied that cyber conduct that merely "prepares the battlefield" by way of positioning activities that are "[i]ntrusions into the systems of potential adversaries in order to secure access of a kind that can be exploited for disruptive or destructive effect if and when the need later arises"[238] would not affect the adversarial states' territorial integrity.[239] Interestingly, this understanding quite closely resembles the view taken by the Tallinn Manual, despite the categorical differences concerning the rule-status of sovereignty.[240] And indeed, acknowledging the existence of a primary rule of territorial inviolability instead of sovereignty generally does not by itself prejudge the question of what kinds of cyber conduct would be in breach of the rule, as its scope can be read either expansively or restrictively.

On the other end of the spectrum, as described above,[241] are the voices who advocate for a broad understanding of the rule of territorial inviolability, asserting that there is in fact no evidence in either state practice or international jurisprudence for any kind of "threshold requirement," meaning that any unauthorized intrusion automatically violates the rule.[242] Among state

---

236. Fischerkeller & Harknett, *supra* note 53, at 269.

237. *See* Corn & Taylor, *supra* note 54, at 211 (calling consequences that remain limited to non-physical effects "cyber effects").

238. Robert Chesney, *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes*, LAWFARE (Sept. 25, 2018, 6:45 PM), https:// www.lawfareblog.com/ 2018- dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes.

239. Jeff Kosseff, *The Contours of 'Defend Forward' Under International Law*, *in* 2019 11TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: SILENT BATTLE 307, 313 (T. Minárik et al. eds., 2019).

240. TALLINN MANUAL 2.0, *supra* note 5, at 20–21.

241. *See supra* text accompanying note 139.

242. Roguski, *supra* note 17, at 73–80; DELERUE, *supra* note 16, at 215–19. Note that both authors use the notion of "territorial sovereignty" purportedly as part of a wider primary rule of sovereignty, and

actors, this interpretation is exemplified by France's official position.[243] According to this view, no persuasive reason exists to treat network infrastructures located on a state's territory in any way differently from its airspace or its territorial sea. Intrusions into networks or systems might be harder to detect than an aircraft crossing a border without authorization, but they nevertheless amount to territorial transgressions.[244] However, while it indeed seems difficult to reconcile the U.K.'s blanket contestation of a rule of territorial sovereignty with the *Rainbow Warrior* arbitration or the UN Security Council's condemnation of Israel's abduction of Adolf Eichmann on Argentinian territory,[245] it would overstate the case to assert that no contrary practice has been emerging at all. This would ignore recent declarations by states emphasizing the specific characteristics of "virtual" intrusions that call for an adjusted legal assessment.[246]

This raises the question whether the practice of "persistent engagement," absent the causation of physical effects on foreign territory, should be considered conduct that merely exploits the technical peculiarities of the "virtual," de-territorialized realm of cyberspace and thus falls outside the scope of the rule of territorial inviolability. Proponents of this view frequently liken the conduct to digital espionage, as these activities are ostensibly similar in both their techniques and objectives.[247] Espionage is in itself not addressed by international law, which implies that it is neither explicitly

---

that Roguski's argument is based on an analysis of the prohibition to exercise state power on foreign territory as a subcategory of territorial sovereignty. Despite these conceptual differences, the legal assessment in regard to offensive cyber operations that do not cause effects outside of cyberspace arrives at the same conclusion.

243. MINISTRY OF THE ARMIES, *supra* note 143, at 6.

244. *See* Tsagourias, *supra* note 181, at 6 ("Since a state can exercise its sovereignty over the physical, social, and logical components of cyberspace, any unauthorised interference by another state will constitute a violation of sovereignty.").

245. S.C. Res. 138 (June 23, 1960).

246. *See* Letter from Ministry of Foreign Affs. of the Neth., *supra* note 146, at 2 ("It should be noted in this regard that the precise boundaries of what is and is not permissible have yet to fully crystallise. This is due to the firmly territorial and physical connotations of the traditional concept of sovereignty . . . In cyberspace, the concepts of territoriality and physical tangibility are often less clear."); N.Z. FOREIGN AFFS. & TRADE, *supra* note 55, ¶ 13 ("In New Zealand's view, the application of the rule of territorial sovereignty in cyberspace must take into account some critical features that distinguish cyberspace from the physical realm. In particular . . . cyberspace contains a virtual element which has no clear territorial link . . . ."); Schöndorf, *supra* note 157, at 403 ("In practice, States occasionally do conduct cyber activities that transit through, and target, networks and computers located in other States, for example for national defense, cybersecurity, or law enforcement purposes. Under existing international law, it is not clear whether these types of actions are violations of the rule of territorial sovereignty, or perhaps that our understanding of territorial sovereignty in cyberspace is substantially different from its meaning in the physical world.").

247. *See* Ney, *supra* note 20.

permitted nor prohibited.[248] Irrespective of the legal status of espionage, however, the persuasiveness of the analogy is questionable. Military cyber activity inside foreign networks aimed at shortening reaction time by installing malware that can be triggered remotely at any time if desired is, if anything, more akin to a warship lingering in foreign territorial waters, which is a clear breach of the right to territorial inviolability of the coastal state in its *lex specialis* manifestation of the (customary) law of the sea.[249] Indeed, it is the result of a deliberate, metaphorical confusion to assume the existence of "high seas" in cyberspace and to equate "defend forward" operations with warships that "patrol the seas . . . to ensure they are positioned to defend our country before our borders are crossed."[250] The concept of "gray" and "red" zones as spatial dimensions detached from physical infrastructures is a military-strategic fiction not grounded in reality.

As explained above, a state's territorial sovereignty is not contingent upon complete and constant control of its virtual dimension.[251] Furthermore, to a much larger degree than mere espionage, offensive cyber conduct under the framework of "persistent engagement" potentially has a seriously destabilizing effect. For technical reasons, the actual purpose of such an operation will usually not be clear or even discernible from the perspective of an adversary whose networks are being breached, which obviously entails considerable risks of escalation. For all these reasons, the activity is not to be misunderstood as some sort of virtual freedom of navigation operation. The rule of territorial inviolability protects the physical and logical layers of a state's network infrastructures against intrusions for purposes such as "positioning" or "battlefield preparation." The strategy of "persistent engagement" is therefore incompatible with the obligations of the U.S. under international law.

D. Legal Implications II: "Cyber Sovereignty"

The same considerations do not apply to the content layer of network infrastructures. It has been shown above that the principle of sovereignty comprises a right, as stipulated in the Friendly Relations Declaration, for a

248. *But see* RUSSELL BUCHAN, CYBER ESPIONAGE AND INTERNATIONAL LAW (2018); Asaf Lubin, *The Liberty to Spy*, 61 HARV. INT'L L.J. 185 (2020) (explaining more granular and differentiated treatments of the question of the legality of espionage).

249. *See* United Nations Convention on the Law of the Sea arts. 17–19, Dec. 10, 1982, 1833 U.N.T.S. 397 (reflecting custom); *see* CRAWFORD, *supra* note 167, at 300–01.

250. Paul M. Nakasone, *A Cyber Force for Persistent Operations*, JOINT FORCE Q. (Feb. 2, 2019), https:// www.459arw.afrc.af.mil/ News/ Article- Display/ Article/1737519/a-cyber-force-for-persistent-operations/.

251. *See* Tsagourias, *supra* note 188, at 811; Tsagourias, *supra* note 181, at 6.

state to choose its own political, social, economic, and cultural systems.[252] This right is an expression of the constituent people's right to self-determination.[253] In the conception of the Declaration, it was thought to be protected mainly through the prohibition of coercive intervention.[254] This understanding has recently started to shift as digital technologies in the networked society have changed the ways in which states can interfere in each other's internal affairs. Foreign interference through digital means, as exemplified by Russia's attempts to influence the 2016 U.S. presidential election via social media, has cast doubt on the continuing efficacy of the principle of non-intervention. As a consequence, we may expect the slow emergence of a rule against the manipulative or covert interference in another state's decision-making processes. But whatever the current status and evolving content of this rule, most (democratic) proponents hasten to clarify that it cannot amount to a general prohibition of the free transmission of content across the global networks.

To be sure, the examples of China, Russia, Iran, and a number of other states that insist on a broad conception of "information security" and "cyber sovereignty" show that it would be wrong to deny the existence of any state practice whatsoever pointing in that direction. With this conception of sovereignty as a shield against any form of "outside interference," these states have remained consistent since the time of the Cold War.[255] But so far, there is no sufficiently uniform practice suggesting the gradual crystallization of such an expansive rule as derived from the principle of sovereignty.[256] Moreover, applicable human rights guarantees inherently limit a state's sovereign prerogatives[257] even if one is of the view that the status of rights such as the freedom of expression and freedom of information, enshrined in Article 19 of the Universal Declaration of Human Rights, is unsettled under customary international law.[258] Whatever the technical means the "Westphalian" actors

252. *See* Besson, *supra* note 205, ¶ 67.

253. *Id.*

254. *See* Dire Tladi, *The Duty Not to Intervene in Matters within Domestic Jurisdiction*, *in* THE UN FRIENDLY RELATIONS DECLARATION AT 50: AN ASSESSMENT OF THE FUNDAMENTAL PRINCIPLES OF INTERNATIONAL LAW 87, 90 (Jorge E. Viñuales ed., 2020).

255. G.A. Res. 36/103, annex II (Dec. 9, 1981).

256. *See* Henning Lahmann, *supra* note 218, at 209–17, for a detailed survey of recent practice.

257. *See* Croxton, *supra* note 97, at 575 (pointing out the fact that the rights of the individual had a limiting effect on a state's sovereignty was already implied in the Treaty of Westphalia).

258. Hurst Hannum, *The Status of the Universal Declaration of Human Rights in National and International Law*, 25 GA. J. INT'L & COMPAR. L. 287, 348 (1996). This problem exists mainly with regard to China, which has signed but not ratified the ICCPR and is thus not treaty-bound to respect these rights. However, according to Article 18 VCLT, China is still under the obligation "to refrain from acts which would defeat the object and purpose" of the Covenant. In 2009, China rejected recommendations made within the framework of the UN Human Rights Council Universal Periodic Review that would advance

implement to separate the content layer of their parts of cyberspace from the global networks in order to enforce their idea of "cyber sovereignty," there is no corresponding obligation derived from sovereignty for other states to refrain from disseminating information to these countries, or allowing their citizens to do so.

VI. CONCLUSION

Maximilian Bertamini recently observed that it is the irony of sovereignty that "it allows for fundamental differences between states, but cannot not be understood differently by them, if they want to have a meaningful conversation in international law."[259] The foregoing analysis has shown that this very much holds true with regard to the discourse on the legal status and substance of sovereignty in cyberspace. Following the Tallinn Manual's important contribution, the understanding of sovereignty as a primary rule of international law has had remarkable success in persuading European and other Western states. Outside this geographic context, where state representatives seem less familiar with the peculiarities of these debates,[260] the perception of sovereignty has remained more equivocal[261] or has been met with more skepticism and sometimes dismissed as a mere "distraction."[262] More significantly, powerful and active states in cyberspace are likely to find the interpretation more problematic. For different reasons, certain expressions of both the "imperialist" and the "Westphalian" approaches are incompatible with existing international law. However, the prevalent academic discourse that insists on the status of sovereignty as one uniform rule is incapable of clearly articulating the nuanced understanding that is necessary to expose the different politics and ideologies that shape the processes of norm clarification and development in cyberspace. Against this backdrop, this essay has proposed an alternative interpretation of the available evidence of practice that retains the traditional status of sovereignty as a principle and a "collection of rights," from which a number of primary rules follow.

---

freedom of expression and information. *See* HUMAN RIGHTS IN CHINA, COUNTER-TERRORISM AND HUMAN RIGHTS: THE IMPACT OF THE SHANGHAI COOPERATION ORGANIZATION 63 (2011), https://www.hrichina.org/ sites/default/files/publication_*pdfs/2011-hric-sco-whitepaper-full.pdf.*

259. Bertamini, *supra* note 164.

260. *See* Organization of American States, *Fourth Report*, *supra* note 153, ¶ 11.

261. *Id.* ¶¶ 50–55.

262. Organization of American States, *Fifth Report*, *supra* note 175, ¶ 45.