University of Reading

Sovereignty in cyberspace: lex lata vel non?

Article

Published Version

Creative Commons: Attribution 4.0 (CC-BY)

Open access

Schmitt, M. ORCID: https://orcid.org/0000-0002-7373-9557 and Vihul, L. (2017) Sovereignty in cyberspace: lex lata vel non? American Journal of International Law Unbound, 111. pp. 213-218. ISSN 2161-7953 doi: 10.1017/aju.2017.55 Available at https://centaur.reading.ac.uk/89705/

It is advisable to refer to the publisher's version if you intend to cite from the work. See Guidance on citing.

To link to this article DOI: http://dx.doi.org/10.1017/aju.2017.55

Publisher: Cambridge University Press

All outputs in CentAUR are protected by Intellectual Property Rights law, including copyright law. Copyright and IPR is retained by the creators or other copyright holders. Terms and conditions for use of this material are defined in the End User Agreement.

www.reading.ac.uk/centaur

CentAUR

Central Archive at the University of Reading

University of Reading

Reading's research outputs online

doi:10.1017/aju.2017.55

SYMPOSIUM ON SOVEREIGNTY, CYBERSPACE, AND TALLINN MANUAL 2.0

SOVEREIGNTY IN CYBERSPACE: *LEX LATA VEL NON*?

Michael N. Schmitt, and Liis Vihul†*

Globalization has not conquered sovereignty. Instead, the notion of sovereignty occupies center stage in discussions concerning the normative architecture of cyberspace. On the diplomatic level, the term is generally employed in its broadest sense, one that signifies freedom from external control and influence. For instance, when Western states raise the issue of human rights in cyberspace, those on the opposite side of the negotiating table fall back on sovereignty-based arguments. Mention of sovereignty in consensus documents is consequently often the price that liberal democracies pay to advance their policy priorities, such as individual freedoms and the availability of self-help measures in response to hostile cyber operations.

Unfettered by the constraints of political agendas and negotiating tactics, the international legal academy has tended to approach sovereignty from a normatively analytical perspective. For legal scholars, the question of how the principle of sovereignty, as well as its derivative rules, govern cyber activities by and against states has become a dominant topic on the research agenda. This essay assesses a recent controversy over whether sovereignty is a primary rule of international law, sets forth the authors' views on sovereignty violations in cyberspace, and highlights several resultant policy issues.

The Sovereignty Violation Controversy

Perhaps the most operationally relevant, and hence politically delicate, legal issue with respect to the cyber environment is the identification of criteria for determining when cyber operations directed against a state violate its sovereignty. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* examines the matter in the commentary accompanying Rule 4, "Violation of Sovereignty": "A State must not conduct cyber operations that violate the sovereignty of another State."[1] Viewed in the larger context of the international law that regulates states' cyber activities, the rule represents the most significant red line between lawful and internationally wrongful conduct. This place of prominence results from the fact that the other key[2] rules—the prohibitions on intervention

* *Professor of International Law, University of Exeter; Charles H. Stockton Professor, U.S. Naval War College; Francis Lieber Distinguished Scholar, United States Military Academy; Director,* Tallinn Manual 2.0 *Project. The views expressed are those of the author in his personal capacity.*

† *CEO, Cyber Law International; Managing Editor,* Tallinn Manual 2.0.

[1] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 17–27 (Michael N. Schmitt gen. ed., 2017) [hereinafter Tallinn Manual 2.0].

[2] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013 Report, para. 19, UN Doc. A/68/98* (June 24, 2013) [hereinafter UN GGE 2013 Report]; Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 Report, paras. 26, 28(b), UN Doc. A/70/174 (July 22, 2015) [hereinafter UN GGE 2015 Report].

The American Society of International Law and Michael N. Schmitt and Liis Vihul © 2017. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

and the use of force—contain thresholds that are seldom reached. Thus, the vast majority of hostile cyber operations attributable to states implicate only the prohibition of violation of sovereignty.

Yet, some states have hesitated to confirm the principle of sovereignty as one that prohibits certain types of cyber operations. This reluctance is tangible within the UN Group of Governmental Experts, the main state-level forum in which international law and cyber-related discussions take place.[3] Hesitant states appear to see the greater latitude to pursue national security objectives in cyberspace that derives from the absence of a primary rule of sovereignty as outweighing the likely costs of hostile cyber operations that might violate their sovereignty.

Against this background, it is understandable that the U.S. Department of Defense (DoD) appears troubled by the *Tallinn Manual 2.0*'s position on sovereignty. As the most cyber-capable nation in the world, the United States executes many of its cyber operations through the DoD. Greater clarity with respect to sovereignty in cyberspace might require the DoD either to exercise more restraint in its cyber operations or risk accusations of having violated international law if its operations came to light.

In this AJIL Unbound Symposium, Colonel Gary Corn and Robert Taylor, a current and former DoD senior attorney, respectively, suggest that the premise that sovereignty bars certain cyber activities even when they fall below the threshold of nonintervention is unfounded.[4] It is notable that, presumably to preserve the DoD's operational leeway, they have elected not to emphasize the substantial interpretive grey area that surrounds the prohibition of sovereignty violations, which the *Tallinn Manual 2.0* goes to great pains to highlight. They simply claim that the principle of sovereignty does not function as a primary rule.[5]

We challenge Corn's and Taylor's position in a forthcoming *Texas Law Review* article.[6] In our view, sovereignty operates to safeguard territorial integrity and inviolability; disregard for another state's territorial integrity and inviolability constitutes an internationally wrongful act. To support this assertion, we cite an array of examples of one state's conduct in another's territory that states, international tribunals, or the Security Council have characterized as violations of sovereignty, rather than intervention or a use of force. These include aerial trespass, unconsented-to activities in the territorial sea and on land, causation of radioactive pollution in national airspace, and the exercise of enforcement jurisdiction abroad.

Corn and Taylor appear to suggest that international law includes distinct prohibitions for each of these activities, but lacks analogous prohibitions for cyber operations. By our approach, the prevailing one in international law, sovereignty serves as the legal basis upon which the unlawfulness of these various forms of conduct rests. Although, as Corn and Taylor submit, the principle of sovereignty is the foundation for sovereignty-related rules such as nonintervention, this does not preclude the existence of a prohibition of the violation of sovereignty as such. To suggest otherwise would deprive the principle of most of its normative valence.

In fact, their objection to the legally binding nature of the principle of sovereignty is internally inconsistent. On the one hand, they assert that the principle does not bar cyber operations against other states, whereas on the other, they opine that it "should factor into the conduct of any cyber operation"[7] and that states engaging in cyber activities "must consider the sovereignty of the states in whose territory these [cyber] infrastructures reside."[8] The question of whether the principle of sovereignty protects, as a matter of international law, a state from certain cyber activities of other states is a binary one—it either does or does not. If the principle requires states to consider

[3] See the cautious approach taken in UN GGE 2013 Report, *supra* note 2, at paras. 20, 27.

[4] Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL Unbound 207, 208–209 (2017).

[5] *Id.* at 209.

[6] Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 Tex. L. Rev. 1639 (2017).

[7] Corn & Taylor, *supra* note 4, at 210.

[8] *Id.* at 210.

the sovereignty of other states when conducting cyber operations, as Corn and Taylor (correctly) suggest, the matter is necessarily resolved in the affirmative.

Those who dispute sovereignty's status as a primary rule would do well to recall that the ICJ has addressed violations of sovereignty on multiple occasions. Although acknowledging a few of these judgments, Corn and Taylor opine that since some of the activities concerned also amounted to uses of force and intervention, they constituted violations of sovereignty and territorial integrity "in the broader sense."[9] This begs the question of why the Court would explicitly refer to a violation of sovereignty, as distinct from the other two prohibitions, when the function of the Court is to assess whether the conduct before it amounted to specific internationally wrongful acts.[10] Corn and Taylor also seem to turn a blind eye to the fact that in *Corfu Channel* and *Certain Activities*, two of the three judgments they cite, the Court concluded, respectively, that the minesweeping operation in Albania's territorial sea[11] and excavation of the channels and establishment of a military presence on Costa Rican territory[12] only constituted violations of sovereignty, not unlawful interventions or uses of force. If it sufficed for the Court to render judgment in those cases on the grounds of sovereignty violations, no conclusion can be drawn other than that the principle of sovereignty operates as a primary rule of international law.[13]

The Threshold for Sovereignty Violations in Cyberspace

The question is which cyber operations, especially those mounted from outside the target state's territory, fall within the protective scope of the principle. In *Tallinn Manual 2.0*, we, together with the seventeen other members of the so-called "International Group of Experts," found that violations of sovereignty could be based on two different grounds: "(1) the degree of infringement upon the target state's territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions."[14]

The former is premised on the integrity and inviolability of sovereign territory. The dilemma lay in determining which cyber operations infringe these rights. Complicating our assessment were the myriad ways in which cyber operations manifest themselves in a target state—they can entail anything from the simple scanning of ports to causing physical effects akin to those of kinetic military operations. A plethora of consequences fall between these extremes, such as the extraction of information that possesses intelligence value, disrupting e-commerce activities, or wiping data from systems on which critical services are run.

Because violations of sovereignty in the non-cyber context typically have entailed physical acts in other states' territory, the *Tallinn Manual 2.0* group reasoned by analogy that remote cyber operations producing physical consequences likewise qualify. This conclusion is in line with the object and purpose of the principle of sovereignty.[15] We also agreed that a violation of sovereignty occurs when the restoration of functionality following a hostile cyber operation requires physical repair, such as the replacement of hard drives. Whether a server park, for instance, is physically destroyed or its systems are permanently compromised by remote means, the ensuing effects

[9] *Id.* at 210 n. 14.

[10] Statute of the International Court of Justice, art. 38(1), June 26, 1945, 33 UNTS 993.

[11] Corfu Channel (U.K. v. Alb.), Merits, 1949 ICJ Rep. 4, 35 (Apr. 9).

[12] 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 (Costa Rica v. Nicar.), para. 229 (Dec. 16, 2015).

[13] Indeed, in the case between Costa Rica and Nicaragua, the Court decided not to assess the use of force issue, noting, the "relevant conduct of Nicaragua has already been addressed in the context of the Court's examination of the violation of Costa Rica's territorial sovereignty." *Id.* at paras. 96–97.

[14] Tallinn Manual 2.0, *supra* note 1, rule 4, cmt. para. 10.

[15] *Id.*, rule 4, cmt. para. 11.

are the same—the server park no longer fulfils its intended role. As to less severe effects on functionality, the experts' views varied.[16]

Whereas state practice and jurisprudence regarding sovereignty violations, including that discussed in our other work,[17] tends to be premised on territorial integrity and inviolability, the International Group of Experts further concluded that it was apposite to view the exercise of a state's inherently governmental functions as protected by sovereignty.[18] The *Tallinn Manual 2.0* cites the *Island of Palmas* arbitral award, which sets forth the authoritative articulation of the crux of sovereignty. There, the distinguished arbiter Max Huber observed, "[s]overeignty in the relations between states signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[19] It was the group's unanimous view that a state violates the sovereignty of another state when it, by means of cyber operations, interferes with or usurps functions that lie at the heart of the other's independence. If sovereignty grants states the exclusive right to exercise state functions, other states necessarily shoulder a corresponding duty to respect that right.

Indeed, cyber operations that breach territorial integrity and inviolability may pose less of a national security threat than those that impede the exercise of inherently governmental functions. For instance, the damage done to Sony Pictures Entertainment's computer systems in 2014 by cyber operations,[20] provided they were attributable to a state, amounted to a violation of U.S. sovereignty due to the infringement on territorial integrity and inviolability. However, such an operation represents less of a national security concern than one that, for instance, "interferes with the delivery of social services, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, [or] the performance of key national defence activities."[21]

Policy Considerations

Corn and Taylor opine that the troubling aspect of the assertion that cyber operations can violate the principle of sovereignty is that the rule would supposedly deprive states of the ability to undertake cyber operations required to disrupt terrorist cyber infrastructure and engage in essential cyber espionage.[22] With regard to countering the online activities of terrorist groups such as ISIS, the two observe that it is sometimes operationally necessary to direct cyber operations against infrastructure that is used by the groups, but is located beyond the area in which hostilities are being conducted. They fear that in these situations the principle of sovereignty could preclude the state from engaging in necessary operations. But whether this is the case depends on the specific nature of the cyber operations in question, the target territory, and other attendant circumstances.

The *Tallinn Manual 2.0* does not offer definitive guidance on whether cyber operations that target terrorist organizations' social media accounts, online fora, recruiting and propaganda websites, or other online resources that are hosted on infrastructure located abroad and beyond the geographic scope of armed conflict violate sovereignty under the territorial integrity and inviolability test. Sensitive to the unsettled nature of international law on this matter, the relevant text in the *Tallinn Manual 2.0* is intentionally laconic. To the extent that the cyber operations Corn and Taylor describe neither cause physical damage to, nor a loss of functionality of, the targeted cyber

[16] *Id.* at paras. 13–14.

[17] Schmitt & Vihul, *supra* note 6.

[18] Tallinn Manual 2.0, *supra* note 1, rule 4, cmt. paras. 10, 15–20.

[19] Island of Palmas (Neth. v. U.S.), 2 R.I.A.A 829, 838 (Perm. Ct. Arb. 1928).

[20] The cyber operation targeting Sony "resulted in the destruction of about three-quarters of the computers and servers at the studio's main operations." David E. Sanger & Michael S. Schmidt, *More Sanctions on North Korea After Sony Case*, N.Y. Times (Jan. 2, 2015).

[21] Tallinn Manual 2.0, *supra* note 1, rule 4, cmt. para. 16.

[22] Corn & Taylor, *supra* note 4, at 211.

infrastructure, the state conducting those operations may have a reasonable argument that such digital penetrations of foreign territory are not in breach of territorial integrity and inviolability. The Manual purposefully leaves it to states, through practice and *opinio juris*, to clarify the interpretation of a sovereignty violation in the cyber context.

International law considerations aside, it is doubtful that a state knowing of such operations directed at its territory would tolerate them from a policy perspective. Of course, to the extent a territorial state remains unaware of cyber operations, the state conducting them risks no legal or political consequences. The latter must, however, be cognizant of the reality that if detected, adverse political reactions could ensue (which would be the case irrespective of the permissibility of the operations under international law).

Political blowback is an especially acute risk for the United States. Still reeling from the reputational damage caused by the Wikileaks and Snowden revelations, disclosure of further covert operations would likely trigger stronger reactions than the discovery of comparable cyber operations conducted by many other states. U.S. operations might well be characterized in the political or legal sense as an abuse of its technological supremacy by acting in disregard of other states' sovereignty. This could lead to further "Westphalianization" of the internet, as well as increased data localization, which runs counter to the long-term U.S. policy objective of the free flow of information.

An additional worrisome element in Corn and Taylor's reasoning is their singling out of terrorists' online activities as justifying a legal green light for cyber operations abroad. While fighting terrorist groups like ISIS is a laudable policy objective from both a domestic and international security perspective, the principle of sovereign equality means that such a justification will be equally available to all other states. Thus, the proposition that cyber operations on foreign soil are permissible if undertaken to counter terrorist activities, which is what Corn and Taylor seem to imply,[23] could open the door to other states' cyber operations against U.S. cyber infrastructure, for understandings of what the term "terrorism" denotes differ dramatically. For example, China's 2015 counterterrorism legislation provides an open-ended definition of terrorism that could extend to nonviolent dissident activities and certain exercises of speech.[24] If the United States justifies unilateral actions in foreign cyber infrastructure on the basis of counterterrorism, it is reasonable to assume that other states will feel entitled to do the same, and may use expansive definitions in doing so. Corn's and Taylor's caveat that they are referring to terrorists or terrorist organizations that are "widely recognized as such"[25] begs the question of the legal basis for this qualifier, while offering little solace from a practical perspective.

Corn and Taylor also appear to be uneasy with treating a state's territory as inviolable out of concern that it would render espionage activities that are physically conducted on foreign territory as a violation of sovereignty. But, as discussed above and contrary to their assertion, territorial integrity and inviolability are firmly grounded in international law; the primary rule prohibiting the violation of sovereignty accordingly has long been *lex lata*. For espionage conducted on another state's territory to be lawful, it would have to constitute a customary exception to the general principle of territorial integrity and inviolability. While extensive state practice offers support for this proposition, the lack of *opinio juris* cuts the other way. As Quincy Wright opined in 1962, the "frequent practice has not established a rule of law because the practice is accompanied not by a sense of right but by a sense of wrong."[26] Indeed, if contrary state practice alone sufficed in the abstract to undercut a customary norm, both the prohibitions on intervention and the use of force would be at risk.

[23] *Id.* at 210, 212.

[24] Zunyou Zhou, *China's Comprehensive Counter-Terrorism Law*, The Diplomat (Jan. 23, 2016).

[25] Corn & Taylor, *supra* note 4, at 211.

[26] Quincy Wright, *Espionage and the Doctrine of Non-Intervention in International Affairs*, *in* Essays on Espionage and International Law 3, 17 (Roland J. Stanger ed., 1962).

Of course, we are sensitive to the fact that states generally act pragmatically in their international relations. Most have an interest in engaging in espionage, although conversely they do not tolerate espionage on their own territory, as evidenced by its universal criminalization in domestic law. The situation is inherently paradoxical—states proscribe the very conduct in which their own agents engage. It is accordingly rational that international law does not prohibit espionage per se, since it is so prevalent, but rather only certain methods by which it is conducted.[27]

Remote cyber espionage represents a less severe incursion into another state's sovereign territory and therefore is less likely to be characterized as a violation of territorial integrity and inviolability. The question is not whether remote cyber operations violate sovereignty; they do not as such. Rather, the correct query is whether the method employed to conduct the espionage, and the resulting effects, render the operation unlawful, as in the case of causing physical damage to cover one's cyber tracks. This approach affords sufficient international law leeway for states to engage in much of the espionage that Corn and Taylor deem necessary to safeguard national security.

Conclusion

On its face, the principle of sovereignty appears to be incompatible with cyberspace. Whereas sovereignty is an inherently territorial concept, cyberspace connects states in ways that seem to dilute territoriality. Nevertheless, the two phenomena have continued to exist in parallel since the emergence of cyber capabilities.

Considering their uneasy coexistence, states and the broader international community have sought to delicately balance the notions of a free flow of information in cyberspace with a state's sovereign control over cyber activities occurring within its territory. Of concern is the fact that an increasing number of states are resorting to rhetoric and practice that seems to strongly favor sovereignty over a free and open cyberspace.[28] For liberal democracies, it is imperative to counter this trend.

What Corn and Taylor suggest, however, takes the principled Western opposition to sovereignty too far. The legally binding nature of the principle of sovereignty cannot be wished away for operational reasons. They have exaggerated the risks posed by the rule prohibiting violations of sovereignty. Rather than decry the existence of such a rule, the United States and other states would be better served by working together to carefully map its parameters. Doing so would enhance the protection that the law affords U.S. cyber infrastructure and activities.

Lastly, we must be realistic. States, whether they are allies of the United States or not, whether they know of the purported U.S. counterterrorist operations occurring on cyber infrastructure located on their territory or not, and whether they are cyber capable or not, are unlikely to tolerate foreign cyber operations on their territory. Given U.S. technological supremacy and the fact that territorial states are often oblivious to effects manifesting on their cyber infrastructure, it may seem sensible to refuse to acknowledge the normative firewall that sovereignty represents. But in the long term, this approach is bound to backfire, with political damage potentially outweighing what can be gained from such cyber operations. Advocates of the approach will inevitably learn that sovereignty-violating cyber operations can only be pursued as a measure of last resort and with full knowledge of the likely reactions.

[27] Tallinn Manual 2.0, *supra* note 1, rule 32.

[28] *See, e.g.*, China, Ministry of Foreign Affairs, International Strategy of Cooperation on Cyberspace (Mar. 1, 2017) (English translation). The strategy lists sovereignty as one of the four basic principles of international cooperation in cyberspace.