doi:10.1017/aju.2019.9

SYMPOSIUM ON DAN EFRONY & YUVAL SHANY, A RULE BOOK ON THE SHELF? TALLINN MANUAL 2.0 ON CYBEROPERATIONS AND SUBSEQUENT STATE PRACTICE

THE SLOW PROCESS OF NORMATIVIZING CYBERSPACE

*Nicholas Tsagourias**

In their article, Dan Efrony and Yuval Shany claim that post-Tallinn Manual practice demonstrates that states entertain doubts about the applicability to cyberspace of the rules contained in the Tallinn Manuals. According to the authors, post-Tallinn practice reveals that states treat the application of international law to cyber operations as optional; operate in parallel—legal and nonlegal—tracks of conduct; and engage in gradated enforcement. They also claim that their study invites further research into the implications of state conduct in cyberspace for general international law theory.[1] I will use this last point as a springboard to explain the process of normativization in cyberspace—that is, the process of subjecting states' cyber operations and behaviors to legal standards.[2] To do this, I will use Oscar Schachter's representation of a normative (legal) order as a three-story building. According to Schachter's metaphor, the third floor is occupied by public values and general policy aspirations; the second floor is occupied by law with its distinctive normative patterns of prescribing, proscribing, and applying; while the ground floor is occupied by the social reality of conduct.[3] The three floors are not isolated but connected by escalators and staircases that go in both directions.

On the basis of Schachter's metaphor, I will argue that the normativization process in cyberspace is iterative and multidimensional and that, currently, the ground and third floors of the putative cyber legal order are populated while the second floor of rules is under construction. I will also argue that the Tallinn Manuals are important but not central to this process because the normativization of cyberspace is controlled by states as the primary juris-generative actors in international law.

The Normativization of Cyberspace: Norms, Principles, Rules, and Practice

States do not treat cyberspace as existing in a normative vacuum but rather as having a putative normative (legal) order. Declarations to the effect that international law applies to cyberspace are too numerous to require specific recounting.[4] Such statements are, however, like an architect's plan for a house—and states are indeed the primary

* *Professor of International Law, University of Sheffield.*

[1] Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AJIL 596, 647 (2018).

[2] For a process-centered approach to norm creation in cyberspace, see Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AJIL 425 (2016).

[3] Oscar Schachter, *Towards a Theory of International Obligation*, *in* THE EFFECTIVENESS OF INTERNATIONAL DECISIONS 9–31 (Stephen M. Schwebel ed., 1971).

[4] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, paras. 19-20, UN Doc. A/68/98* (June 24, 2013) [hereinafter UN GGE 2013 Report]; United Kingdom, The

The American Society of International Law and Nicholas Tsagourias © 2019. 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.2019.9 Published online by Cambridge University Press

architects of international law—but the critical question is how a concrete cyber legal order can be created out of this plan. That process of construction is the focus of this essay.

The Tallinn Manuals set the scene by laying out the international law rules that apply to cyberspace. Their central premise is that they present the law as it is and not as it "ought" to be.[5] The Manuals are the work of independent experts and can be contrasted in that regard with the reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), an intergovernmental process operating under the UN umbrella.[6] The GGE reports lay down binding as well as nonbinding rules, norms, and principles that apply or should apply to cyberspace. For example, the 2015 GGE Report (adopted by consensus) listed eleven voluntary and nonbinding norms, rules, and principles of responsible state behavior aimed at promoting an Information and Communication Technology (ICT) environment that is open, secure, stable, accessible, and peaceful. It also affirmed that international law, in particular the UN Charter, applies to cyberspace, along with the principle of state sovereignty and the international norms and principles that flow from it (such as sovereign equality and the principle of nonintervention).[7] For their part, Efrony and Shany speak of norms, although it seems that they actually mean rules. In light of these different formulations, it is important to clarify the concept of "norms," "principles," and "rules."[8]

A norm is a deontic proposition that not only guides behavior, but also forms the basis for evaluating behavior. As the 2015 GGE Report put it, norms "reflect the international community's expectations, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States."[9] Norms are also consequential, although there are degrees of consequentiality when one moves from the general to the specific. Norms can be divided into principles and rules. In Schachter's metaphor, norms as principles are located in the third floor, while norms as rules inhabit the second floor.

The Third Floor: Principles and the Normativization Process in Cyberspace

Principles are general propositions containing standards and objectives that not only provide guidance, but also determine, operationalize, and constrain social interactions. In this sense, principles are essentially political, but when they become part of a legal order, they acquire legal standing and endow the standards and objectives of the constructed order with legal force. Principles are divided into deontological principles (which set out aggregate standards and objectives) and structural principles (which contain the coordinating standards and processes for realizing the former).

When it comes to the normative structure of cyberspace, states have promulgated its referent principles and hence populated the third floor. The GGE reports are indicative in this respect. They set out the standards

National Cyber Security Strategy 2016 to 2021, para. 8.2 (Nov. 1, 2016); The National Cyber Security Strategy of the United States of America 20 (Sept. 2018).

[5] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 3 (Michael N. Schmitt ed., 2017).

[6] The GGE has not been a technical exercise. In almost all cases, these experts are government officials; the presence of legal advisers is common, and the process often involves diplomatic negotiations. The General Assembly mandates also placed the work of the GGE squarely in the realm of international security and disarmament. *See* Digital Watch Observatory, UN GGE.

[7] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 13, UN Doc. A/70/174 (July 22, 2015) [hereinafter UN GGE 2015 Report]; *see also* UN GGE 2013 Report, *supra* note 4, paras. 19–20.

[8] *See* Ronald Dworkin, Taking Rights Seriously, chs. 2 and 3 (1978); Frederick Schauer, Playing by the Rules, ch. 1 (1971); Joseph Raz, *Legal Principles and the Limits of Law*, 81 Yale L.J. 823 (1972).

[9] UN GGE 2015 Report, *supra* note 7, para. 10.

https://doi.org/10.1017/aju.2019.9 Published online by Cambridge University Press

and goals of the cyber order (the promotion of an open, secure, stable, accessible, and peaceful ICT environment) and lay down the structural principles that will assist in attaining those standards, such as the principles of sovereignty, nonintervention, and sovereign equality. Beyond the GGE framework, states have also confirmed the application of these principles to cyberspace in their cyber strategies, in international fora, and in bilateral and multilateral settings.[10]

Principles can give rise to rules. Rules are specific proscriptions or prescriptions that individuate particular aspects of a referent principle. Rules are monodimensional in the sense that, to use Dworkin's expression, they apply in an "all-or-nothing fashion." They also enjoy direct and immediate normative consequentiality, whereas the normative consequentiality of principles is gradated depending on interpretation and specification. This is completely different from saying that principles lack normative force because of their generality. As a matter of fact, the International Court of Justice has ascribed legal consequences to both principles and rules and often treated them interchangeably.[11]

This normative mapping helps illuminate the current debate on the normative force of the principle of sovereignty in cyberspace.[12] Some contend that sovereignty as a principle cannot produce legal consequences unless it is dissected into specific rules (as with the rule on the nonuse of force), while others claim that sovereignty can itself produce legal consequences. On the basis of the foregoing, I submit that the principle of sovereignty produces legal consequences, which international jurisprudence also confirms.[13] Unlike a rule, however, sovereignty as a principle is more general and applies across different areas, with its content and normative force being subject to interpretation and further specification. The crux of the matter, then, is to identify which aspects of the principle of sovereignty are legally consequential in cyberspace and, above all, how the principle of sovereignty is mapped out in cyberspace. For example, in addition to the nonuse of force and nonintervention, which protect specific aspects of the principle of sovereignty, is cyber interference into a state's political authority—another domain protected by the principle of sovereignty—legally consequential?[14]

The Second and Ground Floor: Rules, Practice and the Normativization Process in Cyberspace

I will now consider what happens in the second and ground floor and what this reveals about the construction of the cyber legal order. According to Efrony and Shany, the ground floor is currently populated with state practice, whereas the second floor is not populated by rules. I agree with the former, but I am more sanguine about the latter. To explain, the ground floor is populated by states' actions, reactions and inactions, name-calling, initiatives, claims, counterclaims, and the like. Beyond this external state conduct, there is also internal conduct in the form of cyber strategies, legislation, and indictments. This shows that states are in the process of translating overbroad

[10] *See, e.g.*, Shanghai Cooperation Organisation, Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security art. 4(1), June 16, 2009; Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to The Secretary-General, UN Doc. A/69/723 (Jan. 13, 2015).

[11] *See* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Merits, 1986 ICJ Rep. 14, paras. 202, 205 (June 27); Delimitation of Maritime Boundary in Gulf of Maine Area (Can. v. U.S.), 1984 ICJ Rep. 246, para. 79 (Jan. 20).

[12] *Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0*, 111 AJIL Unbound (2017).

[13] *See, e.g.*, Corfu Channel (U.K. v. Alb.), Merits, 1949 ICJ Rep. 4, 35 (Apr. 9); 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.), 2015 ICJ Rep. 665, para. 229 (Dec. 16).

[14] One example of aligning existing norms to cyberspace is the treatment of cyber interference with the electoral infrastructure as a violation of the nonintervention norm. *See* UK Attorney General's Office, Cyber and International Law in the 21st Century.

https://doi.org/10.1017/aju.2019.9 Published online by Cambridge University Press

principles into rules and practice and in translating practice into rules and principles. Efrony and Shany actually point to recent developments where states individually or collectively appear to be more forthcoming in translating the content and scope of norms and in evaluating state behavior against those norms. For them, such developments reveal "communicative and norm-consolidation" tendencies.[15]

This process of norm translation, which will eventually lead to the crystallization and consolidation of rules in the second floor, can nonetheless be quite slow. States must weigh interests and options, consider how existing international rules can be applied in the cyber domain, and evaluate the practical implications of any normative commitment. Yet, as Efrony and Shany acknowledge, this state of affairs is not peculiar to cyberspace, as the law of development and environmental law demonstrate. In this regard, there is no reason to despair.

In the process of norm translation, international lawyers—including those who do not work for governments—can play an important role.[16] The experts who promulgated the Tallinn Manuals offer an inventory of rules that apply to cyberspace, explaining their content and how they apply to this new environment. But experts do not produce international law. The main reason why states are not responsive to the Tallinn rules is because, as the primary normative engines of international law, they refuse to delegate this function fully to others, even if those other actors may influence states' thinking and actions. Even if states were to accept or enforce the Tallinn rules at some point in the future, it would not be directly or explicitly. Any suggestion that the Manuals will be employed "lock, stock, and barrel" is misplaced because states have an institutional as well as a vested interest in controlling the process of norm-building, rule specification, and rule application. Whereas the Manuals can be part of the normativizing process, they are not themselves the normativizing process.

It is also in the context of the current process of norm translation that optionality and gradated enforcement—identified by Efrony and Shany as indicators of cyber's lack of normativity—need to be considered. Optionality is part and parcel of international law's structural DNA; whether states will claim that a violation of international law occurred and take countermeasures depends on many factors, primarily political ones. There is no automaticity as far as the application and enforcement of international law is concerned because states are at the same time law creators, interpreters, and enforcers. This state of affairs also explains the gradation in enforcement and the resort to measures of retorsion noted by Efrony and Shany. Although I concur with the authors that retorsion fudges the question of illegality, retorsion is an international law instrument of approbation which is legally consequential in the sense of attempting to induce compliance, deter conduct, or punish a wrongdoing state. Hence—and contrary to what the authors say[17]—states are operating within the four corners of the putative cyber legal order while trying at the same time to reduce the normative silences, uncertainties, ambiguities, and gradations that still exist. To put this slightly differently, the normative pendulum in cyberspace swings from generality to particularity with a lot of bumps in the process.

In sum, states have identified the referent principles of the putative cyber legal order and are engaging in conduct, but they are still determining the content and scope of the applicable rules. This state of affairs is confirmed by the failure of the 2017 GGE to produce a report. The failure was due to differences of opinion on the applicability or on the content of certain rules in cyberspace, but the disagreement did not extend to all rules or to the principles included in the 2015 GGE Report. In fact, the intervening GGE Reports show how normativization has gained momentum since the first GGE, where, according to the Russian Representative, "even with the use of

[15] *See* Efrony & Shany, *supra* note 1, at 649.

[16] *See id.* at 648.

[17] *Id.* at 649.

https://doi.org/10.1017/aju.2019.9 Published online by Cambridge University Press

translation, the members … spoke different languages with respect to essential issues related to international information security" because of different approaches to key concepts and to the applicable law.[18]

Where Do We Go from Here?

Rule consolidation will take place gradually and slowly when states' interests and preferences coalesce around issues, forms, and procedures. In fact, as Efrony and Shany note, consensus is already emerging in outlawing certain cyber operations, as for example operations on critical national infrastructure, and such consensus can gradually extend to other issues. As Efrony and Shany also opine, certain nonbinding norms endorsed in the 2015 GGE Report or in other instruments can gradually attain customary law status. At this juncture, rule consolidation cannot take the form of an international agreement but may be pursued through the United Nations—either through the GGE process or through other processes within the General Assembly or the Security Council[19]—or through bilateral or multilateral processes.[20] Regional institutions such as the European Union can facilitate quicker norm consolidation by bringing together like-minded states.[21] This shows that states have a number of options when engaging in rule consolidation, and it is for states to decide whether to pursue a comprehensive agenda or a more defined agenda of rule consolidation. That said, it should not be forgotten that the normativization process cannot be decoupled from the attitudes of those states most actively involved in cyber operations.

[18] UNGA, Sixtieth Session, First Comm. 13th Meeting, UN Doc. A/C.1/60/PV.13, at 5.

[19] *See, e.g.*, Revised Draft Resolution: Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/C.1/73/L.27/Rev.1 (Oct. 29, 2018); Draft Resolution: Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/C.1/73/L.37 (Oct. 18, 2018).

[20] White House, Fact Sheet: President Xi Jinping's State Visit to the United States (Sept. 25, 2015).

[21] *See* Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, O.J. (L 194) 1 (July 19, 2016).

https://doi.org/10.1017/aju.2019.9 Published online by Cambridge University Press