doi:10.1017/aju.2019.7

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

WAR WITHOUT WORDS

*Fleur Johns**

"Imagine a celebrated politician in an operating theatre, undergoing robot-assisted surgery. The remotely operated machine is hacked from a foreign server and goes awry, inflicting injury." This was the scenario sketched by Financial Times science writer, Anjana Ahuja, in a recent article.[1] "Does this count as an act of war?" she asked, proceeding to issue dire warnings about the paucity of rules of engagement in such settings, beyond a set of guidelines—the Tallinn Manual—that are regrettably "not legally binding." The result, Ahuja claimed, is that cyber warfare is "a virtual free-for-all."

In the article under discussion in this symposium, Dan Efrony and Yuval Shany have parsed this "free-for-all" with nuance and care. One cannot, they suggest, expect the "comprehensive regulatory scheme"[2] that the Tallinn Manual embodies to come with an on/off switch likely to be determinative, immediately, of nations' fate on the field of cyber warfare. Rather, one needs to evaluate in a granular, contextual, discriminating way the extent to which this Manual may be in the process of becoming "a normative point of reference."[3] In particular, they contend, attention needs to be paid to the role that the Manual may or may not play in a range of strategic settings and how it might, in turn, be conditioning states' sense of the arguments available to them in these settings.

In their article, Efrony and Shany draw attention to three modes of states' strategic engagement with the Manual in evidence derived from analysis of eleven briefly outlined "case studies" framed around contentious interstate cyber operations. In focusing in this way on states' deliberate strategies and expressions of intent, theirs is, broadly speaking, a rational choice account of interstate relations.[4] First, they describe a strategy of optionality adopted in some instances: a strategy that entails "treating the applicable legal framework as optional, in the sense that states may choose whether or not to invoke the legal discourse of international rights and obligations in their mutual interactions in cyberspace."[5] Second, they describe a strategy of "parallel tracks of interstate interaction comprising

* *Professor and Associate Dean (Research), UNSW Law, UNSW Sydney, affiliated with the Allens Hub for Technology, Law & Innovation.* *I am grateful to Maggie Gardner of Cornell Law School for guidance and support throughout the process of guest-editing this symposium and to the AJIL Unbound Editors for affording me an opportunity to be part of it.*

[1] Anjana Ahuja, *Lay Down Rules of Engagement for Cyber War Before It Is Too Late*, Fin. Times (Oct. 22, 2018).

[2] Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AJIL 583 (2018).

[3] *Id.* at 585.

[4] *See generally* Duncan Snidal, *Rational Choice in International Relations*, *in* Handbook of International Relations 85 (Thomas Walter Risse & Beth Simmons eds., 2012).

[5] Efrony & Shany, *supra* note 2, at 648 (2018).

acknowledged and unacknowledged practices, with each track governed by separate 'rules of the game'"[6] (a strategy that presumably overlaps with that of optionality). Finally, Efrony and Shany observe that some states emphasize a particular version of optionality, in relation to acknowledged practices, namely "gradated enforcement."[7] This involves setting conduct covered by the Manual on a spectrum of seriousness, with only some subset of such conduct warranting the adoption of responsive measures on the part of victim states.

In answering the question of what states appear to be making (or not) of the Tallinn Manual in their cyber interactions so far, Efrony and Shany also aim to shed light on "the manner in which international law develops and functions under conditions of significant normative uncertainty and in the absence of effective enforcement mechanisms."[8] In their account, such processes of development are generally contingent on "interstate communication and public diplomacy" and "good faith effort[s] to translate existing legal norms to the new circumstances of cyberspace."[9] The capacity for those efforts to occur is, they claim, "undercut" by the practice of states greeting interstate cyber operations with "silence and ambiguity."[10] Law flows from language and its advance stalls in the quiet, they suggest. The result is "a significant normative gap" that the Tallinn Manual has so far been unable to fill.[11] For Efrony and Shany, international law only "develops and functions" if arguments about strategy and good judgment are expressed as legal distinctions on a field of rhetorical struggle in which legal professionals are recognized belligerents (even if only figuratively speaking, as advisors to statesmen and women).

Interactions at one remove from a realm of argument and counterargument—interactions that entail no obvious effort of reasoned justification—are, in Efrony and Shany's account, regressive, counterproductive, and order-eroding. International law's capacity to curtail or condition the exercise of military power, economic might, and tangible or intangible violence in the cyber domain is presumed to depend upon its capacity to saturate the vocabularies of those with means to deploy such power and to do so in visible, recordable ways. Despite all that we now know of the fraught and complex processes of transmission *en route*, a more or less straight line is still assumed (in Efrony and Shany's article as in other international legal circles) to run from the mind to the mouth and pen hand of the world ruler and from there—decisively—out to happenings in the world.[12] In an increasingly pluralized sphere of argumentative possibilities, the practice of war has become, in large part, a practice of dialogue, as David Kennedy has shown.[13] In this world, those who refuse to speak, or refuse to speak clearly, of their conduct and intentions on the global plane attract the greatest suspicion. It is not so much war that seems most fearsome for international lawyers today as war without words.

For Nicholas Tsagourias, international law is similarly a space- and silence-filler.[14] Tsagourias's essay takes Efrony and Shany's article as a "springboard" for "general international law theory." In his brief account, the metaphoric form that international law takes is that of a three-story house full of words—not just any words, but rather "norms, rules and principles," each occupying its own story. It is out of the movement among these stories that legal order is constituted and from which the standard and goal of a peaceful cyber order might yet be

[6] *Id.* at 650.

[7] *Id.* at 652.

[8] *Id.* at 647.

[9] *Id.* at 648.

[10] *Id.*

[11] *Id.*

[12] For examples of work calling this straight line into question, see Jacob Bercovitch & Allison Houston, *Why Do They Do It Like This? An Analysis of the Factors Influencing Mediation Behavior in International Conflicts*, 44 J. Conflict Res. 170 (2000); Christopher B. Kuner, *Linguistic Equality in International Law: Miscommunication in the Gulf Crisis*, 2 Ind. Int'l & Comp. L. Rev. 175 (1991).

[13] David Kennedy, A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy (2016).

[14] Nicholas Tsagourias, *The Slow Process of Normativizing Cyberspace*, 113 AJIL Unbound 71 (2019).

https://doi.org/10.1017/aju.2019.7 Published online by Cambridge University Press

realized (although the leap from normativization to peacefulness is not one that Tsagourias has room in this short piece to project). For the most part, this structure is inhabited only by states (spoken of generically), although the UN Group of Governmental Experts, and the U.S. delegation to that group, do make passing appearances. It is states that are engaged in a process of normativizing cyberspace by extending thereto territorially sourced and defined norms. No technologists or investors are visible, nor is there any infrastructure in the picture beyond normative infrastructure. Indeed, there is very little that distinguishes this as a space concerned with cyber interactions; Tsagourias's borrowing of Oscar Schachter's general metaphor means that one could imagine the three-story building metaphor accommodating debates over the "normativization" of illegal fishing with little if any alteration. Nonetheless, the weakness of which Efrony and Shany write does have, in Tsagourias's account, a specific location: norms and principles abound in relation to cyberspace, but states have not populated yet the second floor of the putative cyber order with rules. This will, however, be remedied if states continue deliberating so as to produce "coalesce[nce]" among their "interests and preferences," Tsagourias suggests. Perhaps "[r]egional institutions such as the European Union can facilitate quicker norm consolidation by bringing together like-minded states."

It is precisely this orientation towards presumptively "bringing together [the] like-minded" through the vehicle of the Tallinn Manual with which Lianne J.M. Boer takes issue in her contribution to this symposium.[15] For Boer, the limits of so doing are manifest in the Tallinn Manual writers' choice of a particular form of international legal writing and in Efrony and Shany's "quiet acquiescence" in that choice. This is because, in Boer's account, "[f]orm dictates substance." Insistence, on the part of its creators, that the Tallinn Manual be readied for actual use by its "customers" (namely, state legal advisors) restricts their task to that of trying to record what the *lex lata* is, as of a certain date—nothing more and nothing less. Similarly, Efrony and Shany's inclination to take this "form" at face value restricts the kind of research question they can address, Boer contends, and ultimately "goes a very long way [towards] predetermining their answers" to that question. To have the success of the Tallinn Manual rest on states' reactions to it as of a specific date, while contemplating (without expressly speaking to) the prospect of normative change before and after that date, renders the Manual's shortfall almost inevitable. A "gap" between the "Tallinn Rules" and states' actual operations in cyberspace seems unavoidable, Boer suggests, when the limits of the Manual writing task are so tightly conceived. Regardless of what Efrony and Shany's "case studies" show, Boer finds in the formal preference for a restatement of the *lex lata* at a single point in time—and Efrony and Shany's disinclination to question that preference—a design for desuetude.

The Tallinn Manual still risks lying on the shelf, in Kubo Mačák's account, but it does so "close at hand" for key players—namely, those states in search of "creative solutions to safeguard their national interests in cyberspace."[16] In Mačák's estimation—in contrast to Tsagourias's assessment—"it is certainly imaginable that the cyber domain might one day be governed by a global binding agreement." In the near term, however, Mačák sees the unusual correspondence between power and vulnerability in cyberspace—the fact that "the most powerful nations are … also the most vulnerable ones" in this domain—impeding normative convergence. Because the same class of states is likely to be both a site of origin for cyber attacks and their likely targets, explicit double-sidedness in international legal argument retains appeal, Mačák observes, echoing Efrony and Shany's finding of prevailing ambivalence. Only in the comfort and safety of well-appointed "norm-making laboratories"—spear-headed by not-for-profits, major industry figures, and/or "ad hoc" expert groupings—does Mačák envisage states working through this dilemma with the Tallinn Manual near at hand. Concluding with a cookbook analogy, Mačák makes the whole

[15] Lianne J.M. Boer, Lex Lata *Comes with a Date; or, What Follows from Referring to the "Tallinn Rules"*, 113 AJIL Unbound 76 (2019).

[16] Kubo Mačák, *On the Shelf, but Close at Hand: The Contribution of Nonstate Initiatives to International Cyber Law*, 113 AJIL Unbound 81 (2019).

https://doi.org/10.1017/aju.2019.7 Published online by Cambridge University Press

process sound like a rather bloodless and low-stakes affair. In contrast to Efrony and Shany's concluding reference to "fully justified professional anxieties," Mačák ends on a sanguine note.[17]

Stakes are far higher in Ido Kilovaty's response to the Efrony and Shany article, with which this symposium concludes.[18] For Kilovaty, the key word is coercion. In so far as Efrony and Shany document reluctance among states to "adopt fully the norms, premises and analogies offered by the Tallinn Manual," Kilovaty attributes this, in large part, to one major deficiency in the international law there recorded: namely, the current formulation of the norm of nonintervention. More precisely, Kilovaty finds evidence of international law's lamentable ill-suitedness to "hybrid warfare," and to cyber operations in particular, in the idea that intervention in another state's affairs will be illegal under international law only when the perpetrator state "uses methods of coercion." In this regard, Kilovaty locates in Efrony and Shany's study both cause for hope and cause for worry. Kilovaty seems heartened by the article's documentation of "how the notion of nonintervention in cyber relations already deviates from the more traditional approach." At the same time, Kilovaty worries that the strategies that Efrony and Shany describe states adopting in responding (or not) to cyber operations might "disrupt such [customary law] development," much as Efrony and Shany conclude themselves.

Although Kilovaty (like Efrony and Shany and the other contributors to this symposium) sees challenges ahead, his preference is to confront these challenges with a relatively narrowly-framed, reformist call to action. States—and presumably scholars—must get behind a "reformulation of the nonintervention norm that does not view coercion as its focal point," Kilovaty contends. Returning to the environs of Tsagourias's essay, we are back on the second floor of the three-story building representative of the "putative legal order" of cyber space—in the realm of rules—only now we are accompanied by a metaphoric tradesperson proposing a specific fix to some part of its plumbing.

That a single article might have provoked such a range of responses—from the theoretical to the stylistic or grammatical, from the championing of multisectoral experiment to the championing of doctrinal reform—is a testament to the richness of Efrony and Shany's analysis. A "regulatory void" might have been "avoid[ed]," in Efrony and Shany's account, thanks to the "Tallinn Rules," but this seems to offer little comfort to them or their readers. Instead, the reader of this symposium will witness agitation over "gaps": some contributors asking from whence they might have emerged, others rushing to plug them in a range of ways. Much is left unsaid and untouched—about resources, and relative access to them, above all. Nonetheless, that both critical suspicions and creative appetites have been stimulated in this fast-moving sector of the international legal field is cause for celebration. Thanks in part to Efrony and Shany and the contributors to this symposium, the war without words of cyber operations might find its legal tongue yet.

[17] Efrony & Shany, *supra* note 2, at 654.

[18] Ido Kilovaty, *The Elephant in the Room: Coercion*, 113 AJIL UNBOUND 87 (2019).

https://doi.org/10.1017/aju.2019.7 Published online by Cambridge University Press