From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers

Kubo Mačák*

Abstract

Several indicators point to a crisis at the heart of the emerging area of international cyber security law. First, proposals of internationally binding treaties by the leading stakeholders, including China and Russia, have been met with little enthusiasm by other states, and are generally seen as having limited prospects of success. Second, states are extremely reluctant to commit themselves to specific interpretations of controversial legal questions and thus to express their cyber *opinio juris*. Third, instead of interpreting or developing rules, state representatives seek refuge in the more ambiguous term 'norms'. This article argues that the reluctance of states to engage themselves in international law-making has generated a power vacuum, lending credence to claims that international law fails in addressing modern challenges posed by the rapid technological development. In response, several non-state-driven norm-making initiatives have sought to fill the void, including Microsoft's cyber norms proposals and the *Tallinn Manual* project. The article then contends that this emerging body of non-binding norms presents states with a critical window of opportunity to reclaim a central law-making position, similarly to historical precedents including the development of legal regimes for Antarctica and nuclear safety. Whether the supposed crisis will lead to the demise of inter-state cyberspace governance or to a recalibration of legal approaches will thus be decided in the near future. States should assume a central role if they want to ensure that the existing power vacuum is not exploited in a way that would upset their ability to achieve their strategic and political goals.

Keywords

attribution; cyber security; governance; norms; rules

* Senior Lecturer in Law at the University of Exeter, United Kingdom. E-mail: k.macak@exeter.ac.uk. Earlier versions of this article were presented at the 8th Annual Conference on Cyber Conflict (CyCon) in Tallinn on 1 June 2016 and at the European Society of International Law Annual Conference in Riga on 9 September 2016. I am grateful to the participants for their feedback and suggestions. I would additionally like to thank Louise Arimatsu, Ana Beduschi, Russell Buchan, Ciarán Burke, Zhixiong Huang, Andrea Lista, Michael N. Schmitt, and Nicholas Tsagourias, as well as the anonymous reviewers for their valuable comments on earlier drafts.

'A small group of thoughtful committed people can change the world. Indeed, it is the only thing that ever has.'

Margaret Mead[1]

'States are, at this moment of history, still at the heart of the international legal system.'

Rosalyn Higgins[2]

'[C]ompliance with international law frees us to do more, and do more legitimately, in cyberspace[.]'

Harold H. Koh[3]

1. Introduction

The international community faces today a wide gamut of diverse global challenges ranging from climate change to international terrorism to cyber threats. What these challenges have in common is that they cannot be adequately addressed by any single international actor, irrespective of how powerful that actor may be. Instead, all such contemporary phenomena necessitate a framework for effective international co-operation. It is international law that 'affords [such] a framework, a pattern, a fabric for international society'.[4]

Although the law establishes a framework of constraints, the flipside of the same coin is that it simultaneously guarantees a sphere of autonomy for its subjects.[5] In the

[1] M. Mead, *The World Ahead: An Anthropologist Anticipates the Future* (2005), 12.

[2] R. Higgins, *Problems and Process: International Law and How We Use It* (1995), 39.

[3] H. H. Koh, 'International Law in Cyberspace', (2012) 54 *Harvard International Law Journal Online* 1, at 10.

[4] L. Henkin, *How Nations Behave* (1978), 5.

[5] Cf. J. Raz, *The Morality of Freedom* (1986), 155 ('Autonomy is possible only within a framework of constraints.').

context of international law, legal norms lay down shared boundaries of acceptable conduct in international relations, while preserving important space for manoeuvre, discretion and negotiation. This is the idea at the root of the famous '*Lotus* presumption',[6] according to which states may generally act freely unless prevented by a contrary rule of international law.[7]

In order to delineate this zone of freedom for states and other international actors with respect to any internationally significant phenomenon, it is necessary to identify, interpret and apply relevant legal rules to it.[8] Despite the ongoing debates about the supposed decline of the sovereign state,[9] it remains the case that states have maintained their centrality in the formation, interpretation, and application of international legal rules in general.[10] But have they kept an equally firm hold on the development of international cyber security law?[11]

There is little doubt that cyberspace, broadly understood, is a phenomenon of international significance in the sense just described. Crucially, the uses and abuses of this complex borderless virtual space impinge on vital state interests in the physical

---

[6] See, e.g., J. Crawford, *The Creation of States in International Law* (2006), 41–42 (describing the presumption as a 'part of the hidden grammar of international legal language'); but see, e.g., *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory Opinion of 22 July 2010, [2010] ICJ Rep. 403, Declaration of Judge Simma, at 478, para. 2 (arguing that the presumption 'reflects an old, tired view of international law').

[7] *SS Lotus case (France v. Turkey)*, PCIJ Rep. Series A No. 10, at 18.

[8] Cf. G. M. Danilenko, *Law-Making in the International Community* (1993), 1 (arguing that in order for the international legal system to remain effective, it needs to engage in (1) law-making in novel, so far ungoverned areas and (2) constant upgrading and refinement of the existing law).

[9] See, e.g., J. A. Camilleri and J. Falk, *The End of Sovereignty?: The Politics of a Shrinking and Fragmenting World* (1992); N. Walker, *Sovereignty in Transition* (2003); J. Bartelson 'The Concept of Sovereignty Revisited', (2006) 17 EJIL 463; T. Jacobsen, C. Sampford, and R. Thakur (eds.) *Re-envisioning Sovereignty: The End of Westphalia?* (2008); T. Endicott, 'The Logic of Freedom and Power' and J. L. Cohen, 'Sovereignty in the Context of Globalization: A Constitutional Pluralist Perspective', in S. Besson and J. Tasioulas (eds.), *The Philosophy of International Law* (2010).

[10] See, e.g., Higgins, *supra* note 2, at 39; M. Byers, *Custom, Power and the Power of Rules* (1999), 13; H. Thirlway, *The Sources of International Law* (2014), 16–19. It is acknowledged that, in addition to state consent, modern international law may at least to some extent also be the product of abstract moral values such as 'humanity', 'fairness', or 'communitarian values'. However, it would be beyond the scope of this article to revisit the longstanding debate about the relative contribution of state consent and abstract values to the process of formation of international law. For more on this topic, see, e.g., H. Charlesworth, 'Law-making and Sources', in J. Crawford and M. Koskenniemi (eds.), *The Cambridge Companion to International Law* (2012), 187 at 187–202 and works cited therein.

[11] The term 'international cyber security law', as understood in this article, refers to an emerging legal discipline and a body of law that concerns the rights and obligations of states regarding cyber security. For an early attempt to define this term in more detail, see W. Heintschel von Heinegg, 'The Tallinn Manual and International Cyber Security Law', (2012) 15 *Yearbook of International Humanitarian Law* 3, at 13.

world, including national security, public safety, and economic development. As such, cyberspace extends far beyond the domain of internal affairs of any state.[12] It therefore follows that it is imperative to clarify the boundary between constraints and autonomy as it applies to actors in cyberspace.

Yet, with respect to the management of cyberspace, it may appear that international law presently fails to deliver. Even though the main building blocks of the Internet's architecture had been laid over two decades ago,[13] it took until 2013 for state representatives to agree on the rudimentary threshold assumption that international law actually applies to cyberspace.[14] The agreement was touted at the time as a 'landmark consensus',[15] but its actual import is controversial.

To begin with, it was expressed in the form of a non-binding report of a Group of Government Experts (GGE) established by the UN General Assembly.[16] At the time, the group was composed of representatives of 15 UN member states,[17] including the three 'cyber superpowers' China, Russia, and the US.[18] On the one hand, the fact of anchoring the process at the UN has added to the legitimacy of its outputs in general.[19] Also, the 2013 report itself can arguably be taken as reflecting a shared understanding in the international community.[20]

On the other hand, the report raised more questions than it answered. International law is supposed to apply, but *which* international law? Although the group endorsed the centrality of the UN Charter,[21] several of its members have questioned the

[12] See also H. H. Perritt, 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance', (1998) 5 *Indiana Journal of Global Legal Studies* 423, at 429; K. Ziolkowski, *Confidence Building Measures for Cyberspace: Legal Implications* (2013), 165.

[13] T. Berners-Lee, 'Information Management: A Proposal', Internal Memo (CERN, March 1989), available at cds.cern.ch/record/1405411/files/ARCH-WWW-4-010.pdf.

[14] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013 ('GGE Report 2013'), at 8, para. 19.

[15] US, Department of State, 'Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues', 7 June 2013, available at www.state.gov/r/pa/prs/ps/2013/06/210418.htm.

[16] GGE Report 2013, *supra* note 14.

[17] Ibid., at 12–13.

[18] See, e.g, A. Segal, *The Hacked World Order* (2016), 40.

[19] M. Finnemore and D. B. Hollis, 'Constructing Norms for Global Cybersecurity', (2016) 110 *American Journal of International Law* 425, at 448.

[20] The UN General Assembly subsequently '[w]elcom[ed]' the GGE report in a unanimously adopted resolution without, however, discussing the details of its contents. See UN GA Res. 68/243, 9 January 2014, preambular para. 11.

[21] GGE Report 2013, *supra* note 14, at 8, para. 19 ('International law, and *in particular the Charter of the United Nations*, is applicable') (emphasis added).

applicability of a prominent subdomain of international law – the law of armed conflict – to cyber operations.[22] Perhaps more importantly, *how* is international law supposed to apply?[23] It is one thing to know that the online realm is not a lawless world, but quite another to understand how existing rules apply to cyber phenomena.[24]

Against this background, this article examines if the current situation is fairly described as one of crisis. To that end, it starts by weighing three key crisis indicators reverberating around states' general reluctance to engage in law-making in the area of the international cyber security law (section 2). Since new binding rules are few and far between, it then looks to the pre-existing landscape of international law and the extent to which it provides a regulatory mechanism in its own right (section 3). Subsequently, the article shows that states' retreat from their traditional legislative function has generated a power vacuum, triggering a number of non-state initiatives seeking to fill it (section 4). On the basis of historical precedents that include the development of legal regimes for Antarctica and nuclear safety, the article then argues that states now have a critical window of opportunity to build on the plurality of emerging non-binding norms and thus reclaim their central law-making position (section 5). Whether they succeed in doing so will determine the future nature of cyberspace governance as well as the role played by international law in this regard.

2. Crisis indicators: International law and cyber security

Three indicators suggesting a crisis in this area of the law stand out. First, the domain of cyber security appears resistant to codification of the applicable rules in a comprehensive multilateral binding treaty.[25] This is not for want of trying by the leading international stakeholders. Already in 1996, France put forward the earliest

[22] See, e.g., US, Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China* (2011), 6 ('China has not yet agreed with the U.S. position that existing mechanisms, such as International Humanitarian Law and the Law of Armed Conflict, apply in cyberspace.'); E. Chernenko, 'Russia Warns Against NATO Document Legitimising Cyberwars', *Kommersant-Vlast*, 29 May 2013, available at rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimising_cyberwars_26483.html (reporting the Russian government's scepticism towards the *Tallinn Manual*'s endorsement of the applicability of international humanitarian law to cyberspace).

[23] For an examination of different approaches to the rule of law in cyberspace taken by, respectively, western countries and China, see Z. Huang and K. Mačák, 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches', (2017) 16 *Chinese Journal of International Law* (forthcoming).

[24] Accord A.-M. Osula and H. Rõigas, 'Introduction', in A.-M. Osula and H. Rõigas (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives* (2016), 11 at 14.

[25] For existing sectoral and regional treaties concerning aspects of cyber security, see text at notes 69–78, *infra*.

proposal with the lofty title *Charter for International Cooperation on the Internet*.[26] Later, a joint Russo-Chinese initiative resulted in two proposals for a *Code of Conduct for Information Security*, submitted to the UN General Assembly in 2011 and 2015, respectively.[27] However, none of these proposals was met with much enthusiasm by other states[28] and scholars describe the prospects of an 'omnibus' treaty being adopted in the near future as slim to negligible.[29] In part, this is no doubt because, whatever the subject, the 'very word "treaty" may conjure up the fearsome formalities of diplomacy', with a chilling effect on states' willingness to engage in this form of law-making.[30] Yet, with respect to cyber security, this aversion appears to be particularly pronounced.

Second, states have shown extreme reluctance to contribute towards the development of cyber-specific customary international rules. In addition to state practice in this area being inevitably shrouded in secrecy,[31] states have been reluctant

[26] T. S. Wu, 'Cyberspace Sovereignty? The Internet and the International System', (1997) 10 *Harvard Journal of Law & Technology* 647, at 660. The initiative was reportedly supposed to 'lead to an accord comparable to the international law of the sea, which governs the world's oceans'. 'France Seeks Global Internet Rules', *Reuters News Service*, 31 January 1996, available at dasalte.ccc.de/crd/CRD19960205.html.de.

[27] 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. 69/723, 13 January 2015, at 3–6.

[28] See, e.g., United Kingdom, Response to General Assembly resolution 68/243 'Developments in the field of information and telecommunications in the context of international security', May 2014, available at s3.amazonaws.com/unoda-web/wp-content/uploads/2014/07/UK.pdf, at 5 (noting that 'attempts to conclude comprehensive multilateral treaties, codes of conduct or similar instruments would [not] make a positive contribution to enhanced international cybersecurity'); M. Kaljurand, 'United Nations Group of Governmental Experts: The Estonian Perspective', in Osula and Rõigas, *supra* note 24, 111 at 123 (stating that 'starting negotiations on the draft Code of Conduct … would be premature').

[29] See, e.g., J. Goldsmith, 'Cybersecurity Treaties: A Skeptical View', in P. Berkowitz (ed.), *Future Challenges in National Security and Law* (2011), available at www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf, at 12; M. C. Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)', (2011) 36 *Yale Journal of International Law* 421, at 425–426; O. A. Hathaway et al., 'The Law of Cyber-Attack', (2012) 100 *California Law Review* 817, at 882; K. E. Eichensehr, 'The Cyber-Law of Nations', (2015) 103 *Georgetown Law Journal* 317, at 356; M. N. Schmitt and L. Vihul, 'The Nature of International Law Cyber Norms', in Osula and Rõigas, *supra* note 24, 23 at 39.

[30] A. Aust, *Modern Treaty Law and Practice* (2000), 26.

[31] See R. A. Clarke and R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (2010), xi ('The entire phenomenon of cyber war is shrouded in such government secrecy that it makes the Cold War look like a time of openness and transparency.').

to offer clear expressions of *opinio juris* on matters related to cyber security.[32] At times, this approach may certainly be understandable, being the consequence of a domestic political gridlock or even a deliberate waiting strategy.[33] On other occasions, it may rather be due to the persisting 'cybersecurity knowledge gap', in other words the striking lack of understanding of cybersecurity matters, which permeates the government structures in countries around the world.[34] On the whole, this reluctance adds to the pervasive ambiguity as far as the specific applicability of international law is concerned.

This trend is visible even in the most recent developments. A representative example of another missed opportunity to steer the development of cyber custom is provided by the recent US *Law of War Manual* adopted in July 2015 and updated in December 2016.[35] Although it does contain a chapter on cyber operations,[36] the *Manual* skirts virtually all of the unsettled issues, including standards of attribution, rules of targeting or the requirement to review cyber weapons.[37]

While the first two indicators relate to states' reluctance to act in ways meaningful for the generation of new rules, the third concerns their actual conduct in relation to cyber governance. It would be inaccurate to claim that states have entirely given up on standard-setting. However, instead of interpreting or developing rules of international law, state representatives have generally sought refuge in the more ambiguous term 'norms'. It is true that law and norms are 'intimately intertwined' concepts and that inter-state agreement on 'norms' may gradually influence the development of the law.[38] Yet, a fundamental difference between the two is that a violation of a binding

[32] Notable exceptions include, e.g., US, The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011); Koh, *supra* note 3; Brian J. Egan, 'International Law and Stability in Cyberspace', Speech at Berkeley Law School, 10 November 2016, available at www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf.

[33] M. N. Schmitt and S. Watts, 'The Decline of International Humanitarian Law *Opinio Juris* and the Law of Cyber Warfare', (2015) 50 *Texas International Law Journal* 189, at 211.

[34] See P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2014), 4–8.

[35] US, Department of Defense, Office of the General Counsel, *Law of War Manual* (2016), available at www.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf.

[36] Ibid., ch. xvi.

[37] See further S. Watts, 'Cyber Law Development and the United States Law of War Manual', in Osula and Rõigas, *supra* note 24, 49 at 60–63.

[38] Finnemore and Hollis, *supra* note 19, at 441–442.

rule of international law gives rise to international legal responsibility,[39] while the same cannot be said of non-legal norms regulating cyber conduct.[40]

The trend of promoting cyber norms is the most visible in the context of the work of the UN GGE. In its latest report, the group touted the advantages of '[v]oluntary, *non-binding norms* of responsible State behaviour'.[41] The report claimed that such norms prevent conflict in cyberspace, foster international development, and reduce risks to international peace and security.[42] The report further recommended 11 such norms for consideration by states,[43] while making it clear that these norms operate on a decidedly non-legal plane.[44] Despite their minimalistic nature, the norms have thus far received very limited endorsement by their addressees. For example, at a US-China summit in September 2015, the two participating heads of state 'welcomed' the report but refrained from committing themselves to any of the proposed norms.[45]

Together, these three indicators signify a trend of moving away from the creation of legal rules of international law in the classical sense. Instead of developing binding treaty or customary rules, states resort to normative activity outside the scope of traditional international law. Although this trend appears to be especially prominent in the area of cyber security, it is by no means limited to it.[46] In legal theory, this phenomenon has been described as 'the pluralisation of international norm-making',[47] characterised by the observation that 'only a limited part of the exercise of public authority at the international level nowadays materialises itself in the creation of norms which can be considered international legal rules according to a classical understanding of international law'.[48] In order to understand the impact this situation

[39] International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, 2001 YILC, Vol. 53 II (Part Two), Art. 1; *Rainbow Warrior Arbitration (New Zealand v. France)*, Special Arbitration Tribunal, (1990) 20 RIAA 215, at 251, para. 75 ('any violation by a State of any obligation, of whatever origin, gives rise to State responsibility').

[40] See further Schmitt and Vihul, *supra* note 29, at 25–27.

[41] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22 July 2015 ('GGE Report 2015'), at 7, para. 10 (emphasis added).

[42] Ibid., at 7, para. 10.

[43] Ibid., at 7–8, para. 13.

[44] Ibid., at 7, para. 10.

[45] US, White House, 'Fact Sheet: President Xi Jinping's State Visit to the United States', 25 September 2015, available at obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[46] For a general discussion of the process of gradual 'surrender [of states'] monopoly on regulatory power' from the perspective of global governance, see E. Benvenisti, *The Law of Global Governance* (2014), 25 et seq.

[47] J. d'Aspremont, *Formalism and the Sources of International Law* (2011), 222.

[48] Ibid., at 2.

has on the international legal regulation of cyber security, we must zoom out slightly to take in the broader context of existing international law.

3. Gaps and patches: Existing legal landscape

3.1. Generally applicable rules

The absence of a cyber-specific system of rules of international law does not mean that there are no legal rules that would apply to cyber activities. As we have seen, states accept that generally applicable rules of international law apply to states' conduct in cyberspace, too. This is undoubtedly correct. If international law is to be an efficient governance structure, it must be adaptable to new phenomena without the need to reinvent an entire regulation framework on each occasion.[49]

By way of an example, the UN Charter was finalised when the invention of nuclear weapons was still a closely guarded secret[50] and this instrument thus understandably did not refer to this type of weapons in its provisions on the use of force.[51] Still, the International Court of Justice (ICJ) had little difficulty in holding, in the *Nuclear Weapons* Advisory Opinion issued decades later, that those provisions 'apply to any use of force, regardless of the weapons employed',[52] notwithstanding the fact that a particular type of weapons might not yet have been generally known or even invented when the Charter was adopted.[53] Following the same logic, cyber operations must equally be subject to the international law regulation of the use of force.[54]

The applicability of international human rights law (IHRL) to states' conduct online is another highly relevant example. The foundations of this body of law were laid in

[49] Cf. US, *International Strategy for Cyberspace*, *supra* note 32, at 9 ('The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete.').

[50] Cf. *Legality of the Threat or Use of Nuclear Weapons Case*, Berchmans Soedarmanto Kadarisman, CR 95/25, 3 November 1995, at para. 46 ('the framers of the United Nations Charter could not be aware of the threat of nuclear weapons').

[51] Charter of the United Nations, 1 UNTS 16 (1945), Arts. 2(4) and 39–51.

[52] *Legality of the Threat or Use of Nuclear Weapons Case*, Advisory Opinion of 8 July 1996, [1996] ICJ Rep. 226, at para. 39.

[53] See further S. Kadelbach, 'Interpretation of the Charter', in B. Simma et al. (eds.), *The Charter of the United Nations: A Commentary* (2012), 71 at 89 (arguing that the utility of the Charter *travaux* is limited given that many problems were not foreseen in 1945, whereas for others shared meanings have been worked out over time).

[54] Accord M. N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013) (hereinafter '*Tallinn Manual*'), 42; M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017) (hereinafter '*Tallinn Manual 2.0*'), 328. See section 4 *infra* for a detailed discussion of the two editions of the *Manual* and their contents.

the post-Second World War period when states adopted instruments which together form the so-called 'International Bill of Human Rights'.[55] Needless to say, these texts predate, by a large margin, the contemporary challenges inherent to and amplified by cyberspace. Still, this chronology does not render IHRL inapplicable to cyber activities. Quite the contrary: the fact that today 'people are as likely to come together to pursue common interests online as in a church or a labor hall' requires that universal human rights 'also apply in cyberspace', as then-US Secretary of State Hillary Clinton argued in a path-breaking speech in 2011.[56] This position has since been endorsed by two resolutions of the UN Human Rights Council in 2012 and 2016, which have included identical phrases affirming that 'the same rights that people have offline must also be protected online'.[57]

While the conclusion that these generally applicable rules of international law apply to conduct in cyberspace may offer some solace, many crucial questions remain unanswered. For instance, it is one thing to posit the applicability of the law on the use of force to cyberspace, but quite another to determine whether a specific cyber attack crosses the threshold of force in concrete circumstances. Although an influential set of factors known after their author as the 'Schmitt criteria' have emerged in the literature,[58] little is known about states' views in that regard.[59] Crucially, no cyber operation—including Stuxnet, which has arguably been the most intrusive one thus

[55] The International Bill of Rights consists of the Universal Declaration of Human Rights (1948); the International Covenant on Civil and Political Rights (1966) and the two Optional Protocols annexed thereto; and the International Covenant on Economic, Social and Cultural Rights (1966) and its Protocol.

[56] US, DIPNOTE (US Department of State Official Blog), 'Internet Rights and Wrongs: Choices and Challenges in a Networked World', 15 February 2011, available at blogs.state.gov/stories/2011/02/15/internet-rights-and-wrongs-choices-and-challenges-networked-world; see also Egan, *supra* note 32, at 15 ('[a]ny regulation by a State of matters within its territory, including use of and access to the Internet, must comply with that State's applicable obligations under international human rights law').

[57] UN GA, Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc. A/HRC/20/L.13, 29 June 2012, at para. 1; UN GA, Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc. A/HRC/32/L.20, 27 June 2016, at para. 1. See also GGE Report 2013, *supra* note 14, at 8, para. 21; GGE Report 2015, *supra* note 41, at 8, para. 13(e) and at 12, para. 26; *Tallinn Manual 2.0*, *supra* note 54, at 179.

[58] M. N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', (1999) 37 *Columbia Journal of Transnational Law* 914 (original list of six criteria: severity; immediacy; directness; invasiveness; measurability; and presumptive legitimacy); M. N. Schmitt, 'Cyber Operations and the Jus Ad Bellum Revised', (2011) 56 *Villanova Law Review* 576 (revised list of seven criteria: severity; immediacy; directness; invasiveness; measurability; presumptive legitimacy; and responsibility); *Tallinn Manual 2.0*, *supra* note 54, at 334–336 (restated list of eight criteria: severity; immediacy; directness; invasiveness; measurability; military character; state involvement; and presumptive legality).

[59] For a notable exception, see Koh, *supra* note 3, at 3–4 (referencing the 1999 version of the 'Schmitt criteria').

far, having caused extensive physical damage to an Iranian nuclear facility in 2010[60]—has ever been described as amounting to a use of force by any state,[61] whether by a victim or a bystander.[62]

Similarly, the general agreement that human rights are also available online tells us very little about the legal qualification of new cyber phenomena that are without precedents from the offline era. A case in point is Tor, a technology that protects users against surveillance and traffic analysis online and thus enables them to communicate anonymously on the Internet.[63] Western states including the US or Sweden apparently see Tor as a means for furthering privacy and freedom of expression and as such worthy of their moral and financial support.[64] In contrast, China views this technology as a security threat and a tool of cyber attacks;[65] in this light, it is unsurprising that the use of Tor is unlawful in China.[66] Likewise, other non-western states including Ethiopia, Iran, and Kazakhstan have reportedly sought to block Tor traffic in the past.[67] In sum, it is unclear how to square states' near-identical proclamations made at a high level of generality with their highly divergent behaviour with respect to particular phenomena unsubstantiated by any corresponding legal justification.[68]

---

[60] See, e.g., Iran, Statement by H. E. Dr. Ali Akbar Salehi, Minister of Foreign Affairs of the Islamic Republic of Iran, 28 September 2012, available at iran-un.org/en/2012/09/28/28-september-2012-2/ (describing cyber attacks against Iran's nuclear facilities as 'a manifestation of nuclear terrorism and consequently a grave violation of the principles of UN Charter and international law' but stopping short of using the *jus ad bellum* language).

[61] But see *Tallinn Manual 2.0*, *supra* note 54, at 342 (noting that all members of the international group of experts considered the Stuxnet operation as a use of force).

[62] See, e.g., C. Henderson, 'The Use of Cyber Force: Is the Jus ad Bellum Ready?' *Questions of International Law*, 30 April 2016, available at www.qil-qdi.org/use-cyber-force-jus-ad-bellum-ready.

[63] See 'Tor Project', available at www.torproject.org. For a recent analysis of legal issues raised by the uses and abuses of Tor from the perspective of international and European law, see T. Minárik and A.-M. Osula, 'Tor Does Not Stink: Use and Abuse of the Tor Anonymity Network from the Perspective of Law', (2016) 32(1) *Computer Law and Security Review* 111.

[64] See G. A. Fowler, 'Tor: An Anonymous, And Controversial, Way to Web-Surf', *The Wall Street Journal*, 17 December 2012.

[65] Singer and Friedman, *supra* note 34, at 107.

[66] K. D. Watson, 'The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks', (2012) 11 *Washington University Global Studies Law Review* 715, at 727.

[67] UN, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, UN Doc. A/HRC/29/32, 22 May 2015, at para. 52.

[68] See also *Tallinn Manual 2.0*, *supra* note 54, at 188 (noting that the international group of experts 'could achieve no consensus on the precise parameters of the right to freedom of expression') and 194–195 ('although actions to prohibit, restrict, or undermine access to devices or technology that foster anonymity may, as a practical matter, reduce the exercise or enjoyment of international human rights online, such actions do not in themselves necessarily implicate international human rights law as a matter of *lex lata* on the basis of infringement with or loss of anonymity').

3.2. Sectoral and regional treaties

In addition to generally applicable rules of international law, certain sectoral and regional treaties taken together provide a 'patchwork of regulations' for cyber activities.[69] These include, in particular, the 1992 Constitution of the International Telecommunication Union;[70] the 2001 Budapest Convention on Cybercrime[71] and its 2006 Protocol on Xenophobia and Racism;[72] the 2009 Shanghai Cooperation Organization's Information Security Agreement;[73] and the 2014 African Union's Cyber Security Convention.[74] Although important in their own right, these international agreements govern only a small slice of cyber-related activities (such as criminal offences committed by means of computer systems[75] or operations interfering with existing telecommunications networks[76]), or have a very limited membership (six states in the case of the Shanghai Cooperation Organization's agreement[77] and none yet in that of the African Union's convention[78]).

Therefore, although cyberspace is certainly not a lawless territory beyond the reach of international law, for now there is no complex regulatory mechanism governing state cyber activities.[79] Moreover, states seem reluctant to engage themselves in the development and interpretation of international law applicable to cyber security. This

[69] Hathaway, *supra* note 29, at 873.

[70] Constitution of the International Telecommunication Union, 1825 UNTS 143 (1992) (hereinafter 'ITU Constitution').

[71] Council of Europe, Convention on Cybercrime, ETS 185 (2001).

[72] Council of Europe, Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, ETS 189 (2003).

[73] Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security (2009) (hereinafter 'Yekaterinburg Agreement').

[74] African Union Convention on Cyber Security and Personal Data Protection, AU Doc. EX.CL/846(XXV) (2014).

[75] Convention on Cybercrime, *supra* note 71, Arts. 2–10.

[76] ITU Constitution, *supra* note 70, Art. 45 (prohibiting harmful interference) and Ann. (defining harmful interference).

[77] Yekaterinburg Agreement, *supra* note 73. In 2017, India and Pakistan are expected to join the Shanghai Co-operation Organization (SCO), which will likely result in a corresponding increase in the number of state parties to the Agreement. See AFP, 'India, Pakistan Edge Closer to Joining SCO Security Bloc', The Express Tribune, 24 June 2016, available at tribune.com.pk/story/1129533/india-pakistan-edge-closer-joining-sco-security-bloc.

[78] See further H. Rõigas, 'Mixed Feedback on the "African Union Convention on Cyber Security and Personal Data Protection"', *CCD COE INCYDER Database*, 20 February 2015, available at ccdcoe.org/mixed-feedback-african-union-convention-cyber-security-and-personal-data-protection.html.

[79] See also Hathaway, *supra* note 29, at 873.

voluntary retreat has generated a power vacuum, enabling non-state actors to move into the space vacated by states[80] and pursue various forms of 'norm entrepreneurship'.[81]

4. Power vacuum: Withdrawal of states and emergence of non-state initiatives

4.1. Power and law

Vectors of power and law do not overlap perfectly. State power is certainly influenced by many other factors, which may include military might, wealth, and moral authority.[82] Nonetheless, it needs little emphasis that the relationship between power and law is a close one, particularly at the international level.[83] In this sense, states may be said to normally opt for one of two archetypal approaches in order to actualize that relationship to further their interests. On the one hand, they frequently choose the path of legal certainty in order to consolidate and project their power. Indeed, if we understand power in the Nyean sense as 'the ability to alter others' behaviour to produce preferred outcomes',[84] then setting specific legal obligations is one way how to exercise this ability.[85] Everything else being equal, it is more likely than not that these 'others' will act in accordance with a certain standard of behaviour when it is required by law than when it is not.[86]

On the other hand, in certain contexts, the competing approach of legal uncertainty may be deemed desirable by even the most powerful states. In other words, states may choose to instrumentalize the ambiguity surrounding the existence, content, and interpretation of legal rules as a power-protecting tool. For example, during the early days of space exploration, only two states were capable of acting in outer space: the US and the Soviet Union. Yet these two states resisted, for a significant time, to commit

[80] This has now been expressly acknowledged even by state representatives. See, e.g., Egan, *supra* note 32, at 5.

[81] M. Finnemore and K. Sikkin, 'International Norm Dynamics and Political Change', (1998) 52 *International Organisation* 887, at 895–899; see also Finnemore and Hollis, *supra* note 19, at 446–448 (examining the concept and function of 'norm entrepreneurship' in the cybersecurity context).

[82] Byers, *supra* note 10, at 5.

[83] See further Higgins, *supra* note 2, at 3–4 (analysing the relationship between law and power from the perspective of international law).

[84] J. Nye, *The Future of Power* (2011), 10.

[85] See also Finnemore and Hollis, *supra* note 19, at 441–444 (arguing that, in addition to law, the bases on which particular conduct in cyberspace is labelled as appropriate or inappropriate include politics, culture, religion, and professional standards).

[86] See further J. Crawford, *Change, Order, Change: The Course of International Law* (2013), 40–49 (demonstrating the effectiveness of international legal obligations on a diverse set of empirical examples including the protection of the ozone layer, restrictions on whaling, and slave trade).

themselves to any binding rules that would govern outer space. Both had believed that the adoption of such rules would only serve to constrain their activities in space. In that vein, '[l]egal uncertainty was useful to those with the power to act in space, on either side of the cold war.'[87]

However, cyberspace and outer space – albeit frequently lumped together as so-called 'global commons'[88] – are decidedly different from one another. This is not only because many states are challenging the very idea of cyberspace as commons by seeking to assert greater control online.[89] More importantly, cyberspace is already a much more crowded domain than outer space could ever be. To wit, the US and the Soviet Union were not just the only states engaged in space exploration for several decades, they were also the only *actors* capable of space flight.[90] In contrast, cyberspace is populated primarily by non-state actors, which include individuals, corporations, and other more loosely organised groups.[91] The possibility of anonymity online combined with the corresponding difficulty of attribution of cyber operations have resulted in the 'dramatic amplification' of power in the hands of these non-state actors at the expense of their state counterparts.[92]

The effect of legal uncertainty is thus much more complex than what we saw in the past in relation to outer space, as it affects a far more populous spectrum of actors, state and non-state alike. It is true that in terms of power and available resources, the relationship between states and non-state actors in cyberspace remains marked by 'a clear disequilibrium in favor of States'.[93] And yet, faced with states' silence, non-state actors have moved into the vacated norm-creating territory, which had previously been occupied exclusively by states. These developments have been primarily driven

[87] S. Banner, *Who Owns the Sky? The Struggle to Control Airspace from the Wright Brothers On* (2008), 278.

[88] See, e.g., M. Barrett et al., *Assured Access to the Global Commons* (2011), at xii; S. Jasper and S. Moreland, 'Introduction: A Comprehensive Approach', in S. Jasper (ed.), *Conflict and Cooperation in the Global Commons* (2012), 1 at 21; N. Tsagourias, 'The Legal Status of Cyberspace', in N. Tsagourias and R. Buchan (eds.), *Research Handbook on International Law and Cyberspace* (2015), 13 at 24–25; P. Meyer, 'Outer Space and Cyberspace: A Tale of Two Security Realms', in Osula and Rõigas, *supra* note 24, 155 at 157.

[89] S. Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations* (2014), 58.

[90] Of course, the situation has dramatically changed since then. The number of space-faring states has been steadily increasing and even some non-state actors have demonstrated their capability to engage in outer space activities. See further P. Jankowitsch, 'The Background and History of Space Law', in F. von der Dunk (ed.), *Handbook of Space Law* (2015), 1 at 1–28.

[91] See further J. Sigholm, 'Non-State Actors in Cyberspace Operations', (2013) 4 *Journal of Military Studies* 1, at 9–23.

[92] C. Czosseck, 'State Actors and their Proxies in Cyberspace', in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace* (2013), 1 at 1–3.

[93] K. Bannelier and T. Christakis, *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors* (2017), 9.

by the private sector and by the academia, as epitomised by Microsoft's cyber norms proposal and by the so-called *Tallinn Manual* project.

4.2. Leading non-state-driven initiatives

Firstly, Microsoft's proposal entitled *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World* was published in December 2014.[94] Interestingly, this white paper was not the first private-sector initiative of this kind. Exactly 15 years earlier, Steve Case, then the CEO of AOL, urged states to revise their 'country-centric' laws and adopt instead 'international standards' governing crucial aspects of conduct online, including security, privacy, and taxation.[95] Still, Microsoft's text was the first comprehensive proposal of specific standards of behaviour online, which, despite its private origin, proposed norms purporting to regulate solely the conduct of states.[96] The openly proclaimed central aim of this white paper was to reduce the possibility that information and communications technology (ICT) products and services would be 'used, abused or exploited by nation states as part of military operations'.[97] To that end, the paper put forward six cyber security norms, which collectively called on states to improve their cyber defences and limit their engagement in offensive operations.[98]

Microsoft's original proposal was met with criticism to the effect that by focussing on states, the paper ignored the crucial role that the industry must itself take on to achieve global cyber security.[99] In 2016, Microsoft responded to these claims by issuing another white paper entitled *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*.[100] In it, the company proposed six further cybersecurity norms,

---

[94] A. McKay et al., *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World* (2014), available at aka.ms/cybernorms.

[95] S. Case, 'Remarks Prepared for Delivery (via satellite) Israel '99 Business Conference', 13 December 1999, cited in J. Goldsmith and T. S. Wu, *Who Controls the Internet?: Illusions of a Borderless World* (2006), 194 (urging nations to 'revis[e] outdated and "country-centric" laws on telecommunications and taxes that could thwart the growth of the medium' and instead embrace 'international standards—from security, to privacy, to taxation.').

[96] McKay et al., *supra* note 94, at 2–3.

[97] S. Choney, '6 Proposed Cybersecurity Norms Could Reduce Conflict', *Microsoft: The Fire Hose*, 5 December 2014, available at blogs.microsoft.com/firehose/2014/12/05/6-proposed-cybersecurity-norms-could-reduce-conflict.

[98] McKay et al., *supra* note 94, at 2. The complete list of the proposed norms may be found in the annex to the document: ibid., at 20.

[99] S. Charney et al., *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms* (2016), available at mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf, at 3.

[100] Ibid.

this time addressed to 'the global ICT industry'.[101] These were meant to complement and strengthen the norms published in the earlier document.[102]

On the whole, however, the text made no secret of the fact that it, like the entire Microsoft-led cyber norms project, was still primarily addressed to states. Even parts that concerned the role of the industry were written in the form of demands that the recognition of that role would place on states. For instance, the paper appealed to states to involve the industry in the norms debate, to draw on its technical expertise, and to give greater weight to its input overall.[103] In early 2017, Microsoft further stepped up its initiative, calling on states to transform its six state-oriented norms into an international treaty with a bold working title: 'a Digital Geneva Convention'.[104]

Secondly, the Tallinn Manual process was a seven-year project undertaken under the auspices of the Estonia-based NATO Cooperative Cyber Defence Centre of Excellence (CCD COE).[105] The project brought together an international group of experts under the leadership of Professor Michael Schmitt and resulted in the publication of two editions of the Manual respectively in 2013[106] and 2017.[107] Although both editions acknowledged the support of the NATO CCD COE, they also made it clear that their text reflected only the personal views of the experts and not the states or institutions from which they originated.[108]

The first edition, entitled *Tallinn Manual on the International Law Applicable to Cyber Warfare*, maintained an almost exclusive focus on activities occurring above the level of the use of force. Its text identified 95 purported rules of customary international law, the vast majority of which related to the law on the use of force (*jus ad bellum*)[109] and the law of armed conflict (*jus in bello*).[110] The Manual quickly became a standard reference point and was deservedly praised for breaking new ground as well as for providing useful practical guidance.[111] However, early reviews and reactions from

[101] Ibid., at 7.

[102] Ibid., at 6.

[103] Ibid., at 2.

[104] B. Smith, President of Microsoft Corporation, Transcript of Keynote Address at the RSA Conference 2017, 14 February 2017, available at mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

[105] See 'Tallinn Manual Process', available at ccdcoe.org/tallinn-manual.html.

[106] *Tallinn Manual*, *supra* note 54.

[107] *Tallinn Manual 2.0*, *supra* note 54.

[108] *Tallinn Manual*, *supra* note 54, at 11; *Tallinn Manual 2.0*, *supra* note 54, at 2.

[109] *Tallinn Manual*, *supra* note 54, rules 10–19.

[110] *Tallinn Manual*, *supra* note 54, rules 20–95.

[111] See, e.g., K. Eichensehr, 'Review of The Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013)', (2014) 108 *American Journal of International Law* 585, at 585–589.

states not involved in the project criticized the project's preoccupation with military uses of cyberspace and noted that in reality, most (if not all) cyber operations fall below the threshold of the use of force.[112]

The 2017 edition, published under the slightly modified title *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, addressed these criticisms by considerably expanding the scope of the study.[113] The second edition thus nearly doubled the number of rules identified, for a total of 154 agreed rules of custom, only about a half of which related to the *jus ad bellum* and the *jus in bello*.[114] In addition, the Tallinn Manual 2.0 covers multiple areas of 'peacetime international law',[115] including state responsibility,[116] the law of the sea,[117] air and space law,[118] and even human rights law.[119] This substantive revision and expansion of the text will likely further strengthen the project's overall relevance as well as its claim to authority. Yet, like the Microsoft paper, both iterations of the *Tallinn Manual* project put forward standards of state behaviour and are avowedly state-centric in their approach.

4.3. Differences and similarities

Understandably, the two initiatives differ in important ways. The 'norms' proposed by Microsoft are clearly meant as broad suggestions only, meaning that states need to transform them into more specific commitments. For instance, norm 2 stipulates that 'states should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them'.[120] As recognised in the 2014 paper, such policies need to be developed by each individual state and tailored to the needs of that state.[121] The 2016 paper complements this general proposal by endorsing the existing best

[112] See, e.g., D. Fleck, 'Searching for International Rules Applicable to Cyber Warfare: A Critical First Assessment of the New *Tallinn Manual*', (2013) 18 *Journal of Conflict & Security Law* 331, at 332–335; Eichensehr, *supra* note 111, at 589; see also Ma Xinmin, 'Key Issues and Future Development of International Cyberspace Law', (2016) 2 *China Quarterly of International Strategic Studies* 119, at 128 (noting the Chinese view that the risk of the law-of-war focus on the regulation of cyberspace was that it would aggravate the arms race and militarisation in cyberspace).

[113] *Tallinn Manual 2.0*, *supra* note 54, at 1–6.

[114] See ibid., rules 68–154.

[115] Ibid., at 2

[116] Ibid., at 79–167.

[117] Ibid., at 232–258.

[118] Ibid., at 259–283.

[119] Ibid., at 179–208.

[120] McKay et al., *supra* note 94, at 12; Charney et al., *supra* note 99, at 7.

[121] McKay et al., *supra* note 94, at 12.

practice standards of co-ordinated vulnerability disclosure by the ICT industry.[122] However, neither of the two texts puts forward any more detailed prescriptions for states.[123]

By contrast, the *Tallinn Manual* 'rules' take on the more restrictive and specific form of purported customary legal obligations, which should simply be observed by states as binding without the need for their further endorsement or adaptation.[124] In other words, both editions of the *Manual* have aimed to interpret how 'extant legal norms' apply to conduct in cyberspace,[125] and not to 'set forth *lex ferenda*'.[126] Nonetheless, the detailed and frequently novel positions put forward by the *Manuals* blur the fuzzy line between norm interpretation and norm development.[127] For example, Rule 99 (ex Rule 37) sets out the prohibition of cyber attacks against civilian objects in the context of an armed conflict.[128] Both crucial terms – 'cyber attacks' as well as 'civilian objects' – are precisely defined by the *Manual*.[129] Although some disagreements may persist about the application of the rule in specific circumstances,[130] the content of the norm is sufficiently clear and precise to generate legal rights and obligations.

Yet, what initiatives like Microsoft's white papers or the *Tallinn Manual* project share is their non-state origin and expressly non-binding nature. Microsoft was keenly aware of its proposal's limitations in this respect and noted that it merely 'encouraged' states to set the proposed norms on the trajectory towards making them first 'politically' and then 'legally' binding.[131] Similarly, the first edition of the *Manual* stated

[122] Charney et al., *supra* note 99, at 8.

[123] See also Smith, *supra* note 104, at 10 (calling on states to adopt a 'global convention' that would include norms from Microsoft's 2014 and 2016 proposals).

[124] *Tallinn Manual 2.0*, *supra* note 54, at 4; see also *Tallinn Manual*, *supra* note 54, at 6.

[125] *Tallinn Manual*, *supra* note 54, at 1; *Tallinn Manual 2.0*, *supra* note 54, at 1.

[126] *Tallinn Manual*, *supra* note 54, at 5; *Tallinn Manual 2.0*, *supra* note 54, at 3.

[127] See further K. Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law', (2015) 48 *Israel Law Review* 55, at 59–63 (discussing the distinction between *lex lata* and *lex ferenda* in the first edition of the *Manual)*.

[128] *Tallinn Manual 2.0*, *supra* note 54, at 434; see also *Tallinn Manual*, *supra* note 54, at 124.

[129] *Tallinn Manual 2.0*, *supra* note 54, at 415 (definition of cyber attack) and at 435, para. 4 (definition of civilian objects); see also *Tallinn Manual*, *supra* note 54, at 91 (definition of cyber attack) and at 125, para. 3 (definition of civilian objects).

[130] See, e.g., the debate whether computer data may constitute an 'object' for the purposes of international humanitarian law (IHL): H. A. Harrison Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives', (2015) 48 *Israel Law Review* 39; Mačák, *supra* note 127; M. N. Schmitt, 'The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision', (2015) 48 *Israel Law Review* 81.

[131] McKay et al., *supra* note 94, at 3; see also Smith, *supra* note 104, at 10 ('And we then need to build on that with a global convention.').

in its introduction that it was meant to be 'a non-binding document'.[132] As all of these texts are in their entirety the products of non-state initiatives, they could hardly amount to anything else. After all, with potential minor qualifications in the area of collective security, it is still true that only 'the states are the legislators of the international legal system'.[133]

If these texts are non-binding, one might question their relevance from the perspective of international law altogether. Admittedly, their normativity (in the sense of the strength of their claim to authority[134]) is lower than that of international legal rules. Similarly, the ongoing International Law Commission (ILC) study on the *Identification of Customary International Law* notes in this regard in its draft conclusion 4(3) that conduct of actors other than states and international organizations 'is not practice that contributes to the formation, or expression, of rules of customary international law'.[135]

But that does not mean that these efforts are wholly irrelevant for the formation of rules of international law, and even less do they document any supposed irrelevance of international law to the area of cyber security. On the contrary, non-state-driven initiatives of this kind potentially amount to 'a vital intermediate stage towards a more rigorously binding system, permitting experiment and rapid modification'.[136] Moreover, they render the law-making process more multilateral and inclusive than the traditional state-driven norm-making can ever be.[137] As the ILC recognizes in the remainder of the cited draft conclusion, conduct of non-state actors may be relevant

---

[132] *Tallinn Manual*, *supra* note 54, at 1. The sentence in question does not appear in the second edition of the *Manual*, however, there is nothing in its text suggesting that the *Manual* should not be seen as a non-binding document. Cf. *Tallinn Manual 2.0*, *supra* note 54, at 2 ('*Tallinn Manual 2.0* is not an official document … *Tallinn Manual 2.0* must be understood only as an expression of the opinions of the two International Groups of Experts as to the state of the law.').

[133] S. Talmon, 'The Security Council as World Legislature', (2005) 99 AJIL 175, at 175. As the title of Professor Talmon's article suggests, the qualification to that general observation arises from the Security Council's recent practice of adopting resolutions containing obligations of general and abstract character. For a recent argument to the effect that non-state actors should be granted a role in international law-making, see A. Roberts and S. Sivakumaran, 'Lawmaking by Nonstate Actors: Engaging Armed Groups in the Creation of International Humanitarian Law', (2012) 37 *Yale Journal of International Law* 107. For more on the supposed ongoing surrender of states' monopoly on regulatory power from the perspective of global governance, see Benvenisti, *supra* note 46, at 25 et seq.

[134] S. Besson, 'Theorising the Sources of International Law', in S. Besson and J. Tasioulas (eds.), *The Philosophy of International Law* (2010), 163 at 173.

[135] ILC, 'Identification of Customary International Law: Text of the Draft Conclusions Provisionally Adopted by the Drafting Committee', UN Doc. A/CN.4/L.872, 30 May 2016, at 2.

[136] Thirlway, *supra* note 10, at 164, paraphrasing M. E. O'Connell, 'The Role of Soft Law in a Global Order', in D. Shelton (ed.), *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (2000), 100.

[137] Besson, *supra* note 134, at 170–171; Charlesworth, *supra* note 10, at 199.

when assessing the practice of states.[138] Therefore, the crucial question is whether states decide to pick up the gauntlet thrown at them by their non-state counterparts.

5. Offline analogies: States at a critical juncture

5.1. Soft law and hard law

The current situation is certainly not without prior historical parallels. Cyberspace is not the first novel phenomenon to have resisted the development of global governance structures for some time after its emergence. A degree of waiting or stalling may even reflect states' desire to obtain a better understanding of the new phenomenon's strategic potential.[139] Yet with states' improved comprehension of the new situation, their willingness to subject themselves to binding rules usually increases, too. Even the domain of outer space was eventually subjected to a binding legal regime,[140] despite the strong initial reluctance of the dominant spacefaring states.[141]

Other domains with a higher number of participants may provide more appropriate analogies. A good example is the legal regime of the Antarctic region. Although its central instrument, the 1959 Antarctic Treaty,[142] is a binding international agreement, it did not establish a comprehensive legal regime regulating all aspects of the Antarctic

[138] ILC, 'Identification of Customary International Law: Text of the Draft Conclusions Provisionally Adopted by the Drafting Committee', UN Doc. A/CN.4/L.872, 30 May 2016, at 2.

[139] Cf. P. W. Franzese, 'Sovereignty in Cyberspace: Can It Exist?', (2009) 64 *Air Force Law Review* 1, at 38; Schmitt and Vihul, *supra* note 29, at 38.

[140] This legal regime consists of five key international agreements: Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 610 UNTS 205 (1967) ('Outer Space Treaty'); Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched Into Outer Space, 672 UNTS 119 (1968) ('Rescue and Return Agreement'); Convention on International Liability for Damage Caused by Space Objects, 961 UNTS 187 (1972) ('Liability Convention'); Convention on Registration of Objects Launched into Outer Space, 1023 UNTS 15 (1975) 'Registration Convention'); Agreement governing the Activities of States on the Moon and Other Celestial Bodies, 1363 UNTS 3 (1979) ('Moon Agreement'). It should be noted that this existing treaty framework does not comprehensively address the issue of military uses of outer space. An ongoing project, the Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS), aims to respond to this need by developing a manual clarifying the fundamental rules applicable to such conduct in times of peace as well as in armed conflict. See further 'McGill University launches the Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS®) Project', 27 May 2016, available at www.mcgill.ca/milamos/files/milamos/mcgill_milamos_announcement_final_1.pdf.

[141] See text at note 87, *supra*.

[142] Antarctic Treaty, 402 UNTS 71 (1959).

environment.[143] Instead, it allowed for and, to some extent, encouraged the adoption of 'recommended measures' and other types of non-binding norms for specific areas of international concern.[144] Indeed, in the 1960s and 1970s, state representatives put forward many 'soft norms' of this kind, which shared the objective of preservation and conservation of living and non-living resources in Antarctica.[145] Subsequently, some of these measures were implemented by many (though not all) parties to the Antarctic Treaty in their domestic law, paving the way towards the consolidation of the norms in question into international 'hard law'.[146] This finally materialized with the adoption of the 1991 Antarctic Environmental Protection Protocol, a complex binding instrument that has since been ratified by all key stakeholders.[147]

Another useful parallel is the regulation of nuclear safety in international law. Although the first nuclear power plant in the world was launched already in 1954 in Obninsk, Soviet Union,[148] it took over three decades until the first international conventions on nuclear safety were adopted.[149] In the meantime, states were guided by non-binding safety standards and criteria, most of which were issued by the International Atomic Energy Agency (IAEA).[150] Afterwards, nuclear safety conventions adopted in the 1980s and 1990s[151] consolidated this emerging body of non-binding norms and made many of the relevant standards mandatory for all member states.[152] Once again, states proceeded cautiously, slowly transforming into binding law those norms that were perceived as workable and acceptable by all stakeholders.

---

[143] Notably, the Antarctic Treaty did not expressly include the protection of the Antarctic environment among the objectives of the treaty regime. However, it did encourage the contracting parties to propose measures regarding, *inter alia*, the preservation and conservation of living resources in Antarctica. Ibid., Art. IX(1)(6).

[144] Ibid., Art. IX(1).

[145] C. C. Joyner, 'The Legal Status and Effect of Antarctic Recommended Measures', in D. Shelton (ed.), *Commitment and Compliance: The Role of Non-binding Norms in the International Legal System* (2003), 163 at 175–176.

[146] See further ibid., at 179–181.

[147] Protocol on Environmental Protection to the Antarctic Treaty, 30 ILM 1455 (1991).

[148] P. R. Josephson, *Red Atom: Russia's Nuclear Power Program from Stalin to Today* (2005), 2.

[149] Convention on Early Notification of a Nuclear Accident, 1439 UNTS 275 (1986); Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, 1457 UNTS 133 (1986). Two additional conventions were adopted in the 1990s: Convention on Nuclear Safety, 1963 UNTS 293 (1994); Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management, 36 ILM 1436 (1997).

[150] For an overview of these standards, see IAEA, 'Measures to Strengthen International Co-operation in Nuclear, Radiation, Transport and Waste Safety', IAEA Doc. GC(45)/INF/3, 31 August 2001, Attachment 2, at 1–7.

[151] See note 149, *supra*.

[152] See further N. Pelzer, 'Learning the Hard Way: Did the Lessons Taught by the Chernobyl Nuclear Accident Contribute to Improving Nuclear Law?', in the Joint Report by the OECD Nuclear Energy

Of course, there are important differences between these areas of international law and the cyber security domain. Perhaps most visibly, unlike the cyber norms initiatives analysed previously, the law-making processes relating to the environmental protection in Antarctica or the global nuclear safety had been predominantly state-driven. However, that should not detract from their value as examples demonstrating the time-tested trajectory of transformation of soft law norms into hard law rules.[153]

After all, there is no doubt that non-state actors have, on many occasions, contributed to the adoption of binding multilateral international treaties. For instance, it is well known that the lawyer Raphael Lemkin played a central role[154] in campaigning for and later drafting the 1948 Genocide Convention.[155] Similarly, the 1984 Convention against Torture[156] was adopted after years of international pressure led by Amnesty International.[157] A yet more recent example is the 2008 Convention on Cluster Munitions,[158] the agreement on which was catalysed by the personal presence of survivors of cluster munition attacks at the formal negotiations.[159] To partially paraphrase Margaret Mead's famous quote,[160] non-state actors might not be the only thing that ever has changed international law, but they are certainly capable of doing so.[161]

Therefore, instead of lamenting over a supposed crisis of international law, it is more appropriate to view the current situation as an intermediate stage on the way towards the generation of cyber 'hard law'. Non-state-driven initiatives provide opportunities for states to identify overlaps with their strategic interests. In other words, these initiatives may serve as norm-making laboratories, allowing states to weigh the pros and cons of various proposals in their context and to decide on this

Agency and the International Atomic Energy Agency, *International Nuclear Law in the Post-Chernobyl Period* (2006), 73 at 86–88.

[153] See further A. Boyle and C. Chinkin, *The Making of International Law* (2007), 211–229 (exploring the significance of soft law for international law-making).

[154] See, e.g., J. Cooper, *Raphael Lemkin and the Struggle for the Genocide Convention* (2008).

[155] Convention on the Prevention and Punishment of the Crime of Genocide, 78 UNTS 277 (1948).

[156] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 1465 UNTS 85 (1984).

[157] Amnesty International, '"No safe haven for torturers" – The rocky road to the Convention against Torture', 19 November 2014, available at www.amnesty.org/en/latest/news/2014/11/no-safe-haven-torturers-rocky-road-convention-against-torture/.

[158] Convention on Cluster Munitions, 2688 UNTS 39 (2008).

[159] J. Borrie, *Unacceptable Harm: A History of How the Treaty to Ban Cluster Munitions Was Won* (2009).

[160] See text at note 1, *supra*.

[161] For a recent comprehensive discussion of the diverse roles played by non-state actors on the international plane, see M. Noortmann, A. Reinisch, and C. Ryngaert (eds.), *Non-State Actors in International Law* (2015).

basis which ones to endorse and which ones to reject. Their usefulness in this sense is confirmed by a 2015 report of the EastWest Institute, which helpfully maps out areas of convergence across various proposals of norms of state behaviour in cyberspace including those analysed in this article.[162] As noted in the report, most norm-making initiatives agree on the general principles ensuring the stability and security of cyberspace as well as on the need for state co-operation in mitigating malicious cyber incidents.[163]

5.2. Timeliness and attribution

Even if this article's contention regarding the feasibility of the soft-to-hard-law pathway in cyberspace is accepted, one might still question whether it already is the right time for states to start taking specific legislative action. It is submitted that the key to this question of timeliness can be found by unpacking the so-called attribution problem, which relates to the difficulty in determining the identity or location of a cyber attacker or their intermediary.[164] In fact, for some time, the attribution problem was rightly seen as an impediment to the development of effective legal regulation of cyber activities. It was argued that the prevailing anonymity online 'makes it difficult – if not impossible – for rules on either cybercrime or cyberwar to regulate or deter.'[165] Indeed, without the victim states being at least theoretically capable of identifying the source of malicious cyber operations against them, any attempts to design rules aimed at constraining the perpetrators of such attacks would have very limited prospects of success.

However, recent technological progress has translated into increased confidence of states with respect to attribution of cyber activities. For instance, since 2012, the US has maintained that it possesses the capacity to locate its cyber adversaries and hold them accountable.[166] It has subsequently put this position in practice by unequivocally

---

[162] G. Austin, B. McConnell, and J. Neutze, *Promoting International Cyber Norms: A New Advocacy Forum* (2015), available at issuu.com/ewipublications/docs/bgcybernorms, at 10–17.

[163] Ibid., at 15.

[164] See D. A. Wheeler and G. N. Larsen, *Techniques for Cyber Attack Attribution* (2003), 1.

[165] D. B. Hollis, 'An e-SOS for Cyberspace', (2011) 52 *Harvard International Law Journal* 374, at 378.

[166] See, e.g., Z. Fryer-Biggs, 'DoD's New Cyber Doctrine: Panetta Defines Deterrence, Preemption Strategy', *Defense News*, 13 October 2012, available at archive.defensenews.com/article/20121013/DEFREG02/310130001/DoD-8217-s-New-Cyber-Doctrine; US, *The DoD Cyber Strategy*, April 2015, available at www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, at 11–12. Compare with US, Testimony of Richard Clarke, Special Advisor to the President for Cyberspace Security, Senate Judiciary Committee, Administrative Oversight and the Courts Subcommittee, 13 February 2002, available at www.techlawjournal.com/security/20020213.asp (expressly admitting that the US had not yet had any evidence linking another state to a particular cyber attack).

attributing several high-profile cyber attacks to other states, including the 2014 'Sony hack' to North Korea[167] and the 2016 'DNC hack' to Russia.[168] In a recent publication, a US Department of Justice official made the link between cyber attribution and norm-making explicit: '[W]e will be able to use our ability to attribute malicious cyber activity to push other countries toward accepting and abiding by cyber norms.'[169]

Other countries have soon followed suit. In 2014, Canada noted that it had robust systems in place allowing it to localize cyber intrusions, including those orchestrated by state-sponsored actors.[170] In 2015, the United Kingdom stated it was 'increasingly confident in our ability to determine from where attacks come'.[171] In 2016, Germany's Federal Office for the Protection of the Constitution reported that it had been able to attribute 'electronic attacks' against targets in Germany to attackers operating from China and Russia as well as to Iranian governmental agencies.[172]

It remains debated to what extent these public statements should be taken at face value.[173] When signalling confidence with respect to their attribution capabilities, states may admittedly be motivated also by other factors, including their legitimate

[167] US Federal Bureau of Investigation (FBI), 'Update on Sony Investigation', 17 December 2014, available at www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation ('the FBI now has enough information to conclude that the North Korean government is responsible for these actions'); see also J. B. Comey, Director, FBI, 'Remarks at the International Conference on Cyber Security, Fordham University', 7 January 2015, available at www.fbi.gov/news/speeches/addressing-the-cyber-security-threat. For a recent analysis of the legality of the cyber operations in question, see C. Sullivan, 'The 2014 Sony Hack and the Role of International Law', (2016) 8 *Journal of National Security Law & Policy* 437.

[168] US, Office of the Director of National Intelligence, 'Assessing Russian Activities and Intentions in Recent US Elections', 6 January 2017, available at www.dni.gov/files/documents/ICA_2017_01.pdf, at ii ('Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election') and 2 ('In July 2015, Russian intelligence gained access to Democratic National Committee (DNC) networks and maintained that access until at least June 2016.'). For a recent analysis of the legality of the cyber operations in question, see J. D. Ohlin, 'Did Russian Cyber-Interference in the 2016 Election Violate International Law?', (2017) __ *Texas Law Review* __ (forthcoming).

[169] J. P. Carlin, 'Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats', (2016) 7 *Harvard National Security Journal* 391, at 430.

[170] Canada, Statement by the Chief Information Officer for the Government of Canada, 29 July 2014, available at news.gc.ca/web/article-en.do?nid=871449.

[171] United Kingdom, Chancellor's Speech to GCHQ on Cyber Security, 17 November 2015, available at www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

[172] Germany, Federal Ministry of Interior, *Verfassungsschutzbericht 2015 [Report on the Protection of the Constitution 2015]*, June 2016, available at www.verfassungsschutz.de/embed/vsbericht-2015.pdf, at 248–249.

[173] See, e.g., Wen Baihua, 'Obama Should Abandon Cyber Deterrence Strategy', China Military Online, 7 April 2016, available at eng.mod.gov.cn/Opinion/2016-04/07/content_4648707.htm (questioning the US-proclaimed unilateral ability to attribute).

aim to deter future attacks in general.[174] After all, to put the point at its lowest, deception is certainly not a behavioural pattern foreign to the cyber domain.[175] Nevertheless, as a matter of general trend, maintaining anonymity online is becoming more difficult and actors in cyberspace may consequently be expected to give increased consideration to the regulation of cyber conduct.

In addition to these technical considerations, significant progress has also been made in the understanding of the legal standards of attribution as applied to online conduct.[176] Although the existing law of state responsibility is certainly not without persisting uncertainties in relation to attribution of cyber operations to states, it can no longer be plausibly claimed that this area of law is unsuitable for conduct in cyberspace. On the basis of the foregoing, it can therefore be summarized that while it is probably correct that the attribution problem can at most be managed but not solved,[177] these developments show that time may be ripe for states to endorse the regulatory and deterrent potential of international legal rules.

5.3. Way forward

Building on the emerging normative convergence identified above, states have today a unique opportunity to reclaim their central role in international law-making as far as the law of cyber security is concerned. Due to the complex nature of the field and the plurality of actors that populate it at present, this will likely not be a quick or a simple process. In this regard, states' prospects of success will depend on their willingness to act in specific legislative ways that can be organized in a chronological order as short-, medium-, and long-term strategies.

In the more immediate future, states should become more forthcoming in expressing their opinion as to the interpretation of existing international law to cyber issues.[178] This will in time enable the applicable *opinio juris* to consolidate, thus

---

[174] J. R. Lindsay, 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack', (2015) 1 *Journal of Cybersecurity* 53, at 63.

[175] See, e.g., N. C. Rowe and E. J. Custy, 'Deception in Cyber-Attacks', in L. J. Janczewski and A. M. Colarik (eds.), *Cyber Warfare and Cyber Terrorism* (2008), 91 at 91–96 (survey on deception in cyber attacks).

[176] See, e.g., N. Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution', (2012) 17 *Journal of Conflict & Security Law* 229; Z. Huang, 'The Attribution Rules in ILC's Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations', (2015) 14 *Baltic Yearbook of International Law* 41; K. Mačák, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors', (2016) 21 *Journal of Conflict & Security Law* 405.

[177] T. Rid and B. Buchanan, 'Attributing Cyber Attacks', (2014) 38 *Journal of Strategic Studies* 1, at 28.

[178] For other similar calls on states to be more proactive in expressing their cyber-specific *opinio juris*, see, e.g., K. Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace', in

facilitating the process of transformation of state power into obligations of customary law.[179] In order to increase their ability to meaningfully engage in this process, all states should make the development of cyber security expertise into one of their domestic priorities; complete or update their national cyber security strategies;[180] and streamline their decision-making leading into the adoption of positions on ambiguous legal matters concerning cyber security.

Crucially, these steps may include the need to engage with those non-state actors that are currently driving the ongoing norm-making efforts.[181] States participating in the UN GGE process acknowledged as much already in their 2013 report.[182] Similarly, Microsoft included a call on states to take industry input into account in its most recent white paper.[183] Finally, in early 2016, over 50 states submitted their observations on the draft second edition of the *Tallinn Manual* to the international group of experts as part of the so-called Hague Process, a joint co-operative effort of the Dutch Ministry of Foreign Affairs and NATO CCD COE.[184] This demonstrates states' growing awareness of the importance of contributing to the international norm-making process.[185] However, the Hague Process consultations were held behind closed doors and the views submitted by the participating states have not and will not be made public.[186] As such, they cannot be seen as contributing to the formation of customary international law per se.[187] Still, the fact that so many states felt ready and able to take part in the consultations suggests that to the extent states remain silent on their *opinio*

Ziolkowski, *supra* note 92, 135 at 175; Schmitt and Vihul, *supra* note 29, at 47; Schmitt and Watts, *supra* note 33, at 230–231; Egan, *supra* note 32, at 6–7.

[179] Cf. Byers, *supra* note 10, at 18.

[180] For existing national cyber security strategies, see NATO CCD COE, 'Cyber Security Strategy Documents', 7 March 2017, available at ccdcoe.org/cyber-security-strategy-documents.html.

[181] See Section 4, *infra*.

[182] GGE Report 2013, *supra* note 14, at 7, para. 12.

[183] Charney et al., *supra* note 99, at 2; see also Smith, *supra* note 104, at 15 (highlighting the role of the industry in working with nation states on issues of cyber security).

[184] NATO CCD COE, 'Over 50 States Consult Tallinn Manual 2.0', 2 February 2016, available at ccdcoe.org/over-50-states-consult-tallinn-manual-20.html.

[185] Asser Institute, 'The Tallinn Manual 2.0 and The Hague Process: From Cyber Warfare to Peacetime Regime', 3 February 2016, available at www.asser.nl/media/2878/report-on-the-tallinn-manual-20-and-the-hague-process-3-feb-2016.pdf ('As a result of the significant impact the Tallinn Manual had, States now want to know of the progress being made and be a part of the process.').

[186] NATO CCD COE, 'Experts: Multiple International Law Regimes Apply to Cyber Operations', 11 February 2016, available at ccdcoe.org/experts-multiple-international-law-regimes-apply-cyber-operations.html.

[187] International Law Association (ILA), Final Report of the Committee on the Formation of Customary (General) International Law: Statement of Principles Applicable to the Formation of General Customary International Law (2000), at 15, principle 5 and commentary.

juris, this decision needs to be explained by factors other than the purported absence of considered legal views on their part.[188]

Although it is important for states to become more open in expressing their cyber *opinio juris*, that is but the necessary first step if they are to succeed in reclaiming a central role in international law-making. In the medium term, states should also aim to gradually overcome their current aversion to treaty commitments. There are some early signs that this process may already be underway. For example, in September 2015, the US and China concluded a 'surprising'[189] agreement to refrain from certain types of cyber espionage.[190] A series of further non-binding bilateral agreements between the key players entered into in the recent period may also gradually pave the way towards legally binding cyber treaties.[191]

Finally, this iterative process of state-appropriated norm-making could in the long run quite plausibly result in the adoption of one or several comprehensive multilateral undertakings. These would likely commence with definitional matters to enable future consensus-building over more substantive issues.[192] There are a number of terms with

[188] See, e.g., D. Bethlehem, 'The Secret Life of International Law', (2012) 1 *Cambridge Journal of International and Comparative Law* 23, at 32–33 (discussing the complexity of considerations that states must take into account before deciding whether or not to make an official statement on a question of international law).

[189] S. W. Harold, M. C. Libicki, and A. S. Cevallos, *Getting to Yes with China in Cyberspace* (2016), at x; see also ibid., at 86 (observing that the agreement was 'not something that, to the best of our knowledge, any serious commentators on either side of the Pacific had predicted before the summit took place').

[190] US, White House, 'Fact Sheet: President Xi Jinping's State Visit to the United States', 25 September 2015, available at obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states; but see P. Bittner, 'US Cabinet Officials Pull Out of China Cyber Talks After Orlando Shooting', *The Diplomat*, 15 June 2016, available at thediplomat.com/2016/06/us-cabinet-officials-pull-out-of-china-cyber-talks-after-orlando-shooting/ (reporting the downgrading of the bilateral dialogue to sub-ministerial level due to domestic developments in the US).

[191] See, e.g., Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation to Ensure International Information Security (2015), available at government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf (in Russian); UK, 'UK-China Joint Statement 2015', 22 October 2015, available at www.gov.uk/government/news/uk-china-joint-statement-2015 (agreement not to conduct or support cyber-enabled theft of intellectual property); US, 'Joint Statement on U.S.-Germany Cyber Bilateral Meeting', 24 March 2016, available at www.state.gov/r/pa/prs/ps/2016/03/255082.htm (agreement on a range of strategic and operational objectives); US, 'JOINT STATEMENT: The United States and India: Enduring Global Partners in the 21st Century', 7 June 2016, available at obamawhitehouse.archives.gov/the-press-office/2016/06/07/joint-statement-united-states-and-india-enduring-global-partners-21st (committing to finalize a cybersecurity agreement in the near term).

[192] See, e.g., Hathaway, *supra* note 29, at 877.

contested or unclear meaning, including such central notions as critical infrastructure,[193] cyber attack, cyber warfare or cybercrime.[194]

Once states agree on a shared definition of these concepts, the next step may be to turn to identification of the 'low-hanging fruit' of possible agreement on matters of substance. Their precise scope falls to be determined by further research. However, studies looking at overlaps between various norms proposals may provide some initial pointers.[195] Equally, states may be willing to act—including by legislating on the international plane—against threats that affect them all. A good example in this regard may be botnets, in other words, networks of private computers infected by malware and controlled as a group without their owners' knowledge.[196] These have rightly been described as 'a scourge to all' and a multilateral consensus to outlaw the building of such systems may indeed be within the realm of the possible.[197]

6. Conclusion

International cyber security law is at a critical juncture today. It is true that states' hesitation to engage in the development and application of international law has generated a power vacuum allowing for the emergence of non-state norm-making initiatives. Still, it would be premature to speak of a situation of crisis.

Several historical parallels show that a mixture of initial soft-law approaches combined with a growing set of binding rules can provide a logical and functioning response to a novel phenomenon. In the twenty-first century, pluralisation of norm-making processes involving diverse state and non-state actors is a common feature at the international level and it need not be feared as such.[198] Moreover, states have recently started to awake to the need to publicly express their views on how international law applies in cyberspace.[199]

To return to the quotes cited at the start of this article, initiatives by small groups of thoughtful committed people from academia, industry or elsewhere should be

[193] Shackelford, *supra* note 89, at 194 (noting that national definitions of critical infrastructure vary broadly due to an array of socioeconomic and political factors); but see Harold, Libicki, and Cevallos, *supra* note 189, at 71 (observing that US and Chinese stakeholders held 'relatively similar views of the definition of critical infrastructure').

[194] Hathaway, *supra* note 29, at 881–882.

[195] See, e.g., Austin et al., *supra* note 162.

[196] UK, House of Commons, Defence Committee, 'Defence and Cyber-security: Sixth Report of Session 2012–13', 9 January 2013, at 12, note 16.

[197] Singer and Friedman, *supra* note 34, at 187–188.

[198] See d'Aspremont, *supra* note 47, at 2–3.

[199] See, e.g., Egan, *supra* note 32, at 6–7.

welcomed because of their potential to change the world by steering the development of the law accordingly.[200] What matters is whether states will decide to respond in a way that will reaffirm their position at the heart of the international legal system also when it comes to cyber security.[201] It appears that at least some state representatives already realize that compliance with international law in fact frees them to do more, and do more legitimately, in cyberspace.[202]

Hence, it remains to be seen whether this awareness will spread and gradually translate into states' general willingness to also shape the content of the law by reclaiming their traditional central legislative role in this area. In this way, states' conduct in the next few years will determine whether we will observe a gradual demise of inter-state governance of cyberspace or a fundamental recalibration of legal approaches with states taking centre stage once again. If they want to ensure that the existing power vacuum is not exploited in a way that might upset their ability to achieve their strategic and political goals, states should certainly not hesitate too long.

[200] Cf. Mead, *supra* note 1, at 12.

[201] Cf. Higgins, *supra* note 2, at 39.

[202] Cf. Koh, *supra* note 3, at 10; see also Egan, *supra* note 32, at 14.