ON THE SHELF, BUT CLOSE AT HAND: THE CONTRIBUTION OF NON-STATE INITIATIVES TO INTERNATIONAL CYBER LAW

Kubo Mačák[*]

In late 2018, the New York Times reported that the U.S. Cyber Command had targeted individual Russian hackers in order to deter them from engaging in conduct that could affect the organization and outcome of the U.S. mid-term elections.[1] This unusual pre-emptive step suggests that states are looking for creative solutions to safeguard their national interests in cyberspace. But to what extent should their conduct be guided by considerations of international law? In this essay, I explore several key aspects of that central conundrum. I argue that (1) we should see cyberspace as an underregulated (but not ungoverned) domain; (2) a main reason for that state of affairs lies in a unique strategic dilemma innate to the cyber domain; and (3) non-state initiatives, including the eponymous "rule book on the shelf,"[2] have a critical role to play in the development of the law in this area.

The Underregulated Domain

In 2019, it is no longer seriously argued that the reach of existing legal rules is or should be limited to the offline world.[3] On the contrary, the most cyber-active nations have reached a consensus, expressed in two consecutive reports of a UN-mandated group of governmental experts, that international law *is* applicable to cyberspace.[4] Although progress in the work of the group halted in mid-2017, both competing visions for its revival (proposed by 36 and 31 countries, respectively) still fully endorse that baseline agreement.[5]

Additionally, since the 1990s, states have occasionally floated the idea of a global cyber treaty.[6] Most recently, China, Russia, and several Central Asian nations put forward two consecutive versions of a "Code of Conduct for Information Security."[7] However, a few crucial provisions in the Code were off-putting to their Western counterparts, including the duty to co-operate in combating terrorism, separatism and extremism[8]—a wide formulation that could negatively impact human rights.[9] As the United States noted in rejecting the instrument, it

---

[*] Senior Lecturer in Law, University of Exeter. I am grateful to Ana Beduschi, Curtis Bradley, Ashley Deeks, Maggie Gardner, Fleur Johns, Tomáš Minárik, and Mike Schmitt for comments on earlier drafts.

[1] Julian Barnes, *U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections*, N.Y. TIMES, Oct. 23, 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] *Cf., e.g.*, David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

[4] UN Doc. A/68/98, para. 19 (June 24, 2013); UN Doc. A/70/174, para. 24 (July 22, 2015).

[5] *Compare* UN Doc. A/C.1/73/L.37 (Oct. 18, 2018) *and* UN Doc. A/C.1/73/L.27/Rev.1 (Oct. 29, 2018). Somewhat surprisingly, *both* proposals were approved by the First Committee of the UN General Assembly in November 2018.

[6] *See, e.g.*, Tim S. Wu, *Cyberspace Sovereignty? The Internet and the International System*, 10 HARV. J.L. & TECH. 647, 660 (1997) (noting a 1996 French proposal).

[7] *See* Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/66/359, 14 September 2011, at 3–5; 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, at 3–6.

[8] *Id.* at para. 2(4).

[9] *See, e.g.*, Leonhard Kreuzer, *Disentangling the Cyber Security Debate*, VÖLKERRECHTSBLOG (June 20, 2018).

"cannot support approaches proposed in the draft Code … that would only legitimize repressive state practices."[10]

To be sure, repeated failures of proposals with global ambitions underscore Efrony and Shany's analysis that cyberspace is "exceptionally difficult to regulate."[11] Still, it is certainly imaginable that the cyber domain might one day be governed by a global binding agreement. After all, many other areas marked by non-national spaces and/or shared resources have proved susceptible to such regulation, including Antarctica,[12] outer space,[13] or the high seas.[14] So how likely is it that there is going to be, say, a 2025 Cyberspace Treaty?

Not very. This is due to a complex mix of reasons. The digital domain may still be awaiting its "constitutional moment," a transformative event that would galvanize states into action and bring their representatives to the negotiating table.[15] The technology probably keeps evolving too fast to allow for a meaningful consolidation of interests, a necessary precursor to any drafting exercise.[16] Relatedly, accurate technical attribution of conduct in cyberspace remains a problem,[17] which in turn undermines potential verification efforts—and why bother drafting a treaty the compliance with which cannot be properly verified?[18] All these reasons weaken the prospects of a global cyber convention. However, the principal obstacle to state-led law-making in the area of international cyber law arguably lies in an unprecedented dilemma posed by the unique nature of cyberspace.

The Glass House Dilemma

Asymmetries of cyberspace mean that the most powerful nations are, in a peculiar way, also the most vulnerable ones. In other spheres of human activity, states that wield the greatest power generally seek the greatest latitude for their actions and thus usually endorse permissive norms of behavior. Conversely, as a rule, weaker states support restrictive norms, seen as shields against their more powerful adversaries. Accordingly, major maritime powers have historically preferred norms that strengthened the freedom of the seas, whereas coastal states have insisted on projecting their sovereignty seawards.[19]

The situation is much less straightforward in the cyber domain. Paradoxically, the more a society relies on its cyber capabilities, the more it becomes vulnerable to malicious cyber operations. On the offensive side, cyber powers may thus prefer permissive rules that would leave some leeway for stone-throwing. But on defense, those same states desperately need restrictive rules to protect the elaborate glass houses they are sitting in. Any development of rules of behavior in cyberspace thus needs to address not only the usual diversity of views held

[10] Statement by the Delegation of the United States of America, Nov. 2, 2012.
[11] Efrony & Shany, *supra* note 2, at 652.
[12] Antarctic Treaty, Dec. 1, 1959, 402 UNTS 71.
[13] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 UNTS 205.
[14] UN Convention on the Law of the Sea, Dec. 10, 1982, 1833 UNTS 397.
[15] *See* Anne-Marie Slaughter & William Burke-White, *An International Constitutional Moment*, 43 HARV. INT'L L.J. 1, 2 (2002).
[16] *See, e.g.*, ANDREW T. GUZMAN, HOW INTERNATIONAL LAW WORKS: A RATIONAL CHOICE THEORY 129 (2008).
[17] *See also* Efrony & Shany, *supra* note 2, at 632–33.
[18] JACK GOLDSMITH, CYBERSECURITY TREATIES: A SKEPTICAL VIEW 10–12 (2011).
[19] *See* René-Jean Dupuy, *The Sea under National Competence*, *in* 1 A HANDBOOK ON THE NEW LAW OF THE SEA 247 (René-Jean Dupuy & Daniel Vignes eds., 1991).

by various states, but also the schizophrenic and sometimes mutually exclusive interests that an individual state may hold.

The best illustration of this dilemma is in the legal qualification of low-level cyber attacks that have come to define our time. Consider, for instance, the statement issued by the British National Cyber Security Centre (NCSC) in October 2018, which attributed a series of cyber attacks against various targets in the UK and elsewhere to the GRU, the Russian military intelligence service.[20] It expressly noted that "[t]hese attacks have been conducted in flagrant violation of international law," but, remarkably, the statement did not explain which specific international obligations had allegedly been breached.[21]

Specifically, the NCSC noted that the GRU was "almost certainly responsible" for accessing e-mail accounts belonging to an unnamed UK-based TV station and for stealing their contents.[22] Similarly, it considered the GRU "almost certainly responsible" for attempting to compromise computer systems belonging to the Foreign and Commonwealth Office (FCO) and the Defence and Science Technology Laboratory (DSTL).[23] Such cyber operations can hardly be described as examples of friendly or responsible behavior. However, it is less certain that this conduct actually violated specific rules of international law.

The most obvious argument that the UK could have relied on, as noted by Schmitt and Biller, is that interference with computer systems on UK territory without its consent violated its sovereignty.[24] Tallinn Manual 2.0 sets out the framework for such an argument in its Rule 4, which prescribes that "[a] State must not conduct cyber operations that violate the sovereignty of another State."[25] However, the Tallinn framework does not equate all interference with a violation. Rather, the experts considered that interference with cyber infrastructure (such as computer systems belonging to a private TV station) would, at a minimum, need to result in a loss of functionality of that infrastructure for the Rule to be violated.[26] It is unlikely that such effect materialized through the cyber operations against the e-mail accounts of the affected British TV station if they were limited to the exfiltration of data. By contrast, regarding the FCO and DSTL attacks, the Tallinn commentary considers that "changing or deleting data such that it interferes with … the effective conduct of diplomacy [or] the performance of key national defence activities" could undermine a state's exercise of one of its inherently governmental functions and thus violate its sovereignty.[27] Depending on the actual or intended effect of those operations, the UK thus could have argued that Russia violated its rights based on the Tallinn interpretation of the law.

However, earlier in 2018, the UK expressly repudiated the view that non-consensual interference in the computer networks of another state amounts to a violation of that state's

---

[20] UK NCSC, "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed" (Oct. 4, 2018).
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] Jeffrey Biller & Michael Schmitt, *Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences*, EJIL: TALK! (Oct. 24, 2018).
[25] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 17 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].
[26] *Cf. id.* at 20–21, para. 13. The experts could not agree on the precise threshold at which such loss of functionality constitutes a violation. *Id.*
[27] *Id.* at 22, para. 16.

sovereignty.[28] Instead, in a speech by its Attorney General, the United Kingdom endorsed the position "that there is no such rule as a matter of current international law."[29] This obviously reduced the United Kingdom's room for maneuver when it came to the legal qualification of the alleged Russian cyber operations.[30] It also likely explains why the NCSC statement did not contain any legal reasoning in support of the accusations.

This example illustrates the difficult dilemma faced by states that use their cyber capabilities in both offensive and defensive ways. In offence, it is in the United Kingdom's interest to "interpret down" the applicable law and assert, as the Attorney General did, that low-level attacks do not violate any existing international legal rules. Conversely, in defense, the United Kingdom's interest is to "interpret up" the law and insist, as the NCSC statement did, that such attacks do amount to violations. These interpretive dances are not only of symbolic value. When a state is the victim of a violation of international law, it is entitled to take action to compel the responsible state to stop, even if that action would otherwise be unlawful.[31] Any such conduct in response is governed by the law of countermeasures, the applicability of which to cyberspace has been expressly endorsed by the United Kingdom.[32]

The glass house dilemma is a key element of the "perfect storm" of challenges for the regulation of cyberspace described in the lead article.[33] As the UK example shows, even those states that desire to move away from Efrony and Shany's "policy of optionality"[34] may find themselves torn between particular interpretations of international cyber law. By contrast, other domains are considerably more linear in terms of specific states' interests. For instance, as the future Outer Space Treaty was being developed in the 1960s, the dividing lines lay between the capitalist West and the communist East, and between the space-faring nations and states without such capability.[35] No such clear categories have yet emerged in the complex world of cyberspace.[36]

The Role of the Non-State Actors

Whatever the reason for states' silence, it has generated a regulatory void, which has in turn prompted other actors to step in. Reflecting the current multi-stakeholder approach to cyberspace governance,[37] these actors are quite diverse. In addition to the two Tallinn groups of experts scrutinized in the lead article, they have included think tanks (EastWest Institute or Carnegie Endowment for International Peace), representatives of industry (Microsoft or Siemens), and ad hoc groupings (like the Global Commission on the Stability of Cyberspace ("GCSC")).

---

[28] *See* Jeremy Wright, Cyber and International Law in the 21st Century (May 23, 2018).
[29] *Id.*
[30] Biller & Schmitt, *supra* note 24.
[31] Articles on Responsibility of States for Internationally Wrongful Acts, *in* Int'l Law Comm'n Rep. on the Work of Its Fifty-Third Session, UN GAOR, 56th Sess., Arts. 22 and 49–53, UN Doc. A/56/10 (2001).
[32] Wright, *supra* note 28.
[33] Efrony & Shany, *supra* note 2, at 652.
[34] *Id.* at 648–49.
[35] *Cf.* Ram Jakhu, *Evolution of the Outer Space Treaty*, *in* 50 YEARS OF THE OUTER SPACE TREATY 14–18 (Ajey Lele ed., 2017).
[36] *But see* Zhixiong Huang & Kubo Mačák, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, 16 CHINESE J. INT'L L. 271 (2017).
[37] *See further* Joanna Kulesza, *Multistakeholderism: Meaning and Implications*, *in* HUMAN RIGHTS, THE DIGITAL SOCIETY AND LAW: A RESEARCH COMPANION (Mart Susi ed., forthcoming 2019).

What connects these efforts is their shared aim to articulate norms of state conduct in cyberspace. For instance, Microsoft called on states to "exercise restraint in developing cyber weapons" and to "commit to nonproliferation activities" concerning such weapons.[38] The Carnegie Endowment has pushed for a state commitment to refrain from conducting cyber operations that "undermine the integrity of data and algorithms of financial institutions."[39] And the GCSC has proposed a norm package on the stability of cyberspace, which includes norms urging states to disclose known vulnerabilities and to enact basic cyber hygiene.[40]

These initiatives serve as "norm-making laboratories" for states.[41] Ultimately, only states make international law; moreover, there are obvious question marks surrounding the legitimacy of endeavors initiated by private actors.[42] Still, these initiatives do contribute in important ways to "the pluralisation of international norm-making."[43] The proliferation of cyber norms initiatives that are non-state driven but state-oriented gives states a unique opportunity to learn from, engage with, and react to those initiatives. It is these reactions that then become building blocks in the edifice of emerging rules of custom and interpretations of treaty rules—in other words, the law.

Several cyber-active (and predominantly western) states have recognized the importance of these initiatives. For example, state representatives have described the Tallinn Manuals as "the first step in codifying cyber law,"[44] as an aid in the creation of national positions on international cyber law,[45] and as a "roadmap" for state action in cyberspace.[46] The GCSC has received funding from states including Estonia, the Netherlands, and Singapore. And in November 2018, France launched the non-binding "Paris Call for Trust and Security in Cyberspace," which was reportedly crafted jointly with Microsoft, and which more than 50 countries and 200 other stakeholders subsequently signed.[47]

However, what is more important than such pronouncements is the extent to which states meaningfully engage with the underlying initiatives. Precedents suggest that states do take some non-state-led proposals seriously. For example, the 1994 San Remo Manual on International Law Applicable to Armed Conflicts at Sea has greatly influenced the text of several national military manuals[48] and, in a submission to the International Court of Justice, the United States expressly stated that it considered most of its provisions to reflect customary law.[49] It is still early days for the cyber norms initiatives, but paradoxically even a repudiation of their interpretations (like the rejection of the Tallinn Manual's sovereignty-as-rule approach by the United Kingdom) confirms their growing influence. By providing much-needed nuance

---

[38] Microsoft, International Cybersecurity Norms: Part 2 (undated).
[39] Tim Maurer et al., "Towards a Global Norm Against Manipulating the Integrity of Financial Data" (Mar. 28, 2017).
[40] GCSC, "Norm Package Singapore" (Nov. 2018).
[41] *See* Kubo Mačák, *From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers*, 30 LEIDEN J. INT'L. L. 877, 894 (2017).
[42] *See, e.g.*, Louise Marie Hurel & Luisa Cruz Lobato, *Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs*, 3(1) J. CYBER POLICY 61, 67–70 (2018).
[43] JEAN D'ASPREMONT, FORMALISM AND THE SOURCES OF INTERNATIONAL LAW 222 (2011).
[44] CCDCOE, Croatian Prime Minister: Tallinn Manual is an Icebreaker (Jan. 27, 2015).
[45] Kersti Kaljulaid, President of the Republic Opening speech at CyCon 2017 (May 31, 2017).
[46] Stef Blok, Speech by Minister Blok on First Anniversary Tallinn Manual 2.0 (June 20, 2018).
[47] Louise Matsakis, *The US Sits out an International Cybersecurity Agreement*, WIRED (Nov. 11, 2018).
[48] *See, e.g.*, THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT vii (2004) (noting that the chapter on Maritime Warfare was "based substantially" on the San Remo Manual).
[49] *Oil Platforms* (Iran v U.S.), Counter-Memorial and Counter-Claim, at 130 n.292 (June 23, 1997).

and granularity, non-state initiatives thus assist states in gradually resolving the glass house dilemma and help foster the international rule of law in the cyber domain.

Conclusion

The fact that a compilation of rules like the Tallinn Manual sits "on the shelves" of legal advisors around the world should not necessarily be seen as a weakness. To borrow an analogy from the culinary world, one doesn't really have to keep the cookbooks on the kitchen stove for them to have an impact on one's gastronomical creations. As long as the chef takes them "off the shelf" here and there and peruses them before beginning the next cooking adventure, they will probably have some influence on what the guests will consume that night. Like cookbooks, rulebooks (and other norms proposals) actually *belong* on the shelves—what matters is that they are easy to reach.