Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace

Jacqueline Eggenschwiler and Joanna Kulesza

Cite as: Eggenschwiler, Jacqueline, and Joanna Kulesza. 2020. "Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace." In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi van den Berg, 245-262. London: Rowman & Littlefield International.

More information about the book and The Hague Program for Cyber Norms is available on:

www.thehaguecybernorms.nl

Chapter 12

Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace

Jacqueline Eggenschwiler and Joanna Kulesza

Over the past two decades, the public domain has experienced far-reaching phases of reconstitution (Ruggie 2004). Forces of globalization and technological advancement have added new degrees of complexity to international affairs and have given rise to a pluralization of actors. Polymorphous non-state actors have come to inhabit central areas of international steering and policy-making, including among others, cybersecurity.

A realm of rising political, economic, and cultural relevance, cybersecurity has been subject to considerable non-state actor engagement. Non-state actors have been key contributors to the development and expansion of cyberspace. In addition to producing hard- and software and providing technological services, they have also come to contribute to the development of global cybersecurity norms. Their normative contributions have, however, received little academic attention so far (Hall and Biersteker 2002; Ruggie 1993). With a view to addressing this deficiency, this chapter seeks to uncover the parts played by non-state actors in processes of international cybersecurity norm-construction.

Drawing on secondary academic literatures in the fields of international relations and international law, as well as primary case materials, this chapter claims that non-state actors have come to exert considerable clout over endeavors of international norm-construction, particularly as active proposers of norms of responsible behavior for state and non-state actors, and contributors to the emergence of international custom. As non-state actors continue to make their voices heard in debates about appropriate conduct in cyberspace, it is important to shed light on their contributions with a view to better understanding current practices and frames of international

cybersecurity governance. The discussions of the roles of non-state actors are exemplary rather than comprehensive but help identify key features and developments.

The term *non-state actors* comprises and refers to a great number of different agents, including among others, multinational enterprises, academic communities, non-governmental organizations, as well as civil society entities, all of which would warrant their own in-depth analysis. Rather than engaging in single case studies, this chapter seeks to identify common threads of normative engagement across a broad variety of non-state actors.

The remainder of this chapter is organized along three sections. The first section summarizes key literatures related to the topic under investigation, recaps important developments, and specifies central concepts such as non-state actors and norms. The second section examines and appraises the contributions of non-state actors to processes of international cybersecurity norm-construction. Finally, the third section sums up the findings and highlights avenues for further research.

LITERATURE REVIEW

The advent of non-state actors on the international plain has presented state-oriented scholarly disciplines, including international law and international relations, with formidable theoretical and practical challenges. Non-state actors have added new layers of complexity to traditional (hierarchical) schemes of international ordering and have challenged conventional sources of agency. Yet, in order to "understand how change occurs in the world polity, [it is necessary] to unpack the different categories of transnational actors and understand the quite different logic and processes in these different categories" (Keck and Sikkink 1999, 99).

Defined in the negative, the term *non-state actors* constitutes a residual category that comprises a broad range of actors other than states (Bianchi 2011). It encompasses both bene- and malevolent individuals and entities. According to Wagner, it is impossible to identify these entities "by common sociological features as they include, inter alia, international organisations, corporations, non-governmental organisations (NGOs), de facto regimes, trade associations, and transnational corporations, terrorist groups and transnational criminal organisations" (Wagner 2009). To somewhat narrow the group of possible subjects of inquiry, this chapter only considers the contributions of benevolent non-state actors to processes of international cybersecurity norm development, that is, the contributions of those that actively seek to promote appropriate conduct in cyberspace and aspire to *improve* the overall state of global cybersecurity.

Debates about the need for rules of the road regulating the conduct of state and non-state entities in cyberspace have acquired increasing prominence over the past decade. In the face of proliferating cybersecurity incidents and reluctance on the parts of governments to agree on and enact legally binding rules at the global level, less formal, norms-based discussions have emerged as alternative pathways to formal regulation.[1] In contrast to binding legal statutes, norms as understood here denote voluntary "standard[s] of appropriate behaviour for actors with a given identity" (Finnemore and Sikkink 1998, 891). They define legitimate social purposes that enable and constrain the behavior of international actors (Florini 1996). "What distinguishes norms from other social facts (e.g., customs, traditions, values, or fashions) is their prescriptive quality, the sense of oughtness attached to them. . . . They are 'prescriptive generalization'. Or, in Onuf's more extended definition, norms (or rules) 'address some class of agents, describe some class of actions as appropriate conduct for those agents, and link agents and standards with ought-statements: agents ought to behave in accordance with standards'" (Sandholtz 2017, 2).

Since the late 1990s, norms have figured prominently across a great variety of research agendas and have witnessed extensive theorization (Keck and Sikkink 1999; Sandholtz 2017; Winston 2017). Constructivist international relations scholars, in particular, have made important contributions to advancing analytically more rigorous understandings of international norms and the roles of non-state actors in changes to normative ideas. Ideational efforts conducted by non-state actors have been subsumed under the analytical umbrella of norm entrepreneurship. Norm entrepreneurship refers to activities conducted by agents with a view to persuading others to adopt new standards of appropriateness and change social understandings (Sjöström 2010; Finnemore and Sikkink 1998). Agents engaging in norm entrepreneurship, so-called norm entrepreneurs, typically promote new understandings of appropriate conduct and mobilize other entities or network of entities to support their normative ideas. These coalitions then "bring pressure to bear from above (transnationally) and below (domestically)" and help the norms advocated to cascade, and eventually become internalized into domestic and international legal codes and institutions (Sandholtz 2017, 2).

A field of growing political importance and social relevance, cybersecurity has seen a number of noteworthy initiatives relating to the creation of international norms (Nye 2018; Hinck 2018). Discussions concerning the creation of rules of the road to curb malicious behavior in cyberspace can be traced back to the mid-1990s. In 1996, the Council of the European Union endorsed a proposal put forward by the French government for a *Charter for International Cooperation on the Internet* (Mačák 2017). At the time, "the French

Minister for Information Technology expressed hope that the initiative would lead eventually to an accord comparable to the international law of the sea" (Wu 1998, 660). The French proposition was followed by a Russian bid in the remit of the UN General Assembly, which sought to ban information weapons and their use by way of enacting legally binding rules. Moscow's draft resolution emerged in consideration of a perceived Western dominance of the ICT landscape, and gave rise to more institutionalized international discussions.

In reaction to Russia's proposal of 1998, and as a result of concerns over the appropriateness of legally binding provisions, particularly on the parts of Western states, the UN GA's First Committee called to life a Group of Governmental Experts to study existing and emerging threats emanating from the digital realm and possible normative measures to address them. The first of a total of five groups met in 2004. While the UN GGEs meeting between 2009 and 2015 managed to issue non-binding consensus reports, the groups convening between 2004–2005 and 2016–2017 did not produce corresponding documents (Väljataga 2017).

Subsequent to the 2016–2017 UN GGE's inability to agree on a consensus report, and following major cybersecurity incidents of transnational magnitude, including WannaCry and Petya/NotPetya, there has been a noticeable surge in the number of non-state initiatives directed at fostering responsible behavior in the virtual domain (Hern 2017). Examples include, among others, the University of Leiden's and ICT4Peace Foundation's co-sponsorship of a *Global Commentary on Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology*, Microsoft's proposal for a *Digital Geneva Convention*, its adoption of a *Cybersecurity Tech Accord*, its initiation of a *Digital Peace Now* campaign, and its support of *the Paris Call for Trust and Security in Cyberspace*, Siemens' conclusion of a *Charter of Trust*, as well as the Global Commission on the Stability of Cyberspace's (GCSC) calls for the *Protection of the Public Core of the Internet*, the safeguarding of electoral infrastructures, and the release of the *Singapore Norms Package* (Smith 2017b, 2018; Siemens 2018a; Global Commission on the Stability of Cyberspace 2017a; ICT4Peace Foundation 2018; Global Commission on the Stability of Cyberspace 2018a).

In what follows, the activities of these actors are highlighted in more detail. Against the background of lacking political agreement at the intergovernmental level and a halting emergence of international hard law directed at addressing the challenges pertaining to nefarious conduct in the digital realm, efforts led by non-state actors deserve particular analytical attention in terms of fostering international peace, security, and stability.

THE NORMATIVE CONTRIBUTIONS OF NON-STATE ACTORS

Non-state actors have been central to the growth and spread of ICTs.[2] As operators of key network infrastructures, developers of products and suppliers of services, they have made important contributions to the "international [. . .] architecture for the governance of cyberspace" (Radu 2014, 4). Apart from acting as executors of public initiatives (e.g., public-private partnerships), they have also been seen to drive normative agendas.

The subsequent paragraphs summarize the norms-based activities conducted by some of the most vocal proponents for rules of the road for cyberspace. The selection of relevant initiatives was informed by substantive as well as temporal considerations. Only proposals by benevolent non-state actors, and only proposals launched post-2017 were selected for examination.

The ICT4Peace Foundation

Since its inception in the context of the United Nations World Summit on the Information Society in Geneva and Tunis in 2004, the ICT4Peace Foundation has actively stipulated the peaceful use and employment of ICTs and new media. Against the background of rapidly emerging threats and acts of cybercrime and -sabotage, in 2011, the ICT4Peace Foundation publicly called for a *Code of Conduct for Cyberconflicts* (Stauffacher, Sibilia, and Weekes 2011). The corresponding report titled *Getting Down to Business: Realistic Goals for the Promotion of Peace in Cyberspace* maintained that

> *nations . . . need to examine and assess the need for modifying existing laws to address cyber-specific issues. At both . . . national and international levels, taskforces need to be established including all the key players to exchange information, provide early warning and explore possible solutions to existing or future challenges.* (Stauffacher, Sibilia, and Weekes 2011)

With the intention of building on the outcomes of the UN GGEs, most recently, the ICT4Peace Foundation has, in a joint initiative with Leiden University's Program for Cyber Norms, co-sponsored the publication of a *Global Commentary on Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology*, which brings together comments and guidance for understanding and operationalizing the recommendations contained in the UN GGE reports of 2010, 2013, and 2015 (Tikk et al. 2017; ICT4Peace Foundation 2017; Adamson 2017). Furthermore, ICT4Peace has commissioned a series of cyber-norms blogposts commenting on developments in the field, and has actively participated

in UN GGE and UN OEWG consultation meetings with a view to contributing to the promotion of peaceful settlements of disputes in cyberspace (Tikk 2019; ICT4Peace Foundation 2019).

Microsoft

Among the first corporate stakeholders to instigate debates about responsible conduct in cyberspace was Microsoft (Betz 2015). Following preceding efforts in 2013, 2014, and 2016, in February 2017, Microsoft president and chief legal officer Brad Smith introduced the idea of a *Digital Geneva Convention to Protect Cyberspace* (Smith 2017a; Microsoft 2013; McKay et al. 2014; Charney et al. 2016). Grounded in the belief that deep-rooted collaboration among states, and between states, the private sector and civil society is needed to curb nefarious doings in the digital realm, the convention as outlined by Smith, asks governments to "come together, affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules, and get to work implementing them" (Smith 2017b). Furthermore, it pleads global technology companies to behave as neutral actors, and recommends the setting-up of an independent non-governmental organization capable of investigating and publicly attributing (nation-state) cyberattacks (Smith 2017b; Maurer and Taylor 2018).

Microsoft's call for a *Digital Geneva Convention to Protect Cyberspace* was succeeded by the unveiling of a *Cybersecurity Tech Accord* among leading industry partners in April 2018 (Smith 2018). In September 2018, Microsoft unveiled a Digital Peace Now campaign, which calls on citizens to protect cyberspace, for example, through measures of cyberhygiene, and urges governments to refrain from endangering the global digital environment. Only two months later, in November 2018, it supported the release of the *Paris Call*, a multistakeholder initiative seeking to safeguard peace and security in the virtual realm by means of nine principles, including the prevention of nefarious interference or theft of intellectual property by foreign actors, the condemnation of hack-backs, and the securing of supply chains (Ministère de l'Europe et des Affaires Étrangères 2018). So far, the *Paris Call* has been acceded to by more than 1000 supporters: 78 governments, 29 public authorities, 343 civil society organizations, and 633 private sector entities (Ministère de l'Europe et des Affaires Étrangères 2018).

Siemens

Two months before the launch of Microsoft's *Cybersecurity Tech Accord*, Siemens, together with eight partner corporations, issued a *Charter of Trust*

for a Secure Digital World (Siemens 2018a). Adopted at the sidelines of the 2018 Munich Security Conference, the charter calls for binding rules, and postulates ten principles ranging from ownership of cyber and IT security, responsibility throughout the digital supply chain, security by default, user-centricity, innovation and co-creation to education, certification for critical infrastructure and solutions, transparency and response, regulatory framework, and joint initiatives (Siemens 2018b; Hinck 2018; Kaeser 2018).

Calling for binding legal rules, the charter recognizes that

> *in order to keep pace with continuous advances in the market as well as threats from the criminal world, companies and governments must join forces and take decisive action. This means making every effort to protect the data and assets of individuals and businesses; prevent damage from people, businesses, and infrastructures; and build a reliable basis for trust in a connected and digital world.* (Siemens 2018a, 1)

In contrast to the politically worded norms advanced as part of the Digital Geneva Convention or the Paris Call, the areas of activities identified by the charter signatories are skewed toward key tenets of responsible product development and engineering practices (Horenbeeck et al. 2019).

Global Commission on the Stability of Cyberspace (GCSC)

A year prior to the postulation of Siemens' *Charter of Trust for a Secure Digital World*, the Munich Security Conference (2017) saw the inauguration of the Global Commission on the Stability of Cyberspace (GCSC), a multi-stakeholder consortium composed of regionally diverse scholars, CEOs, and (former) policy makers. The commission's expressed goal is the development of "proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behaviour in cyberspace" (Global Commission on the Stability of Cyberspace 2017b). Composed of twenty-eight commissioners and supported by a research team and a governmental advisory network, the GCSC draws on a rich pool of technical and political expertise. According to one of its commissioners, Dr. Wolfgang Kleinwächter, "the GCSC has the potential, to become a trusted source of inspiration for global internet policy making in the 2020s" (Kleinwächter 2017).

The GCSC has convened several times along major Internet policy meetings, including the Munich Security Conference, CyCon, Black Hat, the Global Conference on Cyber Space, GLOBSEC, ICANN, EuroDIG, UNIDIR, and G20. During one of its early meetings in November 2017, the GCSC issued its first norm, *A Call to Protect the Public Core of the Internet*, which

states: "Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace" (Global Commission on the Stability of Cyberspace 2017a, 1). The proclamation of the norm drew considerable attention from the international community and the norm has since made its way into a number of political fora, including the Paris Peace Forum, and the European Union (Global Commission on the Stability of Cyberspace 2019; Ministère de l'Europe et des Affaires Étrangères 2018). According to some observers, including the Electronic Frontier Foundation's global policy analyst, Jeremy Malcolm, "the idea of a duty on stakeholders not to attack the internet's core technical infrastructure has the potential to become an influential and important guiding principle for policymakers and business leaders" (Malcolm 2017).

The concept of the public core as advanced by the GCSC was first articulated by associate professor of Security and Technology, Dennis Broeders, in a study published by Netherlands Scientific Council for Government Policy (Broeders 2016). The study argued for the establishment of an international norm directed at protecting "the internet's public core—its main protocols and infrastructure, which are a global public good . . . against unwarranted intervention by states" (Broeders 2017, 367).[3]

Since the publication of its first norm, the commission has issued seven further norms addressing issues such as product tampering, the commandeering of botnets, and the creation of a vulnerability equities process (Global Commission on the Stability of Cyberspace 2018b).

NON-STATE ACTORS AS SHAPERS OF CUSTOMARY STANDARDS OF RESPONSIBLE BEHAVIOR IN CYBERSPACE

The cases introduced above demonstrate that non-state actors have come to insert their voices in debates about responsible behavior in cyberspace. They have taken seats at political tables and have started to behave as diplomatic protagonists. Their proposals are deliberately targeted at the international level and consciously employ policy-oriented language. Naming norms-based endeavors *Charter*, *Accord*, *or Convention* underscores the underlying political ambitions of these efforts.

In terms of agency, the norm-building activities conducted by non-state actors reflect a substantial extension of their traditional authority. From a structural point of view, they suggest a shift in global regulation from state-centric forms of steering toward new non-territorial, multi-actor modes of

governance (Scherer, Palazzo, and Baumann 2006, 506). In international relations and international law, states have long enjoyed (and continue to enjoy) conceptual and analytical preeminence apropos enacting and enforcing global rules (Bianchi 2011; Noortmann, Reinisch, and Ryngaert 2015). Among a select number of personae endowed with international legal personality, states have been considered the main bearers and creators of international rights and duties, and as a result have been ascribed key value allocation authority (Klabbers 2003, 55; Thirlway 2014). Positivist interpretations of international law maintain that international norm-making capabilities sit with states who lay down "shared boundaries of acceptable conduct in international [affairs]" (Mačák 2017, 2). However, in the context of cybersecurity, traditional conceptions of how norms and values come about and achieve legal status appear to be at odds with empirical realities.

With the intention of responding to the inadequacies posed by positivist interpretations of international law, a group of legal scholars has promoted the idea of *Global Administrative Law* (Krisch and Kingsbury 2006). Global administrative law offers a useful lens through which to contextualize the norm-stipulating activities of non-state actors and highlight their contributions.[4] Conceptually, it is closely related to notions of global governance.[5] Global administrative law refers to an emerging body of law which takes into account that a great number of global legal rules, principles, and institutional norms are shaped by administrative processes "that implicate more than purely intra-state structures of legal and political authority" (Kingsbury and Donaldson 2011, para. 1). It "acknowledges the informality of global administration, the diffusion of decision making in a multi-level system and the strong influence of private elements in global administration" (Andjelkovic 2006, 58).

According to Kingsbury, Krisch and Stewart, five different types of administrative processes can be distinguished, all of which can give rise to the emergence of global legal rules, principles, and institutional norms:

1. Administration by formal international organizations;
2. Administration based on collective action by transnational networks of cooperative arrangements between national regulatory officials;
3. Distributed administration conducted by national regulators under treaty, network, or other cooperative regimes;
4. Administration by hybrid intergovernmental–private arrangements;
5. Administration by private institutions with regulatory functions (Kingsbury, Krisch, and Stewart 2005, para. 20).

Of particular relevance for the purposes of this chapter are administrative processes conducted by private protagonists. Whether through company policies,

dedicated normative initiatives or technical standard-setting, non-state actors have contributed substantially to global administrative processes pertaining to cybersecurity and have helped shape global practices and culture. The GCSC's institution-crossing policy efforts to enhance international security and stability and guide responsible state and non-state behavior in cyberspace or Siemens' and Microsoft's propagation of technical security standards are but a few examples in this regard (Global Commission on the Stability of Cyberspace 2018c; European Parliament 2018, para. 48). The same can be said about the interpretation and implementation guidelines issued by ICT-4Peace and Leiden University's Program for Cyber Norms apropos the norms contained in the 2015 UN GGE recommendations.

While contested in terms of legal status, these practices have the potential to constitute important determinants for the emergence of international custom pertaining to cybersecurity. According to traditional notions of customary international law, binding habitus requires the presence of two elements: (1) consistent state practice and (2) opinio juris (Wex Legal Dictionary 2018).[6] Although the practices advanced by non-state actors in the context of international peace and security in cyberspace fit only imperfectly into conventional frameworks of customary international law (as they are not state-driven), their law-like normative and custom-inspiring effects should not be discounted. Global administrative law helps acknowledge these custom and culture-shaping contributions of non-state actors as it lends credence to the idea of non-state actors possessing legislative qualities, that is, having international legal personality (Andjelkovic 2006).

Custom never emerges instantaneously or fully formed. Rather, it represents the product of repeated interactions and exchanges across different institutional contexts and among different entities over time (Finnemore and Hollis 2018). As many regulatory functions are increasingly constituted and performed outside formally public, governmental structures, the norm-advancing activities conducted by non-state actors as well as their political/diplomatic engagement, if sustained over time, have the capacity to act as mold shells for the emergence of customary red lines apropos responsible behavior in the digital realm. By lining out and verbally enforcing normative standards vis-à-vis acceptable conduct in cyberspace, non-state actors can curb the potential for malicious, norm-opposing behavior to become widely accepted, including among sovereign parties. Indeed, as sovereign entities continue to grapple with questions around the applicability of international law to the virtual sphere, the norm-stipulating practices of private protagonists can serve as important sources of input and incubators of customary principles ad interim.

The norm-promoting efforts of non-state actors can effectively be understood as signals of disapproval of certain malicious activities in cyberspace,

for example, the targeting or deliberate destruction of critical (information) infrastructure. These signals, in turn, have the potential to incite counteractions among different parties (including states) and give rise to shared boundaries of acceptable conduct in cyberspace. Furthermore, the practices advanced by non-state actors may provide a model which other protagonists in global administration find persuasive to follow and/or cost-effective to emulate (Kingsbury and Donaldson 2011, para. 26).

CONCLUSION

A decade ago, the protection of critical systems and network infrastructures was considered a topic of low politics, one mainly concerning technical experts (Malcolm 2017). Today, cybersecurity has become a matter of high politics. It has become top of the agenda for a wide circle of stakeholders, including government officials, community leaders, and CEOs. The exorbitant increase in the number of users and processes relying on digital infrastructures since the 1990s has gone hand in hand with a surge in the number of vulnerabilities and insecurities. The rising tide of threats to the stability and future development of cyberspace has led many observers to call for rules and norms to secure the digital environment.

Against the background of progress-inhibiting contention at the intergovernmental level, this chapter has analyzed the contributions of non-state actors to projects of international cybersecurity norm-construction. It has argued that non-state actors have come to exert considerable influence, particularly as active stimulators of norms and shapers of customary standards of responsible behavior in the digital realm.

The normative efforts introduced as part of this chapter indicate that traditional conceptions wherein international standard-setting was seen as the exclusive purview of sovereign actors are fading.

> *The international societal body is changing at a rapid rate and new actors in international law are emerging and gaining prominence. Scholars and practitioners have to think fast to keep pace with global change. As a result, the theoretical discourse is sometimes lost in the attempt to provide a satisfactory explanation of legal processes in a changing and unpredictable world.* (Bianchi 2009)

With the intention of better understanding and classifying the norm-stipulating activities of non-state actors in the context of international peace and security in cyberspace, this chapter turned to global administrative law. Global administrative law recognizes that "much administration is taking place in

what might be thought of as a global administrative space, involving blurring of national and international, and public and private, dimensions" (Kingsbury and Donaldson 2011, para. 1). It also appreciates and helps conceptualize the law-like normative and custom-inspiring practices of non-state actors.

Irrespective of their ontological infancy and their loose connection among each other, the norm-promoting activities of non-state actors as well as their political commitment, if sustained over time, have the capacity to act as mold shells for the emergence of international custom pertaining to responsible behavior in cyberspace. Given the reluctance of states to actively present their views on where the thresholds are, non-state actor engagement is critical apropos effectuating responsible behavior in cyberspace (Vihul 2013). Although not endowed with formal law-making authority under positivist notions of international law, the work of non-state actors such as ICT4Peace Foundation, multinational technology firms, including Microsoft and Siemens, or the Global Commission on the Stability of Cyberspace is exceptionally important in terms of lining out and shaping the outer (non-legal) boundaries of acceptable conduct in cyberspace (Vihul 2013).

Furthermore, as non-state actors continue to be concerned about "the immediate and future threats to their critical services and infrastructures, [resulting] from the misuse of information and communications technologies," and seek diplomatic engagement, it is important to reconsider existing forms of interaction and cooperation among governmental and non-governmental entities (Melissa Hathaway in Hampson et al. 2017, 5). The norm-building activities of non-state actors point to a need for more collaborative forms of governance, in which the former participate in joint steering efforts and share responsibilities with sovereign authorities (Healey 2018, 1:1).

NOTES

1. "The main goals for agreeing on norms are believed to include increased predictability, trust and stability in the use of Information and Communication Technologies" (Osula and Rõigas 2016, 11).

2. Contrary to earlier communication technologies, and despite its emergence in a politically predicated context, sovereign actors initially displayed little inclination toward enacting measures of control over cyberspace. Operation and management of the infrastructure were, for the most part, left to the experts who had contributed to its development, including, among others, Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. Oversight was informal and reflected the academic context within which the digital realm had arisen.

3. According to Broeders the public core "does not comprise the whole of the internet or even enter into the content layer of the internet but is limited to the logical

and physical infrastructural layers of the core internet. It is deliberately a 'lowest common denominator approach' that aims to keep the concept of the public core as close as possible to the minimum that is needed to protect the functionality of the internet," see (Broeders 2017, 367).

4. "Underlying the emergence of global administrative law is the vast increase in the reach and forms of transgovernmental regulation and administration designed to address the consequences of globalised interdependence in such fields as security, . . . banking and financial regulation, law enforcement, telecommunications, . . . intellectual property" (Kingsbury, Krisch, and Stewart 2005, 16).

5. With regard to the governance of global networks, Drake considers global governance to be "the development and application of shared principles, norms, rules, decision-making procedures, and programs intended to shape actor's expectations and practices and to enhance their collective management capabilities in world affair," see (Drake 2008, 8–9).

6. "Opinio juris denotes a subjective obligation, a sense on behalf of a state that it is bound to the law in question. The International Court of Justice reflects this standard in ICJ Statute, Article 38(1)(b) by reflecting that the custom to be applied must be *accepted as law*" (Wex Legal Dictionary 2018).

BIBLIOGRAPHY

Adamson, Liisi. 2017. "Recommendation 13 (C)." In *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use Of Information and Communications Technology: A Commentary*, edited by Eneken Tikk. New York, NY: United Nations Office for Disarmament Affairs. https://www.un.org/disarmament/wp-content/uploads/2018/04/Civil-Society-2017.pdf.

Andjelkovic, Maja. 2006. "Internet Governance: In the Footsteps of Global Administrative Law." University of Kent. https://www.iisd.org/pdf/2006/infosoc_int_gov_law.pdf.

Betz, Chris. 2015. "A Call for Better Coordinated Vulnerability Disclosure." Microsoft. 2015. https://blogs.technet.microsoft.com/msrc/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure/.

Bianchi, Andrea. 2009. "Non-State Actors and International Law." 2009. http://graduateinstitute.ch/home/relations-publiques/news-at-the-institute/news-archives.html/_/news/corporate/2009/news_557.

———. 2011. "The Fight for Inclusion: Non-State Actors and International Law." In *From Bilateralism to Community Interest*, edited by Ulrich Fastenrath, Rudolf Geiger, Daniel-Erasmus Kahn, Andreas Paulus, Sabine von Schorlemer, and Christoph Vedder, 39–57. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199588817.003.0006.

Broeders, Dennis. 2016. *The Public Core of the Internet: An International Agenda for Internet Governance*. Edited by The Netherlands Scientific Council for Government Policy. *The Public Core of the Internet: An International Agenda for Internet Governance*. Amsterdam University Press. https://doi.org/10.26530/OAPEN_610631.

———. 2017. "Aligning the International Protection of "the Public Core of the Internet" with State Sovereignty and National Security." *Journal of Cyber Policy* 2 (3): 366–376. https://doi.org/10.1080/23738871.2017.1403640.

Charney, Scott, Erin English, Aaron Kleiner, Nemanja Malisevic, Angela McKay, Jan Neutze, and Paul Nicholas. 2016. "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms." https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

Drake, William J. 2008. "Introduction: The Distributed Architecture of Network Global Governance." In *Governing Global Electronic Networks*, edited by William J. Drake and Ernest J. Wilson III, 1–80. The MIT Press. https://doi.org/10.7551/mitpress/9780262042512.003.0009.

European Parliament. 2018. "Report on Cyber Defence (2018/2004(INI))." http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2018-0189+0+DOC+PDF+V0//EN.

Finnemore, Martha, and Duncan B. Hollis. 2018. "Naming without Shaming? Accuzations and International Law in Global Cybersecurity."

Finnemore, Martha, and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52 (4): 887–917. https://doi.org/10.1162/002081898550789.

Florini, Ann. 1996. "The Evolution of International Norms." *International Studies Quarterly*, 40: 363–389. http://www.jstor.org/stable/2600716.

Global Commission on the Stability of Cyberspace. 2017a. "Call to Protect the Public Core of the Internet." https://cyberstability.org/wp-content/uploads/2017/11/call-to-protect-the-public-core-of-the-internet.pdf.

———. 2017b. "Mission Statement." https://cyberstability.org/.

———. 2018a. "Call to Protect the Electoral Infrastructure." https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf.

———. 2018b. "Global Commission Introduces Six Critical Norms Towards Cyber Stability." News. https://cyberstability.org/research/singapore_norm_package/.

———. 2018c. "The European Parliament Supports the GCSC in Its Recent Report on Cyber Defence." News. https://cyberstability.org/news/the-european-parliament-supports-the-gcsc-in-its-recent-report-on-cyber-defence/.

———. 2019. "European Union Embeds Protection of the Public Core of the Internet in New EU Cybersecurity Act." News. https://cyberstability.org/news/european-union-embeds-protection-of-the-public-core-of-the-internet-in-new-eu-cybersecurity-act-2/.

Hall, Rodney Bruce, and Thomas J Biersteker. 2002. *The Emergence of Private Authority in the International System*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511491238.

Hathaway, Melissa. 2017. "When Violating the Agreement Becomes Customary Practice." In *Getting beyond Norms: New Approaches to International Cybersecurity Challenges*, edited by Fen Osler Hampson and Michael Sulmeyer, 5–12. Centre for International Governance Innovation. https://www.cigionline.org/sites/default/files/documents/Getting Beyond Norms.pdf.

Healey, Jason. 2018. "Innovation on Cyber Collaboration: Leverage at Scale." Vol. 1. http://www.atlanticcouncil.org/images/publications/Innovation-Cyber-WEB.pdf.

Hern, Alex. 2017. "WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017." *The Guardian*. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

Hinck, Garrett. 2018. "Private-Sector Initiatives for Cyber Norms: A Summary." Lawfare. https://www.lawfareblog.com/private-sector-initiatives-cyber-norms-summary.

Horenbeeck, Maarten Van. 2018. "Taking a Multi-Stakeholder Look at Cyber Norms." CircleID. http://www.circleid.com/posts/20180827_taking_a_multi_stakeholder_look_at_cyber_norms/.

Horenbeeck, Maarten Van, Sheetal Kumar, Global Partners Digital, Frans Van Aardt, Susan Mohr, Carina Birarda, Louise Marie Hurel, John Hering, Duncan Hollis, and Joanna Kulesza. 2019. "Cybersecurity Agreements." http://www.intgovforum.org/multilingual/filedepot_download/4904/1658.

ICT4Peace Foundation. 2017. "Call for Global Open Consultations on the United Nations Cybersecurity Norms Proposals." Activities. https://ict4peace.org/activities/call-for-global-open-consultations-on-the-united-nations-cybersecurity-norms-proposal/.

———. 2018. "ICT4Peace Sponsored First Global Commentary on Norms of Responsible State Behaviour in Cyberspace." https://ict4peace.org/activities/ict4peace-sponsored-first-global-commentary-on-norms-of-responsible-state-behaviour-in-cyberspace/.

———. 2019. "UN GGE and UN OEWG on Cybersecurity: ICT4Peace Supporting OAS Regional Consultations." Activities. https://ict4peace.org/activities/un-gge-and-un-oewg-on-cybersecurity-ict4peace-supporting-oas-regional-consultations/.

Kaeser, Joe. 2018. "Working Together for More Security in the Digital World." LinkedIn Pulse. https://www.linkedin.com/pulse/working-together-more-security-digital-world-joe-kaeser.

Keck, Margaret E., and Kathryn Sikkink. 1999. "Transnational Advocacy Networks in International and Regional Politics." *International Social Science Journal* 51 (159): 89–101. https://doi.org/10.1111/1468-2451.00179.

Kingsbury, Benedict, and Megan Donaldson. 2011. "Global Administrative Law." Max Planck Encyclopedia of Public International Law. http://iilj.org/wp-content/uploads/2016/08/EPIL_Global_Administrative_Law.pdf.

Kingsbury, Benedict, Nico Krisch, and Richard Stewart. 2005. "The Emergence of Global Administrative Law." *Law and Contemporary Problems* 68 (3): 48. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/lcp68&section=35.

Klabbers, Jan. 2003. "(I Can't Get No) Recognition: Subjects Doctrine and the Emergence of Non-State Actors." In *Nordic Cosmopolitanism*, edited by Martti Koskenniemi, Jarna Petman, and Jan Klabbers, 1813: 352–369. Leiden: Martinus Nijhoff Publishers.

Kleinwächter, Wolfgang. 2017. "The Kaljurand Commission: Building Bridges Over Troubled Cyber-Water." http://www.circleid.com/posts/20171202_kaljarund_commission_building_bridges_over_troubled_cyber_water/.

Krisch, Nico, and Benedict Kingsbury. 2006. "Introduction: Global Governance and Global Administrative Law in the International Legal Order." *European Journal of International Law* 17 (1): 1–13. https://doi.org/10.1093/ejil/chi170.

Mačák, Kubo. 2017. "From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers." *Leiden Journal of International Law* 30 (4): 877–899.

Malcolm, Jeremy. 2017. "EFF at Cyberspace Events in Delhi: Protecting the Public Core of the Internet." Deeplinks Blog. https://www.eff.org/deeplinks/2017/11/eff-cyberspace-events-delhi-protecting-public-core-internet.

Maurer, Tim, and Kathryn Taylor. 2018. "Outlook on International Cyber Norms: Three Avenues for Future Progress." Just Security. https://www.justsecurity.org/53329/outlook-international-cyber-norms-avenues-future-progress/.

McKay, Angela, Jan Neutze, Paul Nicholas, and Kevin Sullivan. 2014. "International Cybersecurity Norms." https://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/.

Microsoft. 2013. "Five Principles for Shaping Cybersecurity Norms." https://www.microsoft.com/en-us/cybersecurity/content-hub/five-principles-for-shaping-cybersecurity-norms.

Ministère de l'Europe et des Affaires Étrangères. 2018. "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace." French Foreign Policy. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

Noortmann, Math, August Reinisch, and Cedric Ryngaert. 2015. *Non-State Actors in International Law*. Edited by Math Noortmann, August Reinisch, and Cedric Ryngaert. Studies in International Law. Oxford: Hart Publishing.

Nye, Joseph S. Jr. 2018. "*Normative Restraints on Cyber Conflict*." Cambridge, MA. https://www.belfercenter.org/sites/default/files/files/publication/Nye Normative Restraints Final.pdf.

Osula, Anna-Maria, and Henry Rõigas. 2016. *International Cyber Norms*. Edited by Anna-Maria Osula and Henry Rõigas. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf.

Radu, Roxana. 2014. "Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace." In *Cyberspace and International Relations*, edited by Jan-Frederik Kremer and Benedikt Müller, 3–20. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-37481-4.

Ruggie, John Gerard. 2011. "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework." Vol. HR/PUB/11/. New York, NY. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

Ruggie, John Gerard. 1993. "Territoriality and Beyond: Problematizing Modernity in International Relations." *International Organization* 47 (1): 139–174. http://www.jstor.org/stable/2706885.

———. 2004. "Reconstituting the Global Public Domain—Issues, Actors, and Practices." *European Journal of International Relations* 10 (4): 499–531. https://doi.org/10.1177/1354066104047847.

Sandholtz, Wayne. 2017. *International Norm Change*. *Oxford Research Encyclopedia of Politics*. Oxford: Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.588.

Scherer, Andreas Georg, Guido Palazzo, and Dorothée Baumann. 2006. "Global Rules and Private Actors: Toward a New Role of the Transnational Corporation in Global Governance." *Business Ethics Quarterly* 16 (04): 505–532. https://doi.org/10.5840/beq200616446.

Siemens. 2018a. "Charter of Trust: For a Secure Digital World." https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf.

———. 2018b. "Time for Action: Building a Consensus for Cybersecurity." Cybersecurity. https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html.

Sjöström, Emma. 2010. "Shareholders as Norm Entrepreneurs for Corporate Social Responsibility." *Journal of Business Ethics* 94 (2): 177–191. https://doi.org/10.1007/s10551-009-0255-1.

Smith, Brad. 2017a. "A Digital Geneva Convention to Protect Cyberspace." https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.

———. 2017b. "The Need For a Digital Convention." Microsoft. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv.

———. 2018. "34 Companies Stand Up for Cybersecurity with a Tech Accord." Microsoft. https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/.

Stauffacher, Daniel, Ricardo Sibilia, and Barbara Weekes. 2011. "Getting Down to Business Realistic Goals for the Promotion of Peace in Cyberspace." Geneva.

Thirlway, Hugh. 2014. *The Sources of International Law*. Foundations of Public International Law. Oxford: Oxford University Press.

Tikk, Eneken. 2019. "UN GGE—Eneken Tikk's Cyber Norms Blogposts: Search for Cyber Norms—Where to Look? #4 The Norms Test: Existing Norms." ICT4Peace Foundation. https://ict4peace.org/activities/policy-research/policy-research-cs/un-gge-eneken-tikks-cyber-norms-blogposts-search-for-cyber-norms-where-to-look-4-the-norms-test-existing-norms/.

Tikk, Eneken, Zine Homburger, Mika Kerttunen, Liisi Adamson, Els DeBusser, Barrie Sander, Jason Jolley, Michael Berk, Caitriona Heinl, and Nicholas Tsagourias. 2017. *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use Of Information and Communications Technology: A Commentary*. Edited by Eneken Tikk. New York, NY: United Nations Office for Disarmament Affairs. https://www.un.org/disarmament/wp-content/uploads/2018/04/Civil-Society-2017.pdf.

Väljataga, Ann. 2017. "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly." NATO CCDCOE. https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html.

Vihul, Liis. 2013. "The Tallinn Manual on the International Law Applicable to Cyber Warfare." Blog of the European Journal of International Law. https://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/.

Wagner, Markus. 2009. "*Non-State Actors*." Edited by Rüdiger Wolfrum. Max Planck Encyclopedia of Public International Law. Oxford. https://ssrn.com/abstract=2661832.

Wex Legal Dictionary. 2018. "Opinio Juris." Legal Information Institute. https://www.law.cornell.edu/wex/opinio_juris_%28international_law%29.

Winston, Carla. 2017. "Norm Structure, Diffusion, and Evolution: A Conceptual Approach." *European Journal of International Relations*, 135406611772079. https://doi.org/10.1177/1354066117720794.

Wu, Timothy S. 1998. "Cyberspace Sovereignty? The Internet and the International System." *Harvard Journal of Law & Technology* 10 (3): 647–666. https://doi.org/10.3868/s050-004-015-0003-8.

Governing Cyberspace

OPEN ACCESS

The publication of this book is made possible by a grant from the Open Access Fund of the Universiteit Leiden.