doi:10.1017/aju.2017.58

INTRODUCTION TO SYMPOSIUM ON SOVEREIGNTY, CYBERSPACE, AND TALLINN MANUAL 2.0

*Tom Ginsburg**

In February 2017, a group of nineteen scholars, working as the International Group of Experts under the auspices of NATO's Cooperative Cyber Defense Centre of Excellence, released *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.[1] This followed Tallinn 1.0, released in 2013, which had focused more narrowly on the law of armed conflict and the question of cyber warfare. Tallinn 2.0 extends the project by grappling with cyber activities that do not rise to the level of the use of force or intervention, thresholds that trigger well-known bodies of international law.

This AJIL Unbound Symposium features contributions that address some of the major questions raised by the Manual, with a focus on the role of sovereignty. Just as cyberspace poses fundamental challenges to the territorial conception of the world order, so it also raises profound and interesting questions about core international legal concepts. It thus is of great interest to scholars and legal advisors alike.

Our symposium begins with *Gary Corn and Robert Taylor*, who have served as lawyers for the United States Department of Defense.[2] They take on the concept of sovereignty as applied by Tallinn 2.0 to cyber activities. Rule 4 of the Manual provides that states "must not conduct cyber operations that violate the sovereignty of another State." Corn and Taylor emphasize that sovereignty is a principle of international law, but view it as one that only informs primary rules of conduct, rather than itself operating as a binding rule.

Michael Schmitt, a Professor of Public International Law at Exeter Law School and head of the Group of Experts, contributes a piece co-authored with Liis Vihul of the NATO Centre, who served as Managing Editor on the *Tallinn 2.0* project.[3] They contest Corn and Taylor's vision of sovereignty as only serving as a principle, and demonstrate how and why the Tallinn Working Group considered it to be more operational, particularly in the cyber context.

In the third contribution to the symposium, *Phil Spector*, another member of the Tallinn Group of Experts, interrogates the doctrinal basis for the claim that sovereignty is a binding principle of international law.[4] This is one of the chief axes of disagreement between Corn and Taylor on the one hand and Schmitt and Vihul on the other. Surveying international law treatises and the decisions of international tribunals, he argues that there is ample evidence to assert that sovereignty is in fact a binding rule. He further argues that the rule covers actions that fall below the threshold that triggers the law of armed conflict, defending the position of the Manual.

Ahmed Ghappour, an Associate Professor at Boston University School of Law, calls on states to be more transparent with their views of the law, which might contribute to the further development of international

* *Leo Spitz Professor of International Law, Ludwig and Hilde Wolf Research Scholar, and Professor of Political Science, University of Chicago Law School, AJIL Board of Editors.*

[1] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt gen. ed., 2017).

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

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

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

custom.[5] He notes that the difficulties of attribution in the cyber context raise particular difficulties. A collateral consequence of states' preference for secrecy and deniability in their own operations is the relative lack of public pronouncements when incidents do occur. States may also have genuine difficulty articulating standards that protect their domestic cyber infrastructure while allowing them to engage in their own cyber operations abroad. But, Ghappour argues, these patterns are based on incomplete assumptions about the scope of cyber activities, and there are opportunities for greater cooperation. He notes that states have common interests in hacking techniques used in law enforcement, which in an era of greater transboundary criminal activity could create more jurisdictional conflicts if left without a legal framework. He lays out some of the ways in which law enforcement might motivate states to produce standards in this area.

Altogether, the Tallinn 2.0 Manual reflects a careful effort to move international law forward in the challenging domain of cyberspace. This Symposium presents a debate that challenges us to continue thinking about these issues, but also raises more fundamental questions about the nature of principles and rules in international law, and the manner in which rules of customary international law are articulated.

[5] Ahmed Ghappour, *Tallinn, Hacking, and Customary International Law*, 111 AJIL UNBOUND 224 (2017).

https://doi.org/10.1017/aju.2017.58 Published online by Cambridge University Press