University of Reading

Taming the lawless void: tracking the evolution of international law rules for cyberspace

Article

Published Version

Schmitt, M. N. ORCID: https://orcid.org/0000-0002-7373-9557 (2020) Taming the lawless void: tracking the evolution of international law rules for cyberspace. Texas National Security Review, 3 (3). pp. 32-47. ISSN 2576-1153 Available at https://centaur.reading.ac.uk/93148/

It is advisable to refer to the publisher's version if you intend to cite from the work. See Guidance on citing.

Published version at: https://tnsr.org/2020/07/taming-the-lawless-void-tracking-the-evolution-of-international-law-rules-for-cyberspace/

Publisher: University of Texas

All outputs in CentAUR are protected by Intellectual Property Rights law, including copyright law. Copyright and IPR is retained by the creators or other copyright holders. Terms and conditions for use of this material are defined in the End User Agreement.

www.reading.ac.uk/centaur

University of Reading

CentAUR

Central Archive at the University of Reading

Reading's research outputs online

Texas National Security Review: Volume 3, Issue 3 (Autumn 2020)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

TAMING THE LAWLESS VOID: TRACKING THE EVOLUTION OF INTERNATIONAL LAW RULES FOR CYBERSPACE

Michael N. Schmitt

The myth that cyberspace is a legal Wild West has been roundly rejected by states and scholars. As cyberspace norms evolve, states will advocate interpretations of existing international law rules that advance their national interests. In this regard, states are treating international law rules as normative firewalls that safeguard their interests by deterring malevolent behavior. At the same time, states are interpreting the rules in a manner that maximizes their response options when facing hostile cyber operations.

In February 2020, Adm. Mike Gilday, the U.S. chief of naval operations, observed that "We're not fighting an enemy that people can see ... And we're not fighting a war where international norms exist. But make no mistake, we are in conflict day-in and day-out in the cyber realm."[1] His remarks came on the heels of U.N. Secretary-General António Guterres' pronouncement that "We ... must usher in order to the Wild West of cyberspace,"[2] a characterization of that domain utilized by President Barack Obama five years earlier when he remarked, "The cyber world is sort of the wild, wild West. And to some degree, we're asked to be the sheriff."[3]

Gilday, Guterres, and Obama were not suggesting that cyberspace is a legal void. Both the United Nations and the United States have emphasized international law's applicability to cyber conflict.[4] However, their statements could be understood as suggesting that international law might not be up to the task of governing cyberspace.

This apparent skepticism has been exacerbated by the practice of some states to "cherry-pick" amongst the international law rules that govern cyberspace. In 2017, for instance, the U.N. Group of Governmental Experts charged with identifying consensus norms for cyberspace failed to agree on including references to such fundamental aspects of international law as "self-defense" and "international humanitarian law" in its report due to opposition from Russia, China, Cuba, and several other states. Yet, those same states embraced other rules of international law and had earlier signaled their acceptance of both self-defense and humanitarian law in the 2015 Group of Governmental Experts report.[5] The next year, the U.K. attorney general disputed the existence of an international law rule prohibiting the violation of another state's sovereignty by cyber means, a rule of long lineage that was previously widely understood to apply to cyber operations. However, in the same speech, he endorsed other key international law rules such as the prohibition on cyber intervention into another state's internal affairs and the right to self-defense against severe cyber attacks.[6]

Meanwhile, hostile cyber operations are on the rise, in both frequency and severity. Recall, for instance, the use of cyber operations during the armed conflict with ISIL, the WannaCry attack that hobbled the National Health Service in the United

1 Naomi VanDuser, "NCWDG Celebrates Opening of Cyber Foundry," *Defense Visual Information Distribution Service*, Feb. 18, 2020, https://www.dvidshub.net/news/363356/ncwdg-celebrates-opening-cyber-foundry#.Xkx8I44ONeo.twitter.

2 Secretary-General António Guterres, "Remarks to the General Assembly on the Secretary-General's Priorities for 2020," *United Nations Secretary-General*, Jan. 22, 2020, https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-general-assembly-priorities-for-2020.

3 The White House, "Remarks by the President at the Cybersecurity and Consumer Protection Summit, Stanford University," Office of the Press Secretary, Feb. 13, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

4 For current positions, see, Office of General Counsel, Department of Defense, "Department of Defense: Law of War Manual," June 2015 (Updated Dec. 2016), https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190; U.N. Secretary-General, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc. A/70/174, July 22, 2015 [hereinafter 2015 GGE Report], https://digitallibrary.un.org/record/799853?ln=en.

5 Michael Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms," *Just Security*, June 30, 2017, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

6 Jeremy Wright, Attorney General of the UK, "Cyber and International Law in the 21st Century," *Chatham House*, May 23, 2018, [hereafter Wright Address], https://www.chathamhouse.org/event/cyber-and-international-law-21st-century.

Kingdom, the NotPetya operation against Ukrainian cyber infrastructure that spread globally and caused billions of dollars in losses, and the use of cyber means to exploit the novel coronavirus pandemic. Given the rising importance of cyber conflict, there is an evident need to clarify how such attacks can be defined within the realm of international law.

Despite these troubling occurrences, cyberspace is hardly a lawless void where the "strong do what they can and the weak suffer what they must."[7] In 2017, a distinguished group of international law scholars and practitioners — the International Group of Experts — published the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.[8] The product of a NATO Cooperative Cyber Defence Centre of Excellence project stretching over eight years, the manual contains 154 rules and nearly 500 pages of in-depth commentary on how extant international law applies in the cyber context. Since the manual's publication, there has been a flood of scholarship on the subject.

At the governmental level, states have been active since 2004 in a series of U.N. Groups of Governmental Experts focused on information and communications technology. Three reports have been issued, the most significant of which was the Group of Governmental Experts consensus report of 2015. Endorsed by the U.N. General Assembly, the report included a short catalogue of international law rules and principles that the participating states agreed applied to cyber activities, as well as "voluntary, non-binding norms of responsible state behavior" in cyberspace.[9] And, there are presently two parallel U.N. processes underway: a sixth Group of Governmental Experts iteration and an Open-Ended Working Group. The former consists of representatives from 25 states, while the latter is open to all states.[10] Clearly, cyberspace has taken center stage in international fora.

Just as importantly, individual states are beginning to publicly express their views on the subject. Two statements on international law appended to *Australia's International Cyber Engagement Strategy*,[11] a letter on international law in cyberspace from the Dutch Ministry of Foreign Affairs to Parliament,[12] a report on the issue released by the French Ministry of the Armies,[13] and a discussion by states of their views during an Open-Ended Working Group session in February 2020[14] rank among the most noteworthy statements issued on cyber operations and international law.

Given the rising threat of hostile cyber operations, the importance of cyberspace to 21st-century societies, and the ongoing efforts to identify how international law applies in the cyber context, it is an appropriate moment to assess the prospects for international cyber law's continued development. Some evolution in the applicable law is inevitable, for normative architecture must remain responsive to the context in which it applies if it is to be effective. And, the nature of that context is clear — the reliance of states and societies on cyberspace will continue to grow at a rapid pace while cyberspace will become an ever more dangerous environment in which to operate. The more that states rely upon cyberspace for essential functions, day-to-day activities, and well-being, the starker their strategic choice becomes regarding the evolutionary vector of international law. Moreover, it will be a choice informed by the geopolitical priorities of states,

7 Thucydides, *History of the Peloponnesian War*, trans. John H. Finley (New York: Modern Library, 1951).

8 Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017).

9 2015 GGE Report, 7; U.N. General Assembly, "Developments in the field of information and telecommunications in the context of international security," Resolution 70/237, Dec. 30, 2015, https://undocs.org/en/A/RES/70/237. See also, the earlier report, U.N. Secretary-General, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc. A/68/98*, June 24, 2013, https://digitallibrary.un.org/record/753055?ln=en [hereafter 2013 GGE Report].

10 United Nations Officer for Disarmament Affairs, "Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security," July 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.

11 Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy,* Oct. 2017, 90-1, https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf; Australia's International Cyber Engagement Strategy, "2019 International Law Supplement," https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html.

12 The Netherlands, Ministry of Foreign Affairs, "Letter of 5 July 2019 from the Netherlands Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, and Appendix: International Law in Cyberspace," 2019 [hereafter Netherlands MFA Letter], https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

13 Republic of France, Ministry of the Armies, "International Law Applied to Operations in Cyberspace," 2019, [hereafter Ministry of the Armies Position Paper], 6-7, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

14 United Nations, UN Web TV, "Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Second Substantive Session," Feb. 10–14, 2020 [hereafter OEWG], http://webtv.un.org/search/3rd-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-second-substantive-session-10%E2%80%9314-february-2020/6131646836001/?term=%22Open%20Ended%20Working%20Group%22&lan=English&cat=Meetings%2FEvents&sort=date.

particularly whether they see international law as either supporting or impeding the achievement of those priorities.

To gauge the manner in which international law is likely to evolve, this article first evaluates how normative evolution is likely to occur. There are three possibilities: new treaty law, new customary law, and interpretation of extant rules of international law. Interpretation is likely to occupy most of the normative effort. Second, this article lays out the legal-strategic options open to states in approaching law's evolution. States are at a crossroads in that regard. Their attitudes toward the efficacy of international law in safeguarding their cyberspace determine the path they take. Lastly, this article assesses the general vector of international law's evolution with respect to cyberspace. A trend is emerging — one that acknowledges the power of international law rules to hamper harmful cyber operations.

The Means of Normative Evolution

To remain responsive to the realities of transnational cyber activities, international law rules can develop in one of three ways — through treaties, new customary law, or interpretation of existing law (or a combination thereof). A new treaty governing cyberspace appears unlikely, at least on a global scale. Although Russia has recently secured support in the United Nations for considering this possibility and proffered a draft instrument on cyber crime[15] (despite the existence of the Budapest Convention, which has nearly 70 parties, on the same subject[16]), the move has faced widespread opposition.[17] Typical of the response of many states was Australia's observation at an Open-Ended Working Group session in February 2020:

> A legally binding instrument in this space would take years to negotiate. It would likely end up with the lowest common denominator result and offer less protection than we currently have with the existing framework. Having a treaty would also not solve the question of how it would apply. We would still be left with the question of how to interpret it.[18]

Cynicism about the motives behind the Russian proposal is rife, with concern that it is a subterfuge designed to limit the reach of international human rights law — particularly the rights to privacy and expression — into those states that support it. Such concern is well founded.

Complicating matters is the current international political landscape. A treaty restricting cybercrime would require international cooperation. Unfortunately, since 2016, the United States has demonstrated a hostile attitude towards multilateralism and has proven wary of limiting its own actions through international agreements. Even if this obstacle could be overcome, philosophical disagreement exists over what and how to regulate. This fact is evidenced by the conflict between the concepts of "cyber security" championed by liberal democracies and so-called "information security" supported by China and Russia. Whereas the former generally support the free flow of information, the latter seek to exert control over content. To illustrate, Russia and China have refused to participate in the Budapest Convention, in part because it cedes a degree of control over digital information that each state would otherwise enjoy.[19]

"Crystallization" of new norms of *customary* international law is likewise unlikely. Customary international law consists of rules that are not found in a treaty but are nevertheless widely acknowledged to be binding for states despite being unwritten.[20] For instance, even though the United States is bound by no treaty provision that prohibits conducting attacks against civilians by kinetic or cyber means during an armed conflict, it recognizes that customary law prohibits such attacks.

Crystallization requires a sufficient degree of state practice over time combined with a belief that the practice is engaged in — or refrained from —

15 U.N. General Assembly, "Countering the use of information and communications technologies for criminal purposes," Resolution 74/247, Dec. 27, 2019, https://undocs.org/en/A/RES/74/247; Draft United Nations Convention on Cooperation in Combating Cybercrime, Russia, 2017, Annexed to U.N. General Assembly, "Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General," UN Doc. A/C.3/72/12*, Oct. 16, 2017, https://undocs.org/A/C.3/72/12.

16 Council of Europe, "Convention on Cybercrime," European Treaty Series No.185, Nov. 23, 2001, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

17 "Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online," *Association of Progressive Communications*, Nov. 2019, https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human.

18 See, OEWG.

19 See, e.g., Council of Europe, "Convention on Cybercrime," 17-18.

20 As an example, the United States is bound by no treaty prohibiting cyber attacks against the civilian population during an armed conflict, but nevertheless acknowledged that it is bound by an unwritten customary international law rule to that effect. "Department of Defense: Law of War Manual," 1020-1021.

out of a sense of legal obligation.[21] Satisfying these conditions with respect to cyber operations is unlikely in the near future for a number of reasons. Most state cyber operations are highly classified or otherwise shielded from observation by other states. Practice that is not visible does not contribute to the crystallization of a new customary law. Additionally, states have shown a general reluctance to engage in the verbal practice that might suffice to fill that void. For example, they have seldom condemned the cyber operations of other states as violations of international law.

Most state cyber operations are highly classified or otherwise shielded from observation by other states. Practice that is not visible does not contribute to the crystallization of a new customary law.

Along the same lines, statements by states setting forth the belief that the state practice is required by international law — the second condition for crystallization of a new norm — are rare. Those that have been offered deal solely with the *interpretation* of existing norms in the cyber context. In addition, these interpretations tend to be broad, as with the U.S. acknowledgement in 2016 by the former State Department legal adviser that "cyber operations conducted by non-State actors are attributable to a State under the law of state responsibility when such actors engage in operations pursuant to the State's instructions or under the State's direction or control."[22] Such statements seldom delve into the gritty details of how to apply the rules in practice.

In part, the unwillingness of many states to articulate their legal positions with regard to cyberspace is due to the principle of sovereign equality, by which any customary law norm that crystallizes binds all states. Thus, states are likely to be torn between acceptance of a new norm that constrains other states and acquiescence to restraints on their own cyber operations. The rapid pace of advances in cyber technology along with uncertainty as to how it will be employed in the future reinforce their hesitancy. It is unclear whether there are advantages to be gained by accepting constraints on cyber capabilities that may become more useful at a later date. This reality results in disagreement at the interagency level between departments and organizations responsible for defending against hostile cyber operations and those tasked with conducting cyber operations in the territory of other states in pursuit of their own state's national interests. In the face of such impediments, the requisite articulation of legal views that is necessary for the crystallization of new norms is unlikely to develop in the foreseeable future.

Of course, the same realities plague the *interpretation* of existing rules of international law. However, as these rules already exist, there is greater incentive for states to interpret them in a manner that sets normative precedents, lest other states seize the interpretive high ground by establishing interpretations that serve their specific interests. Some states have wisely recognized that, even though they may not be able to reliably predict future cyber technologies and practices, their national interests are best served by trying to shape the normative environment. This is where most of the normative activity regarding cyberspace will take place over the mid-term.

States will continue to play the key role in this interpretive journey. For example, the work of the U.N. Groups of Governmental Experts, which are comprised of state representatives and the reports of which are endorsed by other states in the U.N. General Assembly, remains at the forefront of this effort. There is, however, a noticeable tendency toward regional fragmentation among states and collaboration among like-minded states. For instance, although not binding law, most efforts to craft confidence-building measures have been regional, as in the case of the Organization for Security and Cooperation in Europe, the Organization of American States, and the Association of Southeast Asian Nations. While like-minded efforts are especially pronounced among the so-called "Five Eyes" (the United States, Canada, the United Kingdom, Australia, and New Zealand), there is frequent norm collaboration between Russia and China because of their shared objective of control over their populations.

Non-state actors also have been active in the in-

21 United Nations, International Law Commission, "Draft Conclusions on Identification of Customary International Law, with Commentaries," UN Doc A/73/10, 2018, https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf.

22 Brian J. Egan, "Remarks on International Law and Stability in Cyberspace," *U.S. Department of State Archive*, Nov. 10, 2016, https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf.

terpretive effort, as well as in the articulation of voluntary, non-binding norms. They enjoy greater normative agility than states because they can focus on objective interpretation without the intrusion of national policy concerns. More to the point, cyberspace is a multi-stakeholder domain. Companies such as Microsoft wield as much power in cyberspace as most states while the economic impact of cyber activities conducted by companies like Amazon is huge.

As a result, certain non-state activities are exerting significant influence on the interpretive process, which is certainly the case with respect to the *Tallinn Manual 2.0* as it continues to serve as the primary reference point for how international law applies in cyberspace. Other efforts have also captured global attention, including Microsoft's Digital Geneva Convention and the establishment of the CyberPeace Institute. Indeed, states and non-state actors have been working together to examine norms for cyberspace, as is the case with Paris Call and the Global Commission on the Stability of Cyberspace.

The positive influence of such endeavors is apparent, for they operate to discredit the false narrative that cyberspace is a norm-less void. However, the development, interpretation, and implementation of international law remain primarily state-centric activities. The positions and interests of states indicate the likeliest vector of international law in cyberspace. Although it is still early, the outlines of that vector are slowly taking shape.

Strategic Options

States taking part in this interpretive venture are facing a crossroads. They can either choose a liberal interpretation of existing laws or restrict their freedom by adopting narrower or more limited interpretations of those laws. Both paths respond to the reliance on cyberspace by states and their populations that is growing at a dizzying rate.

On one hand, states may see international law as a valuable tool in combating hostile cyber operations. By this view, law deters harmful cyber activity conducted by or attributable to states because it allows the international community to condemn bad actors. The approach operates on the premise that states do not want to be seen as violating international law. There is ample evidence that this is so, for most states endeavor to style their actions as complying with international law even when they clearly do not — as in the case of Russian activities in Ukraine. For states that have adopted the approach, international law rules serve as normative firewalls; their corresponding legal strategy is to strengthen those firewalls.

Its advocates are, therefore, likely to pursue clarity in the rules and seek interpretive consensus. They believe that greater clarity prevents malicious state actors from exploiting potential ambiguity.[23] The U.S. response to election meddling by Russia in 2016 provides an example of this belief. Russia cleverly operated in the gray zone of international law with respect to the two rules its operations implicated; the obligation to respect the sovereignty of other states and the prohibition on intervention into other states' internal affairs. This hobbled the American response.[24] Greater clarity in the applicable international law rules would have provided Russia with less room to maneuver.

Clarity can also prevent unintended escalation. Consider a cyber operation causing effects lying in the gray zone of an ambiguous threshold, such as that at which territorial sovereignty is violated.[25] The state launching the operation believes that it did not cross the threshold, but the target state interprets the rule as having a lower threshold and, therefore, considers the first state's operation to be unlawful. As a "countermeasure," a response that is only permissible against an unlawful cyber operation,[26] the target state launches a hack that disables the cyber infrastructure of its adversary. Believing the response marks an escalation to unlawful operations, the first state mounts its own countermeasure. As this scenario illustrates, knowing where the normative red lines lie and having clarity as to the potential consequence under international law of crossing them has the potential to minimize escalatory misunderstandings.

But, on the other hand, states may logically conclude that normative firewalls are counterproductive and, as a result, may work towards keeping them low. They might even intentionally foster normative ambiguity. Two motives underlie this legal strategy. First, states that exploit ambiguity with re-

23 I discuss this dynamic more fully in Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law Online* 42, no. 2 (2017): 1-21, https://ssrn.com/abstract=3180687.

24 See my analysis at Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law* 19, no. 1 (2018): 30-67, https://chicagounbound.uchicago.edu/cjil/vol19/iss1/2/.

25 See discussion in Schmitt, *Tallinn Manual 2.0*, 18-26.

26 "Report of the International Law Commission on the work of its fifty-third session," U.N. Doc. A/56/10, 2001 [hereafter *Articles on State Responsibility*], 32-33, https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf.

spect to how international law rules apply in the cyber context will oppose clarification, for ambiguity affords them an advantage. This observation is particularly true of states that do not respect the rule of law when conducting operations against states that do, the so-called "rule of law states." The former understand that rule of law states will take a cautious approach in the face of gray zone operations as they struggle to determine whether the operations they face are unlawful, and can be condemned as such, as well as whether they open the door to options that are only available in response to internationally wrongful acts like countermeasures.

Second, rule of law states with a realist perspective on international relations might conclude that clarity gives adversaries that ignore legal strictures an asymmetrical advantage, for clear legal lines will — in practice — only limit the former's operational flexibility. They are a one-way normative firewall. By embracing ambiguity, rule of law states can retain the operational flexibility necessary to pick and choose how to characterize their opponents' cyber operations and determine when they have a right under international law to respond. They can beat their opponents at their own game. It is a rational, albeit internationally destabilizing, approach.

The Substantive Rules

It is instructive to look at how states are approaching a number of key international law rules. Although only a few states have publicly set forth their views, those views are representative of trends that are apparent across a wide range of states. States are embracing international law rules rather than ambiguity; they see normative firewalls both as protection against hostile cyber operations and as providing legal justification when they need to respond robustly to such operations.

Sovereignty

An ongoing debate over sovereignty in cyberspace is perhaps the most revealing indicator of the strategic direction in which states are moving with respect to interpreting international law. The International Group of Experts that published the *Tallinn Manual 2.0* concluded that remotely conducted cyber operations can violate the sovereignty of the state into which they are conducted — the target state — on the basis of either territorial inviolability or interference with, or usurpation of, an inherently governmental function.[27]

For the International Group of Experts, a violation of territoriality occurs when certain effects of the cyber operation manifest on the territory of the target state, whether on the government's cyber infrastructure or that of private entities. Qualifying effects include physical damage, injury, and the relatively permanent loss of functionality of the targeted cyber infrastructure — or of infrastructure that relies upon it. By contrast, a sovereignty violation based on interference with, or usurpation of, an inherently governmental function requires no particular physical effects. For example, conducting an operation that even temporarily disables election machinery, thereby affecting the vote count, would qualify as a violation based on territoriality, whereas a remote search of databases on another state's territory would illustrate the usurpation of an inherently governmental act, law enforcement.

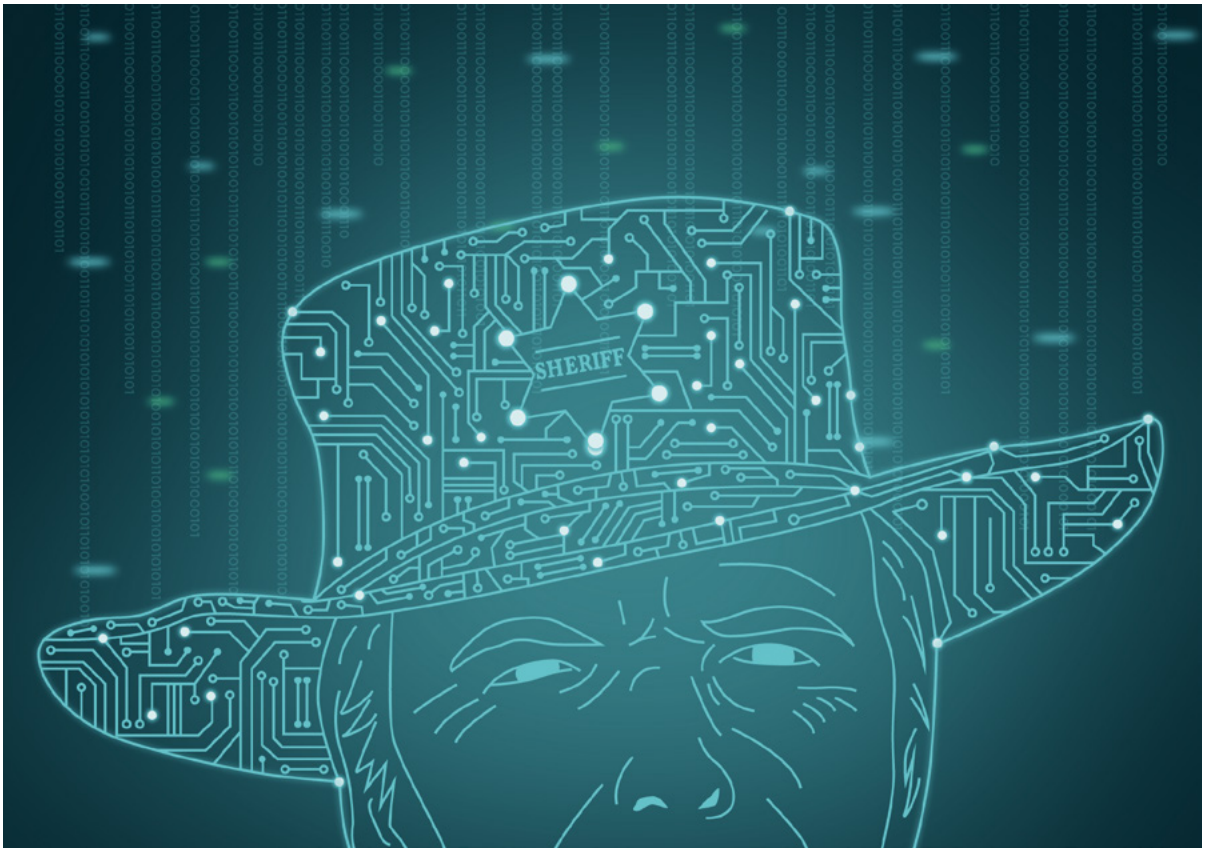
Following the publication of the *Tallinn Manual 2.0*, observers expected significant debate over how sovereignty could be violated short of causing damage or injury as well as over which functions qualify as inherently governmental. That important debate was sidetracked in May 2018 by the United Kingdom's articulation of a view that sovereignty is a principle of international law from which rules like the prohibitions on intervention and the use of force derive — but that is not a rule in itself.[28] In other words, remotely conducted cyber operations into the territory of other states never amount to an internationally wrongful act on the basis of having violated sovereignty.

The premise that there is no rule of sovereignty flies in the face of extensive practice by states and international organizations over many decades, as well as judicial pronouncements by the International Court of Justice and domestic courts.[29] It also runs counter to the first of the strategic approaches, which holds that international law has protective value. This fact provoked a quick reaction from other states. In the aforementioned July 2019 letter to Parliament, the Dutch Ministry of Foreign Affairs confirmed, accurately as a matter of law, that "Respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an interna-

27 See, Schmitt, *Tallinn Manual 2.0*, 11-26.

28 See, Wright Address.

29 See, Michael Schmitt and Liis Vihul, "Respect for Sovereignty in Cyberspace," *Texas Law Review* 95 (Nov. 3, 2017): 1639-1670, https://ssrn.com/abstract=3180669.



tionally wrongful act."[30] In other words, sovereignty is a rule of law having prescriptive effect. That the statement came from a NATO ally that is a generally like-minded state is of particular significance as a (deserved) rebuke to the British position.

The most robust pushback, however, came from France, which not only rejected the British position but has set forth its own position on when it will deem a cyber operation a violation of French sovereignty:

> Any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty.[31]

This French position describes an extremely low threshold of violation, albeit one that is defensible. Moreover, it defines *any* cyber attack against French digital systems, which presumably signifies government systems, *or* the causation of effects, which would extend to not only private cyber infrastructure but also knock-on effects more broadly, as a violation of sovereignty.

Other states are beginning to announce their views. For instance, at the February 2020 session of the Open-Ended Working Group, Switzerland, Austria, and the Czech Republic supported the "sovereignty-is-a-rule" approach that had been adopted by the Netherlands and France.[32] To date, no state has adopted the British view. Even the United States has hedged its bets. At an address during the U.S. Cyber Command annual conference in March 2020, Department of Defense General Counsel Paul Ney noted,

> As a threshold matter, in analyzing proposed cyber operations, DoD lawyers take into account the principle of State sovereignty. States have sovereignty over the information and communications technology infrastructure within their territory. The implications of sovereignty for cyberspace

30 Netherlands MFA Letter, 2.

31 Ministry of the Armies Position Paper, 7.

32 OEWG, fourth session. The Czech approach was especially broad, including in addition to the standard territorial integrity and inherently governmental function violations, "a cyber operation causing damage to, or disruption of, cyber or other infrastructure with significant impact on national security, economy, public health or environment."

> are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law.[33]

A careful parsing of Ney's statement reveals that it is not inconsistent with the views of those supporting sovereignty as a rule. For instance, sovereignty advocates do not claim that all remotely conducted cyber operations violate sovereignty. Ney's reference to the phrase "necessarily involve" suggests that there are cyber operations that will violate sovereignty. That the United States is "continuing to study" the issue and watching state practice indicates that it is leaving open the prospect of joining the sovereignty-is-a-rule group — a move that would force the United Kingdom to rethink its legally implausible position.

Finally, it is important to note that both Russia and China are strong supporters of sovereignty, although their motive is to use the principle as the basis for controlling the cyber activities of people within their territories and of their nationals abroad. In doing so, they are overemphasizing the significance of sovereignty by failing to pay adequate heed to the fact that the enjoyment of sovereignty must be exercised without prejudice to international human rights law. But, their approach does signal the influence of the rule and the extent to which states view it as having protective value for their interests — malign though those interests may be.

Intervention

Interestingly, interpretive discussions regarding the prohibition on intervention into the internal or external affairs of other states, which is universally accepted as a rule,[34] has recently tended to focus on how to accommodate the normative void that would be created by dispensing with the rule of sovereignty.

It is well accepted that a violation of the prohibition on intervention requires two elements: that the object of the intervention involves an area of activity that international law leaves to the state (the so-called internal or external affairs of a state) and that the action be coercive in nature.[35] As explained by the Australian Department of Foreign Affairs and Trade in its *International Cyber Engagement Strategy*,

> A prohibited intervention is one that interferes by coercive means (in the sense that they effectively deprive another state of the ability to control, decide, or govern matters of an inherently sovereign nature), either directly or indirectly, in matters that a state is permitted by the principle of state sovereignty to decide freely. Such matters include a state's economic, political, and social systems, and foreign policy.[36]

The term "internal or external affairs" is often misunderstood as referring to the target of a cyber operation. However, the concept actually refers to the area of activity that the state conducting the operation hopes to coerce. For instance, the WannaCry operation by North Korea impacted the United Kingdom's health sector, but as a ransomware attack it was not designed to coerce any change in U.K. health policy or delivery. By contrast, some of the cyber operations related to the novel coronavirus pandemic, if attributable to a state, would amount to intervention. An example would be the malicious cyber operations that disabled a novel coronavirus testing facility in the Czech Republic. These attacks made it impossible for that state to fully execute its crisis management plan for dealing with the pandemic.[37]

In terms of trend analysis, the fact that the prohibition's existence is uncontroversial supports the premise that law serves a valuable protective function. What has been particularly noteworthy is the tendency of those who question sovereignty — or are concerned about the weakening of the rule — to look to the rule prohibiting intervention to fill any protective gaps that would be left by the absence of

33 Paul C. Ney, Jr., "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," *U.S. Department of Defense*, Mar. 2, 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/. See my analysis of the speech in Michael N. Schmitt, "The Defense Department's Measured Take on International Law in Cyberspace," *Just Security*, Mar. 11, 2020, https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/.

34 2015 GGE, 12-13. On the prohibition generally, see, Schmitt, *Tallinn Manual 2.0*, 312-324.

35 International Court of Justice (ICJ), Reports of Judgements, Advisory Opinions and Orders, "Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua. v. United States of America)," June 27, 1986, 14, 97-98, https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

36 See, Australia's International Cyber Engagement Strategy, "2019 International Law Supplement."

37 On the COVID-19-related hostile cyber operations and international law, see, Marko Milanovic and Michael N. Schmitt, "Cyber Attacks and Cyber (Mis)information Operations during a Pandemic," *Journal of National Security Law & Policy* (forthcoming, published on-line May 28, 2020), https://dx.doi.org/10.2139/ssrn.3612019.

a rule of sovereignty.[38] This could be accomplished by either relaxing the scope of the term "internal or external affairs" through interpretation or by lowering the threshold at which an attempt to influence becomes unlawful coercion.[39] With respect to the former option, "internal or external affairs" could be interpreted more broadly to include the target of the cyber operation and not just the activity or policy that the state conducting the cyber operation hopes to coerce. If this were to be done, operations like WannaCry would qualify as intervention. Indeed, in the same Chatham House speech in which he rejected sovereignty, the U.K. attorney general adopted this approach: "Acts like the targeting of essential medical services are no less prohibited interventions, or even armed attacks, when they are committed by cyber means."[40]

Most discussion within the international law community, however, centers on the element of coercion, as was the case at a May 2020 workshop held by the University of Oxford's Institute for Ethics, Law and Armed Conflict.[41] Advocates of lowering the threshold at which mere influence becomes unlawful coercion, thereby satisfying the second element of intervention, argue that a hostile cyber operation should not necessarily have to deprive a state of all reasonable choice, so long as it renders making the choice difficult. The problem is that, as a result, applying the rule becomes more challenging because "no reasonable choice" is an easier threshold to apply than "making the choice difficult." Interpretive creativity is simply no panacea for weakening the impact of sovereignty. But, the point to be made is that both states and international law experts — faced with one key state's rejection of the sovereignty rule — are working hard to find a way to interpret international law so as to retain its protective effect.

Due diligence

Also indicative of the trend toward viewing international law as an effective normative firewall against hostile cyber operations is the growing tendency of states to embrace the rule of due diligence. This rule requires states to put an end to hostile cyber operations by other states or non-state actors that are mounted either from within or through their territory when the operations affect a legal right of another state and cause serious adverse consequences.[42] For instance, if a hacktivist group is launching cyber operations from one state against another state's government systems, the first state would be required to take all feasible measures to terminate the operations. Such measures could range from law enforcement to a technical solution.

What does appear clear is that states support the notion that members of the international community have a responsibility to ensure their territory is not used as the base of hostile cyber operations.

Although the due diligence rule was set forth by the International Court of Justice in its first case, *Corfu Channel*,[43] and appears prominently in various specialized bodies of law (most notably international environmental law[44]) states have been hesitant to acknowledge its existence. Some states appear concerned that the burden of compliance would be onerous given the number of hostile cyber operations that are mounted from within their territory. For instance, the obligation was set forth as a voluntary non-binding norm in both the 2013 and 2015 Group of Governmental Experts reports because the consensus to characterize it as a bind-

38 On the relationship between sovereignty and intervention, see, Harriet Moynihan, "The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention," Chatham House Research Paper, December 2019, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf.

39 Indeed, in his speech Attorney General Wright asserted that "The precise boundaries of this principle are the subject of ongoing debate between states, and not just in the context of cyber space." See, Wright Address.

40 Wright Address.

41 The author was in attendance.

42 For a discussion of due diligence, see Schmitt, *Tallinn Manual 2.0*, 30-50.

43 International Court of Justice, Reports of Judgements, Advisory Opinions and Orders, "The Corfu Channel Case (Merits)," April 9, 1949, 22, https://www.icj-cij.org/files/case-related/1/001-19490409-JUD-01-00-EN.pdf.

44 U.N. Conference on Environment and Development, "Rio Declaration on Environment and Development," U.N. Doc. A/CONF.151/26/ (Vol. I), Aug. 12, 1992, 1, https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_CONF.151_26_Vol.I_Declaration.pdf.

ing norm in either report could not be achieved.[45]

However, as states have become aware of the numerous limitations that are placed on the due diligence obligation,[46] particularly the absence of any requirement to take preventive measures and an obligation only to take measures that are feasible in the circumstances, they are beginning to accept the rule. For instance, both the Netherlands and France did so in 2019 and Finland took a very expansive view of the obligation at the February 2020 session of the Open-Ended Working Group.[47] The most interesting statement to date has come from Australia, which seemed to straddle the fence in its *International Cyber Engagement Strategy*. On the one hand, it observed, "To the extent that a state enjoys ... sovereignty over objects and activities within its territory, it *necessarily* shoulders corresponding responsibilities to ensure [they] are not used to harm other states." This language is that of binding rules. But, Australia went on to enumerate the requirements as if it was a voluntary, non-binding norm using the term "should": "[I]f a state is aware of an internationally wrongful act originating from or routed through its territory, and it has the ability to put an end to the harmful activity, that state *should* take reasonable steps to do so consistent with international law."[48]

Other states — such as Germany, Estonia, Finland, the Republic of Korea, and Spain — have also supported the rule's binding nature in various official and unofficial fora, while no state has publicly rejected the rule as such. Rather, states that are unwilling to acknowledge the rule's binding character generally take the position that it has not yet matured to that level and, therefore, may only be put forward as a voluntary, non-binding norm. What does appear clear is that states support the notion that members of the international community have a responsibility to ensure their territory is not used as the base of hostile cyber operations. The growing number of states that accept the rule as "hard law" is further indication of a trend towards treating international law as an effective tool in deterring harmful cyber activities.

Use of force

This trend is augmented by the tendency of states to view international law as a normative barrier against unlawful uses of force. All states agree that the prohibition on the use of force, resident in Article 2(4) of the U.N. Charter and customary law, is a binding rule of international law applicable to cyber operations.[49] Indeed, the 2015 Group of Governmental Experts report specifically "identified as of central importance the commitments of States to the following principles of the Charter and other international law ... refraining in their international relations from the threat or use of force."[50] The report was subsequently endorsed by the General Assembly.[51]

Clearly, a cyber operation that causes significant physical damage or injury qualifies as a use of force. As with sovereignty, the notion of functional damage was adopted as the equivalent of physical damage for the purposes of this prohibition. Interestingly, no state has opposed this interpretation — one which would apply almost exclusively in the cyber context.

More importantly, a number of states have accepted the International Group of Experts' adoption of the "scale and effects" test from the law of self-defense for evaluating cyber operations that do not cause such effects with respect to the prohibition on the use of force.[52] The International Group of Experts held that the prohibition extended beyond physical damage (including the relatively permanent loss of functionality) or injury and that certain factors would influence states when assessing whether a particular cyber operation qualifies as a use of force. It identified a number of non-exhaustive factors that states were likely to consider when making that determination. The list included severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, presumptive legitimate legality, identity of the attacker, record of cyber operations by the attacker, and nature of the target.[53]

45 2013 GGE Report, 8; 2015 GGE Report, 8.

46 See my thoughts in this regard in Michael N. Schmitt, "In Defense of Due Diligence in Cyberspace," *125 Yale Law Journal Forum 68* (2015), https://ssrn.com/abstract=2622077.

47 Netherlands MFA Letter, 4-5; Ministry of the Armies Position Paper, 10; Statement of Finland, in OEWG, at third meeting. Finland suggested, "If harmful cyber activities take place and cause serious harm to another state, the state of origin must take appropriate action to terminate it, as well as to investigate the incident and bring those responsible to justice."

48 *Australia's International Cyber Engagement Strategy*, 91. Emphasis added by author.

49 UN Charter art. 2(4). See also, Schmitt, *Tallinn Manual 2.0*, 329-30.

50 2015 GGE Report, 12.

51 U. N. General Assembly, "Developments in the field of information and telecommunications," Resolution 70/237, Dec. 23, 2015.

52 ICJ, "Case Concerning Military and Paramilitary Activities," 103-104.

53 Schmitt, *Tallinn Manual 2.0*, 331-337.

Along the same lines, the Netherlands took the position in 2019:

> It is necessary … to examine both qualitative and quantitative factors. The *Tallinn Manual 2.0* refers to a number of factors that could play a role in this regard, including how serious and far-reaching the cyber operation's consequences are, whether the operation is military in nature and whether it is carried out by a state.[54]

The Netherlands went on to address the oft-asked question of whether a non-destructive cyber operation against the economy could ever qualify as a use of force: "At this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force."[55] This view is a significant indicator of the extent to which the Netherlands, which is a thought leader in the field, treats international law as protective in the cyber context.

And, the Netherlands is not alone. The same year, France noted:

> In the absence of physical damage, a cyber-operation can be considered use of force in the light of several criteria, … such as the origin of the operation and the nature of the instigator (military or non-military), the degree of intrusion, the effects caused or sought by the operation, or the nature of the target. These criteria are, of course, not exhaustive. For example, penetrating military systems with a view to weakening French defense capabilities, or to finance or train individuals so that they can perpetrate cyberattacks against France could well qualify as the use of force.[56]

With respect to economic damage, France went even further than the Netherlands: "A cyberattack could be categorised as an armed attack if it caused substantial loss of life or considerable physical or economic damage."[57] The reference to "armed attack" — the threshold for using force in self-defense — is particularly telling, for most states have adopted the position set forth by the International Court of Justice in its *Nicaragua* judgment that an "armed attack" is the "most grave form" of a use of force.[58]

Overall, there are strong indications that states would like to see normative barriers against the use of force go up in order to protect their cyber assets and activities. This desire has been signaled by the lack of any opposition to the functionality approach, the adoption of the scale and effects test for non-physical effects, and the indication by some states that even cyber operations solely affecting the economy could amount to an unlawful use of force — a prohibition that had heretofore been primarily restricted to operations that caused physical damage or injury, or, as in the *Nicaragua* case, activities in support of operations having those effects.[59] Thus, the trend with respect to the use of force tracks all that appears to be emerging with regard to other internationally wrongful acts, including violation of sovereignty, intervention, and the failure to exercise due diligence.

Responses

Interestingly, normative barriers to *response* options may be lowering. States want international law to not only shield them from hostile cyber operations but also allow them to engage in robust cyber responses that they deem necessary to protect themselves. They look to so-called "circumstances precluding wrongfulness" to achieve this objective. Circumstances precluding wrongfulness allow a state to conduct cyber or non-cyber operations that would otherwise be unlawful. They render unlawful acts — which may include actions or omissions — lawful.

Consider "countermeasures": responses to unlawful cyber operations that themselves would be unlawful except for the fact that they are designed to compel another state (the "responsible state") into desisting in its unlawful course of conduct and providing the "injured state" whatever reparations might be due.[60] Most states appear to accept the legality of countermeasures and have shown a willingness to adapt their use to the cyber context.

54 Netherlands MFA Letter, 4. See also, *Australia's International Cyber Engagement Strategy*, 90: "In determining whether a … cyber activity, constitutes a use of force, states should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force."

55 Netherlands MFA Letter, 4.

56 Ministry of the Armies Position Paper, 7.

57 Ministry of the Armies Position Paper, 8.

58 ICJ, "Case Concerning Military and Paramilitary Activities," 101-102.

59 ICJ, "Case Concerning Military and Paramilitary Activities," 118-119.

60 *Articles on State Responsibility*, 75-76, 129-139; Schmitt, *Tallinn Manual 2.0*, 111-5.

There are other indications that states are uncomfortable with stringent limitations on their right to self-defense in cyberspace.

This approach is best illustrated with respect to the purported "notice" requirement.

The U.N. International Law Commission's *Articles on State Responsibility* suggest that a state should normally provide notice of its intention to engage in countermeasures.[61] Nevertheless, states have repeatedly emphasized that the requirement of notice in the cyber context is tempered by the urgency of the need to respond. For example, France has taken the position that:

> The victim State may, in certain circumstances, derogate from the obligation to notify … where there is a need to protect its rights. This possibility of adopting urgent countermeasures is all the more appropriate in cyberspace given the predominance of concealment and traceability difficulties.[62]

Similarly, the Netherlands has noted that, "if immediate action is required in order to enforce the rights of the injured state and prevent further damage, such notification may be dispensed with."[63] Cyber operations can unfold in a fraction of a second. Interpreting the rule as requiring notice of countermeasures in every case would be impractical.

The most progressive position in this regard was set forth by the United Kingdom in 2018. In his speech at Chatham House, the attorney general observed, "We would not agree that we are always legally obliged to give prior notification … it could not be right for international law to require a countermeasure to expose highly sensitive capabilities."[64] The formulation is significant. Whereas other countries focus on the urgency of the need to take countermeasures and the impracticality of providing notice, the British approach tenders the preservation of highly classified cyber capabilities as further justification.

Also indicative of the trend towards interpreting international law in a manner that allows for effective responses to hostile cyber operations is an emerging discussion of collective countermeasures. In its commentary accompanying the *Articles on State Responsibility*, the International Law Commission noted that cases of countermeasures by an entity other than an injured state are "controversial and the practice is embryonic,"[65] leading to the prevailing view that they are impermissible. Yet, in 2019, Estonian President Kersti Kaljulaid asserted that:

> states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation … International security and the rules-based international order have long benefitted from collective efforts to stop the violations.[66]

This position is sensible for states that may lack the wherewithal to mount effective countermeasures against hostile cyber operations on their own. To date, only France has openly disagreed with the Estonian position, albeit without explaining the basis for its opposition.[67]

Most noteworthy vis-a-vis responses falling below the threshold of armed attacks, which allows for the use of cyber or non-cyber force in self-defense, is the current U.S. approach. According to the U.S. Department of Defense's 2018 *Cyber Strategy*, U.S. forces intend to "[p]ersistently contest malicious cyber activity in day-to-day competition: The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats."[68] Although not framed in legal terms, such a strategy would be difficult to square with a restrictive interpretation of the right to take countermeasures like the one that suggests advance notice of the intent to take countermeasures is required as a matter of law.

---

61 *Articles on State Responsibility*, 119-120, 135-137. The Articles are not binding law themselves, but are widely viewed as accurately reflecting customary international law in most part.

62 Ministry of the Armies Position Paper, 8.

63 Netherlands MFA Letter, 7. See also the submission of the United States to the 2014-2015 GGE, "Applicability of International Law to Conflicts in Cyberspace," in CarrieLyn D. Guymon, ed., *Digest of United States Practice in International Law* (2014), 732, 739, https://2009-2017.state.gov/documents/organization/244504.pdf: "[the State] generally must call upon the responsible State to cease its wrongful conduct, unless urgent countermeasures are necessary to preserve the injured State's rights."

64 Wright Address.

65 *Articles on State Responsibility*, 129.

66 Office of the President, Estonia, "President of the Republic at the Opening of CyCon 2019," May 29, 2019, https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/.

67 Ministry of the Armies Position Paper, 7.

68 Department of Defense, "Summary: Cyber Strategy," 2018, 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF%20. See also, The White House, "National Cyber Strategy of the United States," Sept. 2018, 20-21, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

States have also discovered the "plea of necessity," which seldom drew attention prior to the advent of cyber operations. Like countermeasures, this plea is a circumstance precluding wrongfulness. It is available when a state is facing "grave and imminent peril" to an "essential interest" and no means of putting an end to that peril exists other than actions that would be considered unlawful under different circumstances.[69] Importantly, victim states can rely upon the plea of necessity when the otherwise unlawful response to a qualifying hostile cyber operation would violate a legal obligation owed to a state that had nothing to do with the grave and imminent peril. This distinction is especially significant, for, unlike countermeasures, states can turn to the plea of necessity to justify operations against non-state actors or in situations in which the identity of the attacker is unclear.

France has announced that it "does not exclude the possibility of invoking the state of distress to protect an essential interest against a cyberattack below the threshold of military aggression constituting a serious danger that is imminent."[70] And, while the precise parameters of the concepts of "grave," "imminent," and "essential interest" are unsettled, the Netherlands has suggested that, "in the government's view[,] services such as the electricity grid, water supply and the banking system certainly fall into this category."[71] Other states are likely to embrace the plea for crisis management purposes, for — again as noted by the Netherlands — "[t]his ground for justification is primarily aimed at giving a state the opportunity to protect its own interests and minimise the damage it suffers."[72]

The circumstance precluding wrongfulness that allows for the most robust response is an "armed attack" justifying a use of force in self-defense pursuant to Article 51 of the U.N. Charter and customary law.[73] A cyber operation that generates significant damage, destruction, injury, or death would surely qualify as an armed attack. However, as emphasized by the Netherlands, "At present there is no international consensus on qualifying a cyberattack as an armed attack if it does not cause fatalities, physical damage or destruction yet nevertheless has very serious non-material consequences."[74]

Again, France is a trailblazer in interpreting the norm. In 2019, it announced,

> A cyberattack could qualify as an armed attack when it causes substantial loss of life or significant physical or economic damage. This would be the case of an operation in cyberspace affecting critical infrastructure with significant consequences, or likely to paralyze whole sectors of the country's activity, to trigger administrative or ecological disasters and to cause many victims.[75]

In making this announcement, France became the first state to unequivocally take a view that the notion of an armed attack includes cyber operations that do not cause physical damage or injury at all. Rather, the approach focuses on the severity of an operation. This focus was a possibility that had been raised earlier by the Netherlands' minister of defense, although it does not explicitly appear in the most recent expression of Dutch views on how international law applies in cyberspace.[76]

There are other indications that states are uncomfortable with stringent limitations on their right to self-defense in cyberspace. Some have expressed the view that the right includes defense against cyber operations conducted by non-state actors if the operations cause consequences at the armed attack level. In these cases, self-defense against non-state actors can be conducted in another state's territory when the territorial state is "unable or unwilling" to take action against the operations. Some states have also taken the position that states are entitled to aggregate effects of a series of related hostile cyber operations to reach the severity threshold of self-defense.[77]

69 *Articles on State Responsibility*, 80-84.

70 Ministry of the Armies Position Paper, 8.

71 Netherlands MFA Letter, 8.

72 Netherlands MFA Letter, 8.

73 UN Charter Art. 51. See also, Schmitt, *Tallinn Manual 2.0*, 333-347.

74 Netherlands MFA Letter, 9.

75 Ministry of the Armies Position Paper, 8.

76 The Netherlands, Ministry of Defence, "Keynote Address by the Minister of Defence, Ms. Ank Bijleveld, Marking the First Anniversary of the Tallinn Manual 2.0," June 20, 2018, https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018.

77 See, e.g., "Applicability of International Law to Conflicts," 735; Wright Address; Netherlands MFA Letter, 9; Ministry of the Armies Position Paper, 9 (accumulation of effects).

For its part, even though France has rejected the premise that an armed attack can be conducted by a non-state actor with no affiliation to a state, it hedges its bets: "[I]t cannot be ruled out that general practice may shift towards an interpretation of the law of self-defence as being authorised in response to an armed attack by non-state actors whose acts are not attributable to a State."[78]

Finally, states are confirming that there is a right to anticipatory self-defense. Of particular note, Australia has taken the position that it may respond in self-defense when "the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts."[79] It points to the possibility of a threatened offensive cyber operation at the armed attack level that could "cause large-scale loss of human life and damage to critical infrastructure. Such an attack might be launched in a split-second … Is it seriously to be suggested that a state has no right to take action before that split-second?" Since no state in such a situation would likely hesitate to defend itself, the Australian interpretation is prescient.

In fairness, there are a few indicators that appear contrary to the broad trend towards ensuring international law is interpreted in a manner that allows leeway for victim state responses. For instance, there now appears to be a growing consensus that countermeasures must be "necessary" in the sense of there being no alternative to taking them to resolve the situation[80] and that they do not allow for the use of force.[81] Furthermore, some states still cling to a traditional interpretation of circumstances precluding wrongfulness, as France does with respect to collective countermeasures and self-defense against non-state actors. And, recall that Russia, China, and a number of other states were unwilling to mention the term "self-defense" or include text referring to countermeasures in the aborted final report of the 2016-2017 Group of Governmental Experts. But the interpretive vector certainly points in the direction of a liberal interpretation of circumstances precluding wrongfulness, signaling support for relying on international law as a viable and useful tool in the fight against hostile cyber operations.

Concluding Thoughts

It is clear that the prospects for *new* laws applicable to cyberspace are slim. Instead, most progress will come in the form of the *interpretation* of longstanding rules of international law, primarily by states. That interpretation is likely to be motivated by a prevailing perception that international law is a useful normative firewall against hostile cyber operations attributable to or launched from within other states. This approach is a laudatory one that will enhance stability and security in cyberspace.

Yet, there will be obstacles along the way. As noted, states sometimes cherry-pick amongst international law rules to suit themselves. To embrace certain rules of international law while rejecting others without a sound legal basis for doing so is to place the entire normative enterprise at risk. Moreover, some states will continue to profess fidelity to international legal norms while violating them with impunity — as is common with respect to international human rights law obligations. And, short-sighted tactics are impeding an interpretive journey that will benefit all members of the international community. Hopefully, governments will grasp the long-term costs of such strategies.

Nevertheless, there are reasons to be optimistic. The vector of the interpretive efforts in support of international law is clearly positive, and the scope and pace of such efforts are growing. Of greatest significance is the commitment of many states to ensuring that cyberspace becomes and remains a rule of law domain. Such states are to be commended.

Michael N. Schmitt *is a professor of international law at the University of Reading; Strauss Center distinguished fellow at the University of Texas; Francis Lieber distinguished scholar at the U.S. Military Academy at West Point; Charles Stockton distinguished scholar-in-residence at the U.S. Naval War College; and senior fellow with the NATO Cooperative Cyber Defence Center of Excellence. A version of this article is forthcoming as "The Law of Cyber Conflict: Quo Vadis 2.0?," in* The Future of Armed Conflict, *eds. Matthew Waxman and Thomas Oakley, (Oxford: Oxford University Press, 2021).*

Photo: Air Force photo J.M. Eddins, Jr.

78 Ministry of the Armies Position Paper, 9.

79 Australia's International Cyber Engagement Strategy, "2019 International Law Supplement;" see also, Schmitt, *Tallinn Manual 2.0*, 351-353.

80 "Applicability of International Law to Conflicts," 739; Wright Address.

81 "Applicability of International Law to Conflicts," 739; Wright Address; Australia's International Cyber Engagement Strategy, "2019 International Law Supplement;" Netherlands MFA Letter, 7; Ministry of the Armies Position Paper, 8.