ESIL Reflections

9 June 2017 Volume 6, Issue 5

Yuri Samoilov (cc)

Cyber Insecurity and the Politics of International Law

Barrie Sander
Visiting Researcher, FGV Direito Rio, Brazil

In recent decades, cyberspace has become woven into the fabric of societies around the world. Consider, for example, that by 2020, it is estimated that there will be over 26 billion Internet-connected devices and over 4 billion Internet users around the world.[1] However, cyberspace extends beyond the Internet, constituting a globally interconnected network of information and communications technologies (ICTs), comprised of at least four interrelated layers:[2] a *physical* layer, which includes the servers, fibre-optic cables and other infrastructure that enable the network to operate; a *logical* layer, which includes the Internet protocols, the World Wide Web, and software that make use of the physical infrastructure; an *information* layer, encompassing the text, photos, videos and other content that is stored and transmitted through the network; and a *social* layer, encompassing the users who operate on the network.

The open and global nature of cyberspace has generated significant societal opportunities for social and economic development, as well as governmental transparency and efficiency. Equally, however, the multi-layered structure of cyberspace, in conjunction with the propensity of societies to increasingly depend on ICTs to control many of their critical infrastructures and communications systems, has also led to growing concerns over cybersecurity.[3] As Finnemore and Hollis recently observed, in the current climate "cyber *in*security has become the new normal".[4]

[1] S. Baller et al., *The Global Information Technology Report 2016: Innovating in the Digital Economy* (World Economic Forum, 2016), at ix.

[2] N. Chocri and D.D. Clark, 'Who controls cyberspace?', 69 *Bulletin of the Atomic Scientists* (2013) 21, at 22. For an overview of the regulation of cyberspace by public international law, see generally K. Kittichaisaree, *Public International Law of Cyberspace* (Springer, 2017).

[3] See, in this regard, K.B. Sandvik, 'Towards a Militarization of Cyberspace? Cyberwar as an Issue of International Law', *Peace Research Institute Oslo (PRIO) Paper* (2012), at 23-26 (summarising the different forms of "threat framing" identifiable in cyber discourse).

[4] M. Finnemore and D.B. Hollis, 'Constructing Norms for Global Cybersecurity', 110 *American Journal of International Law* (2016) 425, at 426 (emphasis in original).

Although subject to significant contestation,[5] cybersecurity may be defined as the protection of ICTs from unauthorized access that leads to a loss of at least one of the following:[6] *confidentiality* (accessing confidential data without authorization); *integrity* (changing data to generate fabricated information or results); *authenticity* (concealing or falsifying the source of data); and/or *availability* (blocking or impeding access to the ICT). These hostile cyber activities occur when adversaries – ranging from hackers and activists to organized criminals and states – learn about, gain access to, and exploit vulnerabilities, namely weaknesses that make ICTs susceptible to infiltration by unauthorized actors.[7]

Hostile cyber activities vary in terms of their duration, scale and indirect effects.[8] The latter variable is particularly significant since losses of confidentiality, integrity, authenticity and availability are typically designed with other spill-over effects in mind. Notorious examples include the Stuxnet virus used to disrupt Iran's nuclear facilities in 2009 and 2010, [9] the surveillance activities of the US National Security Agency alleged in the disclosures of Edward Snowden in 2013,[10] and the WannaCry ransomware that attacked computers across the world earlier this year.[11]

As the threat landscape in cyberspace has become multifaceted, characterised by an increasing number and range of vulnerabilities and actors, the question of cybersecurity has been placed firmly on the international agenda. Today, the question is no longer *whether*, but *how* cyberspace should be governed in order to ensure cybersecurity around the world. It is in this context that international lawyers have also begun wrestling with the question of how they might contribute to the security and stability of cyberspace.[12]

Against this background, this post seeks to map the different modalities by which international lawyers have attempted to promote and preserve cybersecurity to date. The post begins by identifying two of the most common modalities of engagement: first, as *law-articulators*, international lawyers have sought to identify the extent to which existing international legal frameworks already apply to cyber activities; and second, as *law-entrepreneurs*, international lawyers have sought to devise new international rules to respond to the unique challenges posed by cybersecurity. Bearing in mind the limits of these forms of engagement, the post identifies the emergence of a third modality: as

[5] See generally, T. Maurer and R. Morgus, *Compilation of Existing Cybersecurity and Information Security Related Definitions* (New America, 2014).

[6] Finnemore and Hollis (n 4), at 431; and D.B. Hollis, 'An e-SOS for Cyberspace', 52 *Harvard International Law Journal* (2011) 373, at 380.

[7] Finnemore and Hollis (n 4), at 432-436.

[8] Hollis (n 6), at 380-383.

[9] C. Baylon, 'Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare', in M. Taddeo and L. Glorioso (eds.), *Ethics and Policies for Cyber Operations* (Springer, 2017) 213.

[10] 'Decoded: The Main Stories from the Snowden Files Explained', *The Guardian*, 2 December 2013.

[11] 'Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool', *The New York Times*, 12 May 2017.

[12] See also, J. d'Aspremont, 'Cyber Operations and International Law: An Interventionist Legal Thought', 21 *Journal of Conflict & Security Law* (2016) 575 (characterising such contributions as "interventionist").

norm-articulators and *norm-entrepreneurs*, international lawyers are beginning to broaden their perspective beyond international cyber *law* towards a concern for global cyber *norms*.

Ultimately, the post aims to shed light on the *politics* of these different modalities of engagement – where “politics” is understood to refer to the choices confronted by international lawyers in their attempts to respond to perceived problems of the world with a view to managing them. In this vein, the post seeks to offer a clear illustration of how the engagement of international lawyers in a particular context constitutes an expression of the political.[13]

International Lawyers as *Law-Articulators*: Extending Existing International Legal Frameworks into Cyberspace

To date, international lawyers have primarily engaged with issues of cybersecurity by examining the extent to which existing international legal frameworks already apply to cyber activities. As Jean d’Aspremont recently explained, the popularity of this form of engagement reflects a clear preference amongst international lawyers for “elevating themselves into the managers of contemporary problems, whilst keeping any explicit legislative role at bay”.[14] This posture has also been legitimised by states and international organisations, many of which have affirmed the application of existing international law to cyber activities.[15]

As law-articulators, international lawyers are unavoidably embroiled in the argumentative practice of legal interpretation.[16] When engaging in this practice, international lawyers tend to premise their authority on two claims:[17] first, an impersonal claim of objectivity and independence rooted in their reliance on the doctrine of sources and rules of interpretation; and second, a personal claim of expertise rooted not only in their own reputation but also the reputations of the international lawyers whose prior work they rely upon to support their interpretations.[18]

Yet, despite the self-professed apolitical nature of this modality of engagement, the practice of interpretation inevitably engages law-articulators in what may be termed the *politics of definition* and the *politics of uncertainty*.

[13] M. Koskenniemi, *The Politics of International Law* (Hart Publishing, 2011), at v-vii.

[14] d’Aspremont (n 12), at 583.

[15] For a useful summary of various statements, see M. Roscini, *Cyber Operations and the Use of Force in International Law* (OUP, 2014), at 20-32.

[16] See generally, I. Venzke, *How Interpretation Makes International Law: On Semantic Change and Normative Twists* (OUP, 2012).

[17] O. Kessler and W. Werner, ‘Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare’, 26 *Leiden Journal of International Law* (2013) 793, at 802-806.

[18] See, in this regard, L.J.M. Boer, ‘‘The greater part of jurisconsults’: On Consensus Claims and Their Footnotes in Legal Scholarship’, 29 *Leiden Journal of International Law* (2016) 1021.

The *politics of definition* has both macro and micro dimensions. On a macro-level, the term refers to the practice of defining cybersecurity issues by reference to particular fields of international law – for example, international humanitarian law, international human rights law, the law on the use of force – so as to open the door for applying the particular technical idioms associated with those fields. The choice of vocabulary can have a significant impact on how cybersecurity is understood, rendering "some aspect of the carriage visible, whilst pushing other aspects to the background, preferring certain ways to deal with it, at the cost of other ways".[19] In the cybersecurity context, for example, it is notable that there has been a relative abundance of scholarship examining the contours of the law governing cyber warfare, with less attention devoted to defining a law of cyber peace.[20]

On a micro-level, the politics of definition refers to the interpretative choices, or "argumentative twists",[21] made by international lawyers for the purpose of extending the application of particular international rules and principles to cyber activities. In the cybersecurity context, international lawyers have frequently resorted to a "law-by-analogy" interpretative approach whereby "the extent to which cyberspace and the context that generated the existing rule are similar (or dissimilar) serves to delimit the basic boundaries of the existing international law".[22]

Analogical reasoning is not a unidimensional practice, but encompasses a number of different forms. For instance, pursuant to *consequentialist* analogical reasoning, cyber activities have been found to fall within the scope of international legal concepts such as "use of force" or "armed conflict" by demonstrating that the effects of such activities are sufficiently similar to kinetic operations.[23] By contrast, pursuant to *conceptual* analogical reasoning, the precise content of certain international legal obligations deemed applicable to cyber activities – for instance, the obligation of due diligence – has been found to hinge on the conceptual similarity between cyberspace and the contexts regulated by other fields of law such as international environmental law, the law of sea, and the law of counter-terrorism.[24] Importantly, both the decision to rely on analogical reasoning, as well as the precise analogies drawn, are not automatic or given, but constitute choices on the part of international lawyers engaged in the interpretative exercise.

[19] M. Koskenniemi, 'The Politics of International Law – 20 Years Later', 20 *European Journal of International Law* (2009) 7, at 11.

[20] See, however, M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017) (expanding the scope of inquiry of the Tallinn Manual to cover peacetime legal regimes).

[21] d'Aspremont (n 12), at 584.

[22] D.B. Hollis, 'Re-Thinking the Boundaries of Law in Cyberspace', in J.D. Ohlin et al. (eds.), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP, 2015) 129, at 144.

[23] C. Focarelli, 'Self-defence in cyberspace', in N. Tsagourias and R. Buchan (eds.), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2015) 255, at 281.

[24] See, for example, I.Y. Liu, 'State Responsibility and Cyberattacks: Defining Due Diligence Obligations', 4 *Indonesian Journal of International & Comparative Law* (2017) 191 (examining the extent to which a cyber due diligence obligation can be derived by analogy with due diligence models within international environmental law, the law of the sea, and the law of counter-terrorism).

Turning to the *politics of uncertainty*, this term encompasses the various ways in which international lawyers produce legal uncertainty through their interpretative practices. Legal uncertainty is an inevitable outcome of the tension between the competing prerogatives of stability and change that confront international lawyers attempting to extend existing legal frameworks to new technologies.[25] In their analysis of the first edition of the *Tallinn Manual on Cyberwarfare*, Kessler and Werner identify three ways in which international lawyers may "officially stamp uncertainty" regarding the application of existing international legal rules to the particular context of cyberwarfare:[26] first, by expressly notifying the existence of irreconcilable views concerning the content of a particular rule; second, by reaching consensus that a particular rule is too under-determined to draw any definitive conclusions regarding its precise content; and finally, by introducing open-ended contextual factors into the reasoning process, the ambiguous status and content of which end up exacerbating the uncertainties they were intended to alleviate. Again, these uncertainties are not automatic or given, but constructed by international lawyers through their interpretative practices.

As this analysis reveals, far from a neutral enterprise, attempts to extend the application of existing international legal frameworks to the cybersecurity context have confronted international lawyers with a range of choices that render their engagements inescapably political.

Yet, acknowledging the political nature of such engagements merely begs the question as to the *quality* of the politics that they represent.[27] In this regard, it is notable that the recent surge in engagements of this nature has been accompanied by a significant degree of skepticism in certain quarters, with some international lawyers questioning the capacity of existing international law to adequately promote and preserve cybersecurity in practice. For instance, Duncan Hollis has argued that the law-by-analogy interpretative approach suffers in terms of both *coverage* – leaving a high number of cyber activities unregulated – and *compliance* – providing insufficient answers to the challenge of attributing specific violations to particular actors in cyberspace.[28] In a similar vein, Carlo Focarelli has raised concerns about the constructed ambiguities that result from these types of interventions, specifically arguing that analogical reasoning in use of force contexts "may disguise, given the high uncertainty of the analogized rules deemed to be applied, the willingness of a few strong States to free ride 'legitimately' with no really constraining rules".[29] In light of such concerns, some international lawyers have turned their attention to devising new international rules specifically attuned to cyberspace.

[25] Kessler & Werner (n 17), at 801-802.

[26] Kessler & Werner (n 17), at 806-809.

[27] See generally, J.N. Shklar, *Legalism – Law Morals, and Political Trials* (Harvard University Press, 1964).

[28] Hollis (n 22), at 150-153.

[29] Focarelli (n 23), at 281.

International Lawyers as *Law-Entrepreneurs*: Designing New International Rules for Cyberspace

In recent decades, international legal scholarship has experienced increasing hostility towards prescriptive interventions,[30] instead favoring either the practice of legal articulation outlined above or diagnostic critical analyses which have sought "to bring to the surface that *underlying world of beliefs* that controls our institutional practices, and accounts for the way decisions are made and resources are distributed".[31] With respect to cybersecurity, however, the limits of legal articulation, as well as the paucity of legal practices for critical discourse to critique,[32] have created space for a number of international lawyers to propose new international rules specifically tailored to promoting and preserving cybersecurity.

In contrast to law-articulators, law-entrepreneurs tend to premise their authority on demonstrating that cyberspace constitutes a context so qualitatively distinct from existing environments that new international rules are required to regulate it – referring, for example, to the multi-layered architecture of cyberspace and the complex interaction of public and private actors within it.[33] Similar to legal articulation, however, these more prescriptive interventions are also political, presenting international lawyers with a range of choices concerning the precise scope and content of their proposals.

In terms of *scope*, proposals have ranged from global treaties governing a broad range of cybersecurity issues to more focused approaches that seek to alter particular international rules in light of the specific attributes of cyberspace. Advocates of the former approach have emphasized the importance of establishing baseline agreement on defining the security problems encountered in cyberspace. Oona Hathaway and her colleagues, for example, have proposed the establishment of a new multilateral treaty to define the notions of cyber-attack, cyber-crime and cyber-warfare, which could serve as a foundation for domestic criminal legislation as well as more extensive international cooperation.[34] By contrast, advocates of the latter "bottom-up" approach have emphasized the advantages of reduced complexity and enhanced feasibility that a more focused examination of particular international rules might deliver. Duncan Hollis, for example, has called for the recognition of a "Duty to Hack" in international humanitarian

[30] See similarly, d'Aspremont (n 12), at 593.

[31] M. Koskenniemi, 'What is Critical Research in International Law? Celebrating Structuralism', 29 *Leiden Journal of International Law* (2016) 727, at 733 (emphasis in original).

[32] See, in this regard, J. Stewart, 'Thin Justice as an Escape from Koskenniemi's Long Shadow?', *Blog of James G. Stewart*, 29 November 2016 ("there was always a nagging sense that […] critical discourse […] depended on an intellectual division of labor that was never fully realized without a constructive normative field to rail against").

[33] M. Hoisington, 'Regulating Cyber Operations Through International Law: In, Out or Against the Box?', in M. Taddeo and L. Glorioso (eds.), *Ethics and Policies for Cyber Operations* (Springer, 2017) 87, at 94-96.

[34] O.A. Hathaway et al., 'The Law of Cyber-Attack', 100 *California Law Review* (2012) 817, at 880-884.

law, which would require that "states use cyber operations in their military operations when they are the least harmful means available for achieving military objectives".[35]

With respect to *content*, proposals have focused on a diversity of issues, encompassing new primary rules identifying affirmative duties related to cyber activities,[36] new secondary rules aimed at overcoming challenges of attributing responsibility for cyber activities,[37] as well as calls to establish new international bodies with mandates tailored to the cybersecurity context.[38]

As this overview indicates, considerable energy has already been devoted to devising new ways to regulate cyber activities using the vocabularies of international law. However, what is particularly striking about such practices has been the general failure of international lawyers to take seriously the processes by which their proposed rules might come into being. This is an especially important issue in the cybersecurity context where the diverse range of actors with competing interests and value systems, together with the fast pace of technological change, can make garnering sufficient political traction to adopt new international rules particularly challenging.[39] At least partially with this challenge in mind, some international lawyers have begun shifting their analytical perspective beyond the confines of international cyber *law* towards a broader concern for the production of global cyber *norms*.

International Lawyers as *Norm-Articulators* and *Norm-Entrepreneurs*: From International Cyber Law to Global Cyber Norms

Reflecting on twenty years of collaboration between scholars of international law and international relations, Anne-Marie Slaughter recently identified "liberty and security in virtual space" as a priority area for this type of interdisciplinary work in the future.[40] According to Slaughter, the principal value of such collaborative efforts in the past has been to enable scholars from both disciplines "to draw on a wider range of sources and

[35] Hollis (n 22), at 156.

[36] See, for example, Hollis (n 6) (proposing an e-SOS system, pursuant to which states should recognise a duty to assist victims of the most severe cyber threats regardless of their ability to identify those responsible).

[37] See, for example, N. Tsagourias, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts', 21 *Journal of Conflict & Security Law* (2016) 455, at 467-474 (proposing holding non-state actors that exercise effective power over territories and people directly responsible for their malicious cyber activities).

[38] See, for example, Liu (n 24), at 224-231 (proposing the establishment of a new committee modelled on the UN Security Council's Counter-Terrorism Committee to regulate international capacity building efforts for cyber due diligence).

[39] T. Erskine and M. Carr, 'Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace', in A-M. Osula and H. Rogias (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE Publications, 2016) 87, at 96-97; and Finnemore and Hollis (n 4), at 457-458.

[40] A-M. Slaughter, 'International Law and International Relations Theory: Twenty Years Later', in J.L. Dunoff and M.A. Pollack (eds.), *Interdisciplinary Perspectives on International Law and International Relations: The State of the Art* (CUP, 2013) 613, at 621.

intellectual perspectives to ask questions and generate insights on an issue that would not necessarily occur to a scholar working only in IR or IL".[41]

In the cybersecurity context, these types of interdisciplinary collaborations are beginning to emerge in response to calls to articulate and cultivate global cybersecurity *norms*. Such calls are identifiable not only within scholarship, but also amongst states, international organizations, industry actors, civil society groups and academic institutions.[42]

Norms and laws are overlapping but distinct concepts.[43] A "norm" is generally understood to refer to "collective expectations for the proper behavior of actors with a given identity".[44] As such, whilst a norm might be codified in law, and a law might serve as a basis for generating a norm, the two are not equivalent. For instance, a law might fail to generate sufficiently internalized expectations amongst its target actors to generate a norm, whilst a norm might arise from voluntary and non-binding bases such as political agreements or professional-cultural commitments.

Importantly, adopting a norm-perspective has the potential to significantly expand the horizons of international lawyers in their efforts to respond to cyber insecurity:[45] first, by bringing into analytical focus a broader range of normative bases beyond international law – including political, professional and cultural commitments; and second, by providing a more flexible avenue for regulating non-state actors – such as individuals and industry actors – free from the strictures of international legal frameworks.

Whilst it remains to be seen the extent to which international lawyers will shift their analytical perspective in this direction, such a move would open up new avenues of engagement. As *norm-articulators*, international lawyers could trace the evolution and regression of cybernorms amongst particular categories of actors.[46] As *norm-entrepreneurs*, international lawyers could design proposals for new cybernorms, relying on a broader range of tools and processes to try to generate their internalization within particular communities.[47] In either case, beyond expanding the choices open to international lawyers in responding to cyber insecurity, such engagements would also constitute a more or less conscious attempt to heighten their relevance within cybersecurity discourse.[48]

[41] ibid, at 614.

[42] Finnemore and Hollis (n 4), at 426-427 and 436-437.

[43] Finnemore and Hollis (n 4), at 441-442; and Erskine and Carr (n 39), at 90-91.

[44] Finnemore and Hollis (n 4), at 438 (citing Katzenstein).

[45] See generally, Finnemore and Hollis (n 4); and Erskine and Carr (n 39).

[46] Erskine and Carr (n 39), at 93 and 107.

[47] Finnemore and Hollis (n 4), at 436-456.

[48] See generally, J. d'Aspremont, *Formalism and the Sources of International Law* (OUP, 2011), at 133-134.

Conclusion

Cybersecurity does not speak for itself; it is constructed by the way in which participants in the field look at it. As art historian John Berger famously observed, “We only see what we look at. To look is an act of choice”.[49] In his landmark text *Ways of Seeing*, Berger illustrates this point by explaining how the reproduction of the image of Venus in Botticelli’s *Venus and Mars*, in isolation from the rest of the painting, can transform the way the image is seen. By zooming in on a detail and extracting it from the whole, its meaning is modified: “An allegorical figure becomes a portrait of a girl”.[50] Such a perspective is similar to what has commonly been referred to as the “politics of framing”.[51] The way an issue is framed can have a significant bearing on the way it is analyzed, explained or justified. And since there are no self-evident ways to handle issues, the practice of framing may be characterised as an exercise in politics.[52]

By mapping the different ways that international lawyers have engaged in the promotion and preservation of cybersecurity, this post may also be understood as an exercise in framing. The modes of engagement identified in this post are not given or inevitable, but have been constructed on the basis of the author’s observational viewpoint of the international landscape of cybersecurity.

By examining the different ways in which international lawyers have engaged with issues of cybersecurity, this post has also revealed the politics of framing *within* each mode of engagement. Specifically, the post has revealed how each mode confronts international lawyers with choices through which they frame their response to the threats and vulnerabilities of cyberspace. Looking to the future, it remains to be seen how these frames will evolve and whether new frames of engagement – a critical frame for example – will begin to emerge.

Cite as: Barrie Sander, “Cyber Insecurity and the Politics of International Law” 6:5 *ESIL Reflection* (2017).

[49] J. Berger, *Ways of Seeing* (BBC and Penguin Books, 1972), at 8.

[50] ibid, at 25.

[51] J. Klabbers and T. Piiparinen, ‘Normative Pluralism: An Exploration’, in J. Klabbers and T. Piiparinen (eds.), Normative Pluralism and International Law: Exploring Global Governance (CUP, 2013) 13, at 25.

[52] ibid.