doi:10.1017/aju.2019.10

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

THE ELEPHANT IN THE ROOM: COERCION

*Ido Kilovaty**

Dan Efrony and Yuval Shany's article offers some critically important observations on the reception of the Tallinn Manual 2.0 by states, as well as subsequent state practice and *opinio juris* with regard to the international use of cyber operations. Based on their case studies, Efrony and Shany conclude that states have largely been reluctant to adopt fully the norms, premises, and analogies offered by the Tallinn Manual. The authors argue that there is a "deep uncertainty about the treatment of cyberspace as just another physical space, like land, air, or sea—over which states may exercise sovereignty or control."[1] The authors further explain that there is an "uneasy fit" between traditional international law regarding internal and external state power, and the regulation of a unterritorial cyberspace. In other words, cyberspace is a *sui generis* domain, such that analogies to physical-space domains are often ill-suited, and at times doomed to failure.

In particular, Efrony and Shany's eleven case studies suggest that the notion of coercion, a "requisite component of the non-intervention rule,"[2] is becoming blurrier with the emerging state practice of offensive and defensive cyber operations and ought to be reconsidered, whether by states individually or through a subsequent multilateral codification of norms for international use of cyber capabilities. This blurring reflects the absence of any guiding norms and principles on what constitutes coercion, and it is arguably contrary to the ICJ judgment in *Nicaragua*,[3] where the Court unequivocally held that "intervention is wrongful when it uses methods of coercion" and that coercion is "the very essence" of intervention.[4] The ICJ's view cannot hold in an era where cyberspace is used for harmful interference that cannot, almost by definition, be coercive.

Coercion, as traditionally understood, is absent from all of the cyber interferences identified in Efrony and Shany's eleven case studies, precluding a determination of illegality under international law. These case studies thus reveal that the Tallinn Manual's reliance on a coercion standard in its rule on nonintervention is underinclusive, and therefore underprotective of essential state interests. Instead, cyber operations require a more nuanced definition of nonintervention that departs from the narrow coercion standard. Such a norm would not categorically condemn all interference, but rather reevaluate which cyber operations significantly jeopardize the internal

* *Frederic Dorwart Endowed Assistant Professor of Law, University of Tulsa, College of Law; Cybersecurity Policy Fellow, New America; Visiting Faculty Fellow, Center for Global Legal Challenges, Yale Law School; Affiliated Fellow, Information Society Project, Yale Law School.*

[1] Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AJIL 583, 653 (2018).

[2] *Id.* at 641.

[3] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, 1986 ICJ Rep. 14, para. 205 (June 27).

[4] *Id.*

and external affairs of a state, including election integrity, territorial and political sovereignty, self-determination, and many other values that international law has long recognized and defended from undue external influence.

Cyber Intervention

As Efrony and Shany observe, the Tallinn Manual recognizes the applicability of a customary international law rule on nonintervention to cyber operations.[5] The Tallinn Manual provides that "States may not intervene, including by cyber means, in the internal or external affairs of another State"[6] and subsequently clarifies that in order to be wrongful under international law, such intervention "must be coercive in nature."[7] This definition dovetails with the ICJ's limitation of prohibited intervention only to acts that employ methods of coercion. Applying this rule in the cyberspace context would mean that intervention in internal or external affairs through the use of cyber operations is prohibited only if it is unequivocally coercive, a problematic notion that excludes a variety of harmful cyber operations. States can achieve their strategic and political goals vis-à-vis other states without having to openly coerce them into a decision they would otherwise not have taken,[8] or without usurping "essential governmental functions," as Efrony and Shany stipulate. Efrony and Shany themselves consider at least ten out of their eleven case studies to be in breach of the norm of nonintervention, even though most of these cyber operations are noncoercive by nature.[9]

The Tallinn Manual's delimitation of wrongfulness of cyber intervention to only those acts that are coercive in nature is a missed opportunity on the Manual's part to address the novelty and thus legal uncertainty surrounding cyber intervention. Perhaps such failure is understandable given the narrow, self-proclaimed methodology of the Tallinn Manual, which seeks to identify law at present (*lex lata*) rather than future or optimal law (*lex ferenda*). By focusing on *lex lata*, the Tallinn Manual created a considerable normative gap when it distinguished coercion from "persuasion, criticism, public diplomacy, propaganda … retribution, [and] mere maliciousness" based on the logic that these latter tools would merely influence voluntary state actions.[10] This logic ignores the ability of other uncoercive methods—such as manipulation, deception, disruption, and disinformation—to trigger the involuntary actions of the victim state. In addition, the Tallinn Manual's experts could not reach a consensus on whether knowledge of the intervention is required as a precondition for wrongfulness.[11] This normative gap could explain why states currently deviate from the rules proposed by the Manual and why they have not endorsed the Manual's approach to cyber interventions. Efrony and Shany provide a detailed account of how the notion of nonintervention in cyber relations already deviates from the more traditional approach when they argue that ten out of their eleven case studies could plausibly be in violation of the norm on nonintervention.

The Manual further attempted to express its view on a contentious and very realistic hypothetical: the hacking of electronic ballots. At first blush, it would seem that hacking electronic ballots would seriously undermine the very basic and central function of a sovereign state: the choice of its political identity and organization. As Steven Barela put it, "[T]he disruption of a free and fair election strikes at a *sine qua non* for the State."[12] The Manual's experts

[5] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 312, Rule 66 (Michael N. Schmitt ed., 2017) [hereinafter Tallinn Manual 2.0].

[6] *Id.*

[7] *Id.* at 320.

[8] Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30 (2018).

[9] Efrony & Shany, *supra* note 1, at 655–57.

[10] Tallinn Manual 2.0, *supra* note 5, at 318.

[11] *Id.* at 320.

[12] *See* Steven Barela, *Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion*, JUST SECURITY (Jan. 12, 2017).

https://doi.org/10.1017/aju.2019.10 Published online by Cambridge University Press

were split as to whether such cyber operation would violate the norm on nonintervention, indicating that the law is unsettled and lacks granularity on the scope of prohibited cyber intervention. While the majority of experts believed this to be an act of prohibited intervention, a few experts argued that it would only qualify as prohibited intervention if the victim state knows of such a cyber operation.[13]

This minority view is impractical in the cyber context since victim states would rarely be aware in real time that their or their citizens' decisions are being affected by manipulation, disruption, or disinformation. Such lack of knowledge should not preclude the wrongfulness of the initial intervening cyber operation. Even Michael Schmitt subsequently admitted that the ambiguity on this question "represents a troubling threat to the democratic process."[14] This hypothetical demonstrates the difficulty of applying coercion to a manipulation of election integrity. It is not a coercive act (do X, or else), but rather an act that deprives either the victim state or its citizens of a free choice. The Tallinn Manual approach to cyber interference generates an uncomfortable question as to whether coercion is the only standard that should govern wrongful interventions, in particular in cyberspace, as certain uncoercive methods enabled by cyberspace would nonetheless violate a state's ability to freely pursue its internal and external affairs. Efrony and Shany indicate that the rule on nonintervention may be changing, however, as evidenced by the U.S. indictments of Russian hackers involved in the DNC hack and the UK attorney general's view of election meddling as a form of coercive intervention.[15]

More generally, their analysis of recent cyber interference demonstrates the uneasy fit and practical limits of territorial norms as applied to cyberspace. This notion that territorial norms cannot accommodate the realities of cyberspace is central to what Efrony and Shany identify as "suitability," or the legitimacy of utilizing current international law, and the norm on nonintervention in particular, in the cyberspace context. This critique is focused on the incompatibility of Westphalian geographical and political notions with the "structure, design and operating protocols of the internet."[16] The irrelevance of territoriality is also due to the way in which cyber capabilities have transformed the nature of intervention. Indeed, throughout their article, Efrony and Shany identify the resistance of states to legal translation, namely using traditional concepts of international law for cyber operations, which do not seem to fit well considering the novelty and unique characteristics of cyber operations.[17]

This tension has led to debate over the scope of the coercion standard. Some have argued that states that merely spread disinformation or fake news on social media to influence potential voters are engaging in coercive interference,[18] while others have ignored the coercion standard altogether, arguing that even the use of noncoercive cyber tactics to undermine sovereign functions runs afoul of the norm on nonintervention.[19] The long-term difficulty with such approaches to cyber intervention is that they either expand coercion beyond any reasonable boundaries, or they ignore the doctrinal requirement of coercion entirely. For example, a minority of the Tallinn Manual experts believe that the coercion requirement is satisfied when "an act has the effect of depriving the State of control over the matter in question."[20] Similarly, Steven Barela holds the view that the Russian breach of the DNC's servers, with the intent to manipulate voters and "public opinion on the eve of elections," is inherently coercive.[21]

[13] Tallinn Manual 2.0, *supra* note 5, at 320–21.

[14] Schmitt, *supra* note 8.

[15] *See* Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 Tex. L. Rev. 1579, 1580 (2017).

[16] Efrony & Shany, *supra* note 1, at 589.

[17] *Id.* at 653.

[18] Harold Hongju Koh, *The Trump Administration and International Law*, 56 Washburn L.J. 413, 450 (2017).

[19] Efrony & Shany, *supra* note 1, at 642.

[20] Tallinn Manual 2.0, *supra* note 6, at 318.

[21] Barela, *supra* note 12.

https://doi.org/10.1017/aju.2019.10 Published online by Cambridge University Press

Coercion is not a tenable standard for restraining the use of cyber means to influence or otherwise restrict sovereign functions. It provides no consistency, guidance, or clarity as to how international law ought to view cyber intervention. Further, conditioning the wrongfulness of cyber intervention on whether such intervention is coercive reveals some naiveté, considering how uncoercive these methods currently are. Current practice represents emerging attempts to legally constrain cyber intervention, but there is no consensus suggesting what standard ought to prevail. Consequently, we need a new standard to identify wrongful cyber interventions, one that recognizes that cyber intervention can be achieved through manipulation, deception, disruption, disinformation, and many other methods that a limited conception of coercion would not be capable of capturing.

A New Standard

If coercion does not work to delineate wrongful cyber interference, the norm of nonintervention needs an alternative standard that accounts for the unique characteristics surrounding the offensive use of cyber capabilities. In short, the wrongfulness of cyber intervention ought to be defined not by whether it is coercive by nature, but by whether a cyber intervention prevented a state from freely exercising functions associated with its internal and external affairs. This alternative standard would look at the degree of influence, conscious or subconscious, exerted by a cyber operation on the protected *domain réservé* of a victim state. In other words, the nonintervention standard ought to focus on the deprivation of free choice, on which the current coercion standard only lightly touches. States would be wise to clarify this alternative standard and the threshold above which interference will be considered a violation of the norm.

Efrony and Shany identify three strategies adopted by states, however, that may disrupt such development: optionality, parallel tracks, and gradation in law enforcement.[22] In particular, the emergence of a new standard may be hindered by the transparency challenge identified by Efrony and Shany. The building blocks of a new norm of customary international law include information about the occurrence of a cyber intervention, the method used, direct and indirect consequences, and the response (or lack thereof) of the victim state. But in the cyber context, it is difficult to access such evidence due to the secrecy that states maintain by default in that space. The *optionality* and *parallel tracks* strategies identified by Efrony and Shany are emblematic of this evidentiary challenge. The covert nature of cyber operations has become the norm since states believe that publicity or transparency "might expose their vulnerabilities, adversely affect their offensive or defensive capabilities, and weaken their power of deterrence."[23] Brian Egan identified this difficulty in a speech given at Berkeley in which he highlighted the need for "increased transparency … to clarify how the international law on non-intervention applies to States' activities in cyberspace."[24] Schmitt, reacting to Egan, seems to support the need for more transparency on the part of states operating in cyberspace.[25] Until more public information and evidence is available, identifying a new customary international legal standard for cyber intervention may prove difficult. States whose practices in cyberspace are transparent may therefore benefit from the ability to control and steer the development of customary international law toward a desirable direction.

That being said, Efrony and Shany indicate that as many as ten out of eleven case studies had potentially triggered the norm on nonintervention to some extent. This may suggest some form of emerging norm on intervention through cyber operations, though crucial questions remain: Are states attempting to replace coercion with an

[22] Efrony & Shany, *supra* note 1, at 648–52.

[23] *Id.* at 631.

[24] Brian Egan, Legal Adviser, U.S. Dep't of State, *Address at University of California-Berkeley School of Law: International Law and Stability in Cyberspace*, Just Security (Nov. 10, 2016).

[25] Michael Schmitt, *US Transparency Regarding International Law in Cyberspace*, Just Security (Nov. 15, 2016).

https://doi.org/10.1017/aju.2019.10 Published online by Cambridge University Press

alternative standard? Would such a norm be specific to cyberspace or also applicable in the physical space? Do responses by individual victim states follow any long-term strategy, or do they represent one-off responses to real-time incidents? What evidence do victim states use to develop their international legal approaches to countering hostile cyber operations? It may be the case that egregious interventions—such as hacking an election—may push states to directly address emerging forms of cyber operations, as well as the new norms required to tackle them. This, perhaps, will lead to more transparency around the evidence required for the establishment of an emerging norm.

Conclusion

This response to Efrony and Shany's article calls for the expansion of the current notion of intervention, arguing that intervention through cyberspace, even when lacking a forceful or dictatorial coercive element, may still be wrongful if it violates the protected internal and external affairs of a state, in particular its free choice. Indeed, wrongful intervention may use methods of manipulation, deception, disruption, or disinformation, all of which are not necessarily coercive methods. Efrony and Shany's work reveals a broader reluctance on the part of states to apply territorial legal norms in this regard to cyberspace conduct. The authors identify emerging state practice that already deviates from traditional notions of intervention, though such practice may lack any inherent logic, consistency, long-term strategy, or normative legitimacy considering the underlying state strategies of *optionality, parallel tracks,* and *gradation in law enforcement*. The way forward should focus on providing more transparency, cooperation, and collective action to develop alternative norms to counter hostile cyber operations. It is unclear how unexplained deviations in applying the nonintervention norm, as identified in Efrony and Shany's case studies, serve the long-term rule of law of the international legal system. This essay, in response, suggests that a reformulation of the nonintervention norm that does not view coercion as its focal point is much needed to contain the adverse effects of cyber interventions.

https://doi.org/10.1017/aju.2019.10 Published online by Cambridge University Press