Is the International Law of Cyber Security in Crisis?

Kubo Mačák
Law School
University of Exeter
Exeter, United Kingdom
k.macak@exeter.ac.uk

Abstract: Several indicators suggest that the international law of cyber security is in the midst of a crisis. First, proposals of internationally binding treaties by the leading stakeholders, including Russia and China, 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 the controversial legal questions and thus to express their opinio juris. Third, instead of interpreting or developing rules, state representatives seek refuge in the vacuous term ‘norms’. This paper 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 development of information and communication technologies. In response, a number of non-state-driven norm-making initiatives have sought to fill this vacuum, such as Microsoft’s cyber norms proposal or the Tallinn Manual project. The paper 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 of international law will lead to the demise of inter-state governance of cyberspace or the recalibration of legal approaches will thus be decided in the near future. States should assume a central role in the process 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, international law, international norms, power
1. INTRODUCTION

None of the global challenges facing the modern international community can be adequately addressed by any single international actor, irrespective of how powerful that actor may be. Whether one thinks of climate change, international terrorism, or cyber threats, all such challenging contemporary phenomena necessitate a framework for international co-operation. It is international law that ‘affords [such] a framework, a pattern, a fabric for international society’.1

By establishing a framework of constraints, the law simultaneously guarantees a sphere of autonomy for its subjects.2 In the 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’,3 according to which states may generally act freely unless prevented by a contrary rule of international law.4

In order to delineate this zone of freedom for states and other international actors with respect to a new phenomenon of international significance, it is necessary to identify, interpret and apply relevant legal rules to it.5 Cyberspace, broadly understood, is precisely such a phenomenon. Crucially, the uses and abuses of this complex borderless virtual space impinge on vital state interests in the physical world, including national security, public safety, or economic development. As such, cyberspace extends far beyond the domain of internal affairs of any state.6

Yet, with respect to the management of cyberspace, it may appear that international law fails to deliver. Although the main building blocks of the Internet’s architecture were laid over two decades ago,7 it took until 2013 for state representatives to agree on the rudimentary threshold assumption that international law actually applies to cyberspace.8

Although that agreement was touted at the time as a ‘landmark consensus’,9 its actual import is controversial. It was expressed in the form of a non-binding report of a Group of Government

---

2 Cf Joseph Raz, The Morality of Freedom (Clarendon Press 1986) 155 (‘Autonomy is possible only within a framework of constraints.’).
3 See, e.g, James Crawford, The Creation of States in International Law (2nd edn, OUP 2006) 41–42 (describing the presumption as a ‘part of the hidden grammar of international legal language’).
4 PCIJ, Lotus Case (France v Turkey) (Merits) [1927] PCIJ Rep Series A No 10, 18.
5 Cf Gennady M Danilenko, Law-Making in the International Community (Martinus Nijhoff 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 United States, Department of State, ‘Statement on Consensus Achieved by the UN Group of Governmental Experts On Cyber Issues’ (7 June 2013) <http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm>.
Experts (GGE) established by the United Nations (UN) General Assembly.\textsuperscript{10} At the time, the group was composed of representatives of 15 UN member states,\textsuperscript{11} including the three ‘cyber superpowers’ China, Russia, and the United States.\textsuperscript{12} Its position can thus perhaps be taken as confirming a shared understanding in the international community.\textsuperscript{13}

Still, the report poses more questions than it answers. International law is supposed to apply, but which international law? Although the group endorsed the centrality of the UN Charter,\textsuperscript{14} several of its members have questioned the applicability of a prominent subdomain of international law – the law of armed conflict – to cyber operations.\textsuperscript{15} Perhaps more importantly, how is international law supposed to apply? It is one thing to know that the online realm is not a lawless world, but quite another to understand how its rules precisely apply to cyber phenomena.\textsuperscript{16}

Against this background, this paper examines if the current situation is fairly described as one of crisis. To that end, it weighs three key crisis indicators reverberating around states’ general reluctance to engage in law-making in the area of the international law of cyber security\textsuperscript{17} (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 paper shows that states’ retreat from their traditional legislative role has generated a power vacuum (section 4), triggering a number of non-state initiatives seeking to fill it (section 5). On the basis of historical precedents that include the development of legal regimes for Antarctica and nuclear safety, the paper 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 6). Whether they succeed in doing so and in what way will determine the answer to the overarching question of this paper.

2. CRISIS INDICATORS

Three indicators of the apparent crisis of international law stand out. First, the area of cyber security appears resistant to codification of the applicable rules in a comprehensive multilateral
binding treaty. This is not for want of trying by the leading international stakeholders. Already in 1996, France put forward the earliest proposal with the lofty title *Charter for International Cooperation on the Internet.* 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. However, none of these proposals was met with much enthusiasm by other states and scholars describe the prospects of an ‘omnibus’ treaty being adopted in the near future as slim to negligible.

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, states have been reluctant to offer clear expressions of *opinio juris* on matters related to cyber security. At times, this approach may certainly be understandable, being the consequence of a domestic political gridlock or even a deliberate waiting strategy. On the whole, however, it 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 new United States (US) *Law of War Manual* adopted in July 2015. Although it does contain a chapter on cyber operations, the Manual skirts virtually all of the

---

18 For existing sectoral and regional treaties concerning aspects of cyber security, see text to notes 40–49 below.


23 See Richard A Clarke & Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (Harper Collins 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.”).


27 Ibid ch xvi.
unsettled issues, including standards of attribution, rules of targeting or the requirement to review cyber weapons.\textsuperscript{28}

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 sought refuge in the vacuous term ‘norms’. We can see this trend most clearly 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’.\textsuperscript{29} The report claimed that such norms prevent conflict in cyberspace, foster international development, and reduce risks to international peace and security.\textsuperscript{30} The report further recommended 11 such norms for consideration by states,\textsuperscript{31} while making it clear that these norms operate on a decidedly non-legal plane.\textsuperscript{32} 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.\textsuperscript{33}

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. In legal theory, this phenomenon has been described as ‘the pluralization of international norm-making’,\textsuperscript{34} characterised by the observation that ‘only a limited part of the exercise of public authority at the international level nowadays materializes itself in the creation of norms which can be considered international legal rules according to a classical understanding of international law’.\textsuperscript{35} In order to understand the impact this situation 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. EXISTING LEGAL LANDSCAPE

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

\textsuperscript{28} See further Sean Watts, ‘Cyber Law Development and the United States Law of War Manual’ in Osula and Rõigas (n 16).


\textsuperscript{30} Ibid 7 [10].

\textsuperscript{31} Ibid 7–8 [13].

\textsuperscript{32} Ibid 7 [10].


\textsuperscript{34} Jean d’Aspremont, Formalism and the Sources of International Law (OUP 2011) 222.

\textsuperscript{35} Ibid 2.
adaptable to new phenomena without the need to reinvent an entire regulation framework on each occasion.\textsuperscript{36}

By way of an example, the UN Charter was finalised when the invention of nuclear weapons was still a closely guarded secret and this instrument thus understandably did not refer to this type of weapons in its provisions on the use of force.\textsuperscript{37} 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’,\textsuperscript{38} notwithstanding the fact that a particular type of weapons might not yet have been generally known or even invented when the Charter was adopted. Following the same logic, cyber operations must equally be subject to the international law regulation of the use of force.\textsuperscript{39}

In addition to these generally applicable rules of international law, certain sectoral and regional treaties taken together provide a ‘patchwork of regulations’ for cyber activities.\textsuperscript{40} These include, in particular, the 1992 Constitution of the International Telecommunication Union;\textsuperscript{41} the 2001 Budapest Convention on Cybercrime\textsuperscript{42} and its 2006 Protocol on Xenophobia and Racism;\textsuperscript{43} the 2009 Shanghai Cooperation Organisation’s Information Security Agreement;\textsuperscript{44} and the 2014 African Union’s Cyber Security Convention.\textsuperscript{45} 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\textsuperscript{46} or operations interfering with existing telecommunications networks\textsuperscript{47}), or have a very limited membership (six states in the case of the Shanghai Cooperation Organisation’s agreement\textsuperscript{48} and none yet in that of the African Union’s convention\textsuperscript{49}).

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.\textsuperscript{50} Moreover, states seem reluctant to engage themselves in the development and

\textsuperscript{36} Cf US, International Strategy for Cyberspace (n 24) 9.
\textsuperscript{37} Charter of the United Nations (signed 26 June 1945, entered into force 24 October 1945) 1 UNTS 16, Arts 2(4) and 39–51.
\textsuperscript{38} ICJ, Legality of the Threat or Use of Nuclear Weapons Case (Advisory Opinion) [1996] ICJ Rep 226 [39].
\textsuperscript{40} Hathaway (n 22) 873.
\textsuperscript{41} Constitution of the International Telecommunication Union (concluded 22 December 1992, entered into force 1 July 1994) 1825 UNTS 143 (hereinafter ‘ITU Constitution’).
\textsuperscript{44} Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (signed 16 June 2009, entered into force 5 January 2012) (‘Yekaterinburg Agreement’).
\textsuperscript{46} Convention on Cybercrime (n 42) Arts 2–10.
\textsuperscript{47} ITU Constitution (n 41) Art 45 (prohibiting harmful interference) and Annex (defining harmful interference).
\textsuperscript{48} Yekaterinburg Agreement (n 44).
\textsuperscript{50} See also Hathaway (n 22) 873.
interpretation of international law applicable to cyber security. This voluntary retreat has
generated a power vacuum, enabling non-state actors to move into the space vacated by states
and pursue various forms of ‘norm entrepreneurship’. 51

4. POWER VACUUM

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. 52 Nonetheless, it
needs little emphasis that the powerful normally seek to use legal regulation to consolidate and
project their power. 53 If we understand power simply as ‘the ability to alter others’ behaviour
to produce preferred outcomes’, 54 then setting legal obligations is one way how to exercise
this ability. 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.

Yet, legal uncertainty may at times be deemed desirable by even the most powerful states. 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 themselves to any binding rules that would govern outer space. Both 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.’ 55

However, cyberspace and outer space – albeit frequently lumped together as so-called ‘global
commons’ 56 – 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. 57 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 as such. In contrast, cyberspace is populated primarily by non-state actors, which
include individuals, corporations, and other more loosely organised groups. 58 The possibility of
anonymity online combined with the corresponding difficulty of attribution of cyber operations

International Organization 887.
52 Michael Byers, Custom, Power and the Power of Rules (CUP 1999) 5.
53 See further Rosalyn Higgins, Problems and Process: International Law and How We Use It (Clarendon
Press 1995) 3–4 (analysing the relationship between law and power from the perspective of international
law).
55 Stuart Banner, Who Owns the Sky? The Struggle to Control Airspace from the Wright Brothers On
(Harvard University Press 2008) 278.
56 See, e.g., Mark Barrett et al, Assured Access to the Global Commons (NATO 2011) xii; Scott Jasper and
Scott Moreland, ‘Introduction’ in Scott Jasper (ed), Conflict and Cooperation in the Global Commons
(Georgetown University Press 2012) 21; Nicholas Tsagourias, ‘The Legal Status of Cyberspace’ in
Nicholas Tsagourias & Russell Buchan, Research Handbook on International Law and Cyberspace
Osula and Rõigas (n 16) 157.
57 Scott Shackelford, Managing Cyber Attacks in International Law, Business, and Relations (CUP 2014) 58.
Studies 1, 9–23.
have resulted in the ‘dramatic amplification’ of power in the hands of these non-state actors at the expense of their state counterparts.59

The effect of legal uncertainty is thus much more complex than what we saw in relation to outer space, as it affects a far more populous spectrum of actors, state and non-state alike. Accordingly, non-state actors have now moved into the vacated norm-creating territory previously occupied exclusively by states. These developments have been primarily driven by the private sector and by the academia, as epitomised by Microsoft’s cyber norms proposal and by the so-called Tallinn Manual project.

5. NON-STATE-DRIVEN INITIATIVES

The more recent of the two, Microsoft’s proposal entitled International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World was published in December 2014.60 Interestingly, this 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.61 Still, Microsoft’s text is the first comprehensive proposal of specific standards of behaviour online, which, despite its private origin, proposes norms purporting to regulate solely the conduct of states.62 The openly proclaimed central aim of this white paper was to reduce the possibility that ICT products and services would be ‘used, abused or exploited by nation states as part of military operations’.63 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.64

In 2013, an international group of experts led by Professor Michael Schmitt published the Tallinn Manual on the International Law Applicable to Cyber Warfare.65 Although the project was undertaken under the auspices of the Estonia-based NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), the Manual makes it clear that its text should be seen as reflecting the views of the experts themselves and not the states or institutions from which they originated.66 As apparent from its title, the Manual maintains a clear military paradigm throughout, focussing on the law on the use of force (jus ad bellum) and the law of armed conflict (jus in bello).67 Its text identifies 95 rules adopted by consensus among the group of experts who

62 McKay et al (n 60) 2–3.
64 McKay et al (n 60) 2. The complete list of the proposed norms may be found in the annex to the document: ibid 20.
65 Tallinn Manual (n 39).
66 Ibid 11.
67 Ibid 5.
were guided by the ambition to ‘replicate customary international law’. 68 Early reviews of the *Manual* criticised its almost exclusive focus on activities occurring above the level of the use of force, whereas in reality, most (if not all) cyber operations fall below that threshold. 69 However, the ongoing ‘Tallinn 2.0’ project, scheduled for completion in 2016, should dispel some of these objections by turning its attention to ‘below-the-threshold’ operations and by addressing issues of state responsibility, the law of the sea, international telecommunications law, and even human rights law. 70 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.

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’. 71 As recognised in the paper itself, such policies need to be developed by each individual state and tailored to the needs of the concerned state. 72

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. 73 In other words, the *Manual* aims to interpret how ‘extant legal norms’ apply to conduct in cyberspace, 74 and not to ‘set forth *lex ferenda*’. 75 Yet, given that the *Manual* frequently puts forward detailed and novel positions, it does not always succeed in maintaining a bright line between norm interpretation and norm development. 76 Nevertheless, the purported rules it contains are much more specific than Microsoft’s cybersecurity norms. For example, rule 37 sets out the prohibition of cyber attacks against civilian objects in the context of an armed conflict. 77 Both crucial terms – ‘cyber attacks’ as well as ‘civilian objects’ – are precisely defined by the *Manual*. 78 Although some disagreements may persist about the application of the rule in particular circumstances, 79 the content of the norm is sufficiently clear and precise to generate legal rights and obligations.

However, what initiatives like Microsoft’s white paper or the *Tallinn Manual* project share is their non-state origin and expressly non-binding nature. Microsoft was keenly aware of its proposal’s

68 Ibid 6.
71 McKay et al (n 60) 12.
72 Ibid.
73 *Tallinn Manual* (n 39) 6.
74 Ibid 1.
75 Ibid.
76 See further Kubo Mačák, ‘Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law’ (2015) 48(1) Israel Law Review 55, 59–63 (discussing the distinction between *lex lata* and *lex ferenda* in the *Tallinn Manual*).
77 *Tallinn Manual* (n 39) 124.
78 Ibid 91 (definition of cyber attack) and 125 [3] (definition of civilian objects).
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.80 Similarly,
the Manual noted in its opening pages that it was meant to be ‘a non-binding document’.81 As
the texts in question 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’.82

If these texts are non-binding, one might question their relevance from the perspective
of international law altogether. True, their normativity (in the sense of the strength of their
claim to authority83) is lower than that of international legal rules. 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’.84 Moreover, they render the law-making process more multilateral and inclusive
than the traditional state-driven norm-making can ever be.85 Therefore, the crucial question is
whether states decide to pick up the gauntlet thrown at them by their non-state counterparts and
reclaim their role as principal lawmakers.

6. STATES AT A CRITICAL JUNCTURE

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.86 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 has been eventually
subjected to a binding legal regime,87 despite the strong initial reluctance of the dominant
spacefaring states.88

Other domains with a higher number of participants may provide more appropriate analogies.
For instance, in the context of Antarctica, many non-binding norms were put forward in the
1960s and 1970s with the aim to conserve living and non-living resources of the Antarctic

80 McKay et al (n 60) 3.
81 Tallinn Manual (n 39) 1.
82 Stefan Talmon, ‘The Security Council as World Legislature’ (2005) 99 AJIL 175, 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.
83 Samantha Besson, ‘Theorizing the Sources of International Law’ in Samantha Besson & John Tasioulas
(eds), The Philosophy of International Law (OUP 2010) 173.
84 Hugh Thirlway, The Sources of International Law (OUP 2014) 164, paraphrasing Mary E O’Connell, ‘The
Role of Soft law in a Global Order’ in Dinah Shelton (ed), Commitment and Compliance: The Role of Non-
Binding Norms in the International Legal System (OUP 2000) 100.
85 Besson (n 83) 170–171.
86 Cf Patrick W Franzese, ‘Sovereignty in Cyberspace: Can It Exist?’ (2009) 64 Air Force Law Review 1, 38;
Schmitt and Vihul (n 22) 38.
87 See, principally, 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 (opened for signature 27
88 See text to n 55 above.
environment. These norms gradually evolved into the 1991 Antarctic Environmental Protection Protocol, a complex binding instrument that has since been ratified by all key stakeholders.

Similarly, it took over three decades since the 1954 launch of the first nuclear power plant in the world in Obninsk, Soviet Union, until the first international conventions on nuclear safety were adopted. 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). Afterwards, nuclear safety conventions consolidated this emerging body of non-binding norms and made many of the relevant standards mandatory for all member states.

As these examples demonstrate, 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 and they may serve as norm-making laboratories. Their usefulness in this sense is confirmed by a recent 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 paper.

A final point to consider is the so-called attribution problem (understood as the difficulty in determining the identity or location of a cyber attacker or their intermediary). For some time, it 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.’ However, recent technological progress has translated into increased confidence of states with respect to attribution of cyber activities. For instance, the US has claimed that it now has the capacity

---


to locate its cyber adversaries and hold them accountable.98 In a similar statement, Canada noted that it has robust systems in place allowing it to localise cyber intrusions, including those orchestrated by state-sponsored actors.99 Significant progress has also been made in the understanding of the legal standards of attribution as applied to online conduct.100 Although it is probably correct that the attribution problem can at most be managed but not solved,101 these developments show that time may be ripe for states to endorse the regulatory and deterrent potential of international legal rules.

Building on the emerging normative convergence identified above, states should be able to reclaim their central role in international law-making. In the more immediate future, they should become more forthcoming in expressing their opinion as to the interpretation of existing international law to cyber issues.102 This will in time enable the applicable opinio juris to consolidate, thus facilitating the process of transformation of state power into obligations of customary law.103 Additionally, states should gradually overcome their current aversion to treaty commitments. Reports from late 2015 that the US and China started negotiating a binding arms control treaty for cyberspace are possible early signs that this process is already underway.104 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, possibly commencing with definitional matters to pave the way towards future consensus-building over more substantive issues.105

7. CONCLUSION

International law of cyber security 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

---

102 For other similar calls on states to be more proactive in expressing their cyber-specific opinio juris, see, e.g., Katharina Ziolkowski, ‘General Principles of International Law as Applicable in Cyberspace’ in Ziolkowski (n 59) 175; Schmitt and Vihul (n 22) 47; Schmitt and Watts (n 25) 230–231.
103 Cf Byers (n 52) 18.
105 See, e.g., Hathaway (n 22) 877.
phenomenon. In the 21st 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.106

What matters is whether, and to what extent, states will reclaim their traditional central legislative role. Their 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.

ACKNOWLEDGMENTS

I am grateful to Louise Arimatsu, Ana Beduschi, Russell Buchan, Michael N. Schmitt, and the anonymous reviewers for their valuable comments and suggestions on earlier drafts of this paper. Any remaining errors or omissions are my own responsibility.

106 See d’Aspremont (n 34) 2–3.