doi:10.1017/aju.2017.77

CONCLUDING OBSERVATIONS ON SOVEREIGNTY IN CYBERSPACE

Gary P. Corn and Robert Taylor†*

In *Sovereignty in Cyberspace:* Lex Lata Vel Non?, Michael Schmitt and Liis Vihul argue that territorial sovereignty is a primary rule of international law that limits cyber activities.[1] They recognize, however, that not all cyber effects constitute violations of territorial sovereignty, and like Rule 4 in the *Tallinn Manual 2.0* and its commentary, they acknowledge a distinct lack of consensus among the Tallinn participants on the critical question of applicable thresholds. Problematically, they do not identify the necessary state practice and *opinio juris* that would be required to establish either the primary rule that they proffer or the existence and contours of the exception they would recognize.

Schmitt and Vihul, as well as Phil Spector,[2] look to sources dealing with very different domains and very different kinds of activities, and attempt to divine a rule where we see an absence of binding law. In this regard, it is telling that at no point has the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), the only international body to date charged with the task of examining how international law applies to cyber operations by states, identified sovereignty as a primary rule of international law that would, absent a justification, bar some or any nonconsensual cyber operations below the threshold of a prohibited intervention within the territory or on the infrastructure of another state. On the contrary, before backtracking and failing to reach a consensus report in 2017 on the applicability of international law to cyber operations *vel non*, the 2015 UNGGE adopted "general and declaratory" language that "[state sovereignty] *and international norms and principles that flow from sovereignty* apply to the conduct by States of [information and communications technologies]-related activities," a position fully consonant with the preponderance of sources cited in Phil Spector's essay.[3] The 2015 UNGGE then went on to adopt a number of nonbinding, voluntary peacetime norms, many if not all of which would be superfluous if sovereignty were the primary rule that Schmitt, Vihul, and Spector assert it is.

Outside of the clearly established primary rules against the use of armed force and against unlawful intervention, it remains for states to consider the demarcation between what is lawful and what is not. How traditional principles and extant rules of international law apply to the emerging cyberspace domain are critical questions requiring the work and attention of the international community. That work must take into account the unique nature of cyberspace, as well as the foundational principle of respect for a nation's sovereign authority, without sliding into the overly simplistic position that any prejudicial action in another state's territory constitutes a breach of international

* *Staff Judge Advocate, United States Cyber Command.*

† *Visiting Scholar, Harvard Law School Spring Term 2017, Former Principal Deputy General Counsel, Department of Defense. The views expressed are those of the authors and do not necessarily reflect the views of the United States Cyber Command, the Department of Defense, or the U.S. Government. Authors are listed in alphabetical order.*

[1] Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace:* Lex Lata Vel Non?, 111 AJIL Unbound 213 (2017).

[2] Phil Spector, *In Defense of Sovereignty in the Wake of Tallinn 2.0*, 111 AJIL Unbound 219 (2017).

[3] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 Report para. 27, UN Doc. A/70/174 (July 22, 2015) (emphasis added).

The American Society of International Law and Gary P. Corn and Robert Taylor © 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.

https://doi.org/10.1017/aju.2017.77 Published online by Cambridge University Press

law whenever those actions might violate that state's domestic law. It also must take into account the need of states to effectively defend against actors—state, nonstate, and hybrid actors—intent on causing harm from outside the borders of the defending state.

https://doi.org/10.1017/aju.2017.77 Published online by Cambridge University Press