Governing Cyberspace: Behaviour, Power and Diplomacy

Dennis Broeders & Bibi van den Berg

Chapter 1

Governing Cyberspace

Behavior, Power, and Diplomacy

Dennis Broeders and Bibi van den Berg

WELCOME TO CYBERSPACE

When states look at cyberspace, they do not necessarily see the same as most end users do. Sure, they see the massive added value in terms of the digital economy and, like their citizens, they have difficulties imagining life without the constant interactions and communication that is the bedrock of modern digital society. However, many parts of the government see cyberspace increasingly as a source of threat, insecurity, and instability. Where states looked at the early stages of the development of cyberspace with a certain degree of "benign neglect," it became much more of a government interest when the digital economy started off in earnest. Now, states increasingly view cyberspace through a lens of security. Not just in terms of cybercrime but more and more in terms of the high politics of international security (Klimburg 2017; Segal 2016; DeNardis 2014; Deibert 2013; Betz and Stevens 2011). Many states have formally declared the cyber domain to be the fifth domain of warfare—after land, sea, air, and space—and increasingly states conduct intelligence and pseudo-military operations in the cyber domain that fall short of "cyber war" but do create a permanent state of "unpeace" (Kello 2017; see also Boeke and Broeders 2018). The increase in cyber-attacks among states, or at least those that come out into the open, seem to be intensifying in terms of damage and impact, and provoke reactions from states and corporations. Cyber operations like WannaCry and NotPetya, politically attributed to North Korea and Russia, respectively, were both damaging and indiscriminate, which added to the feeling of vulnerability in the digital domain. However, even with NotPetya, of which the global damages have been estimated at roughly $10 billion (Greenberg 2018), no state was willing to say this operation was in violation of international law. More in general, all public attributions of cyberattacks to states have not invoked international law other than in the most general terms possible (Efrony and Shany 2018).

In cyberspace, a state of unpeace is heating up and although most states agree in principle that international law applies in cyberspace as it does in the analogue world, they do not seem to be able to agree on specifics. Furthermore, "the" regulation of "the" Internet does not exist. Nye (2014) has shown that the Internet is regulated through an elaborate cyber regime complex that has pockets of dense regulation in some subject areas as well as patches that are largely unregulated. Moreover, there are many aspects on which states are still struggling to find an effective governance structure to address the issues at hand (see also Klimburg and Faesen 2020 in this volume). Moreover, some elements of governance are firmly in the hands of private parties (companies, the technical community), whereas others—for example, military, intelligence, and diplomatic—are firmly in the hands of states. The mix between public and private actors in Internet governance is called "multistakeholder governance," a concept that is embraced by Western liberal states (at least in theory) but is disputed by states that favor a much stronger role for sovereign states in the regulation and governance of cyberspace. States like Russia and China would like to bring "Internet governance" into a multilateral setting where sovereign states, rather than a wide array of stakeholders, steer the direction of cyberspace. This archetypical divide between multistakeholderism and multilateralism when talking about cybersecurity and Internet governance structures is connecting with rising geopolitical tensions between the major global powers. The global strife between the United States and China and Russia—with the European Union somewhere in the middle of the mix—works as a force multiplier for tensions in both interstate behavior—cyber operations among states—and positions in diplomatic negotiations on "responsible state behavior" in cyberspace (Broeders, Adamson, and Creemers 2019). In this volume, Klimburg and Faesen (2020) search for ways to square the circle the between classic balance of power politics and the complicated governance structures that are needed to regulate cyberspace.

OF LAWS AND NORMS

The possible negative effects of the use of ICTs for international peace and security were flagged by Russia in 1998 when it submitted a resolution on "Developments in the field of Information and Telecommunications in the context of International Security" to the UN's First Committee, which deals with disarmament and international security (UNGA 1999). While recognizing that the Internet brought many good things, Moscow feared an arms race in this new domain and aimed for the negotiation of a treaty that would ban the use of information weapons in order to prevent information wars. To some extent, Russia feared in 1998 what many now consider Moscow to be the best at: information operations and the spread of disinformation. Russia was aiming for a new treaty specifically for cyberspace but ran into Western resistance to the notion that cyberspace needed *lex specialis*. Western states, in this field often loosely assembled under the heading of the "like-minded" states, depart from the notion that international law, including International Humanitarian Law, applies in the digital domain as it does in the "real world." The UN Group of Governmental Experts (UN GGE) process was started in 2004 to create a venue at the UN level for deliberation of the issue without going down the road of a treaty. Out of five iterations of the process the group of experts produced a consensus report three times, with as main yields the principle that international law applies in cyberspace in 2013 and the formulation of a number of nonbinding norms for responsible state behavior in the 2015 consensus report (UN General Assembly 2010, 2013, 2015). After the 2017 round of the UN GGE failed to achieve consensus, there were many reports of the "death of the norms process" (see, e.g., Grigsby 2017), but in November 2018, the UN General Assembly voted on two parallel and competing resolutions. The first was submitted by the United States and supported by the "like-minded" states calling for a new round of the GGE. The second was submitted by Russia and called for an Open-Ended Working Group (OEWG) to discuss roughly the same issues. Both were voted through by the General Assembly in substantial and significantly overlapping numbers, and the twin processes have started in 2019.

In a parallel trajectory to the diplomatic processes at the UN and regional organizations, international legal scholars embarked on a project to flesh out how exactly international law applies in cyberspace. This project under the sponsorship of the NATO CCDCOE—which does not make it a NATO project—resulted in the Tallinn Manual (2013) and the Tallinn Manual 2.0 in 2017 (Schmitt et al. 2013, 2017). Both are academic, nonbinding studies on how international law applies to cyber conflicts and cyber warfare and on many issues contain majority and minority opinions. The first manual focuses on the *jus ad bellum* and International Humanitarian Law and the second focuses on cyber operations that are "below the threshold" of armed conflict, or "peacetime operations." The Tallinn manuals are the most comprehensive analyses of International Humanitarian Law and cyberspace available and serve as an important reference point. However, and as indicated before, states are reluctant to refer to (specific principles of) international law when they publicly address cyber operations and conflict, leading Efrony and

Shany (2018) to refer to the manual as “a rulebook on the shelf.” Many legal scholars in this fieldwork on different aspects of international law and how these relate to state operations in the cyber domain. In this volume, Roguski (2020) analyses the principle of territorial sovereignty in cyberspace through a lens of an “intrusion-based approach” and Tsagourias (2020) looks at cyber interference with election processes in light of the legal principle of non-intervention. Principle-by-principle and case-by-case legal scholars are adding to the growing literature on the application of international law to state behavior in cyberspace.

The limited diplomatic progress on the application of international law to cyberspace also led to what is called the cyber-norms process, both in diplomatic practice as in academia. The 2015 UN GGE consensus report included a section on “general non-binding, voluntary norms, rules and principles for responsible behaviour of states.” This section contained eleven “new” recommendations for norms and gave an impetus to the international debate about cyber norms. These norms are often juxtaposed with international law. The states that participate in the GGE process went the route of norms, in part because achieving agreement on the question of *how* exactly international law applies to cyberspace proved a size too big for the negotiations. However, it is also misleading to set norms and international law totally apart from each other in this domain. In this volume, Adamson (2020) highlights the fact that many of the norms in the 2015 UN GGE report actually reflect existing international law. Norms and international law can and do mutually reinforce each other and should not be seen as two completely different and parallel discourses.

International law and international norms—as well as Confidence Building Measures (CBMs), which are also part of the GGE process—all serve the same basic function in the context of cyberspace. They are all meant to make state behavior more predictable—especially in times of conflict—when operating in a context that is unpredictable and where actions are easy to obfuscate and misinterpret. Norms and international law serve to set benchmarks against which we can measure and evaluate state behavior and call actors out on bad behavior. International law would be the gold standard for this but is problematic for two reasons. Firstly, because it has proven hard to get substantial agreement on the question of how specific principles of international law apply in cyberspace. Secondly, because many of the cyber operations that have states worried are below-the-threshold operations and, moreover, they are usually executed by intelligence agencies and proxy actors, which are not meaningfully regulated by international law in the first place (Boeke and Broeders 2018; Maurer 2018). In order to make some progress, academics and states have gone down the route of norms.

THE CYBER-NORMS DISCOURSE

Norms have been a part of the academic debate for far longer than the rise to fame of the cyber-prefix. In international relations theory, Peter Katzenstein's definition of a norm is often the point of departure. According to him, a norm in international politics is "a collective expectation for the proper behaviour of actors with a given identity" (Katzenstein 1996, 5). This implies that there is some sort of community that has—or develops—an idea of what appropriate behavior is. And even though there is no enforcement mechanism in place, the community expects its members to behave a certain, appropriate, way. In the cyber-norms discourse that community is often equated with states, especially in the diplomatic, state-led norms debate, even though many other public and private actors populate the cyber domain and even dominate important aspects of Internet governance. Finnemore and Sikkink (1998) argue that norms are often championed by a norms entrepreneur and when successful the norm they champion goes through a norms cycle. This cycle starts with "norms emergence," in which the role of the norms entrepreneur(s) to propagate the norm is vital. If their advocacy for the norm is successful, the community to which the norm should apply may reach a tipping point which leads to the second stage, labeled the "norms cascade." During this phase, the pioneering work of the norms entrepreneur gets taken over by many other actors within the community who see the norms as central to their identity and propagate its spread. In the last stage, actors "internalize" the norm into their everyday behavior and the norms effectively come to serve as a benchmark for appropriate behavior. Finnemore and Hollis (2016) have taken this classic approach to norms creation into the cyber domain and highlighted the dynamic and interdependent character of cyber norms. They also found that much of the debate about norms in this domain was (too) centered on norms as an end goal and not enough on the value of the process itself. Kurowska (2019) takes that argument further and emphasizes that the classic model of the norms cycle—perhaps especially in the cyber-norms debate—often has a teleological character and does not take norms contestation into account as an important part of the model. This blind spot has consequences not only for the empirical analysis of the norms process but also for the legitimacy of the norms process as a political and a policy process: "a norm that cannot be contested, cannot be legitimate" (Kurowska 2019, 8).

Cyber norms as they stand today are highly contested among governments, despite the efforts of diplomats over the last decades. Moreover, the community to which the norms apply—and who feel part of it as norm entrepreneurs—is by no means convincingly demarcated. States consider themselves to be the core community, but civil society and corporations are increasingly vocal about their place and role in this normative and regulatory domain and engage with the norms debate on their own accord. In this volume, Eggenschwiler and Kulesza (2020) analyze the role of a number of civil society and corporate initiatives that engage with, and shape the norms debate. Gorwa and Peez (2020) and Hurel and Lobato (2020), both also in this volume, analyze the role, goals, and strategies of Microsoft that has put itself forward as a major actor in the international cyber-norms debate.

However, the diplomatic track does not easily open up to "outside" actors even when it has failed to make much substantial progress on the issue. The 2015 UN GGE norms may be agreed upon but are in the words of Maurer (2019) "considered voluntary, defined vaguely, and internalized weakly." After the attacks on the Ukrainian grid in December 2015, many wondered why this was not called out as a violation of the norm that states do not attack critical infrastructures in peacetime as formulated in the 2015 UN GGE consensus report.[1] Now that the stalemate that came into being after the 2017 round of the UN GGE failed to produce consensus has been replaced with the political surprise of the creation of two UN processes in 2018, states bear a great responsibility for moving the process forward. If they do not, the UN is unlikely to remain the focal point for discussion. And while the United States is heavily invested in the GGE as a format and Russia is heavily invested in the OEWG, and more generally in the idea of a multilateral approach, the differences of opinion remain substantial.

Meanwhile, cyber norms are also emerging through state practice rather than diplomatic agreement. States engage in certain behavior in cyberspace: they conduct cyber operations, develop (military) cyber doctrine, change cybersecurity policies and thus create new facts on the digital ground. States also draw red lines that are either respected or violated. When violated, some are met with consequences and some are not. All of this is norm-setting behavior. Actual state behavior shapes normative behavior but is "implicit, poorly understood, and cloaked in secrecy" (Maurer 2019). A good example of that is the norm-setting behavior of intelligence agencies that is analyzed by Georgieva (2020b) in this volume (see also Georgieva 2020a). Power relations and actual state behavior go a long way in explaining how state relations in cyberspace develop.

POWER AND NORMS

One complicating factor of state relations is the Orwellian notion that all states are equal, but some are more equal than others. Even the UN, an organization founded on the principle of the equality of sovereign states, acknowledges this through the mechanism of the five permanent members of the Security Council that hold a veto. As "cyber" rose to the top of the international and national security agenda, geopolitics and strategic considerations became more prominent in the debate about responsible state behavior in cyberspace. States may agree that cyberspace is a source of threats to national security, but simultaneously it is also a possible strategic military advantage, especially to the top-tier cyber powers. Powerful states are usually reluctant to give up capabilities, especially when it is uncertain that others will do the same (Broeders 2017). Countries like the United States, China, Russia, the United Kingdom and Israel, but also Iran and North Korea, have invested heavily in military and foreign intelligence capacity to operate in cyberspace. Other countries have followed suit in different degrees creating a landscape in which operational cyber capacity and cyber power are unequally divided among states.

Moreover, in recent years, the global balance of power has been shifting. American global dominance is challenged by the rising star of China. While China's cyber power is still mostly focused on (economic) espionage and control on the domestic information sphere, rather than all-out military cyber power, China is also asserting itself as a tech developer and vendor at the global level as one of the underpinnings of its status as an economic superpower (Inkster 2016). Russia is trying to reassert itself in terms of being a key player in international cyber peace and security. In cyberspace it does so by—allegedly—being one of the most active cyber powers operating below the threshold of armed conflict in the networks of a great number of countries, as well as by being one of the leading countries in the diplomatic processes on responsible state behavior in cyberspace (see Kurowska 2020 in this volume). China and Russia are also formally and informally aligned on a number of foreign policy objectives, including in the cyber domain. They present a seemingly united front to the world, largely aimed at countering US hegemony, but underneath the façade of unity there are also structural differences that may put cracks into Sino-Russian cooperation in the longer run (Broeders, Adamson, and Creemers 2019).

As a general principle, all states want other states to be bound by a framework of rules while retaining as much room to maneuver for themselves. Great powers like strategic ambiguity in military affairs (Taddeo 2017) and exceptionalism in political affairs. To global powers, like the United States, China, and Russia, the latter is almost an informal doctrine: they all apply a sense of exceptionalism to themselves. China and Russia have clear, explicit, and extensive rules and regulations with regard to cyberspace for their own territories, and (global) companies wishing to do business there must comply or else face the consequences. In this volume, Hoffman (2020) analyses the ways in which China has dealt with US pushback on freedom of expression surrounding Google's entry into the Chinese market.

Russia and China both rally around the idea of "cyber sovereignty" as one of the main organizing principles for interstate relations in cyberspace (see Creemers 2020 and Kurowksa 2020 in this volume). To these countries, cyber sovereignty means control over the domestic information sphere internally, and strict adherence to the principle of non-intervention and self-determination externally. Both China and Russia see information operations in their nation's information sphere as the greatest ICT-related threat. Ironically, what Moscow fears most is what it is generally considered to be best at: information operations and the spread of mis- and disinformation. More in general, "sovereignty" is a bone of contention between Western states and authoritarian states. In this volume, Creemers (2020) highlights that tension in the Chinese case: "China's definition of sovereignty primarily concerns the integrity of its political structure, while Western states consider this a defence of exactly those abuses that the more conditional, post-Cold War reading of sovereignty sought to curtail" (Creemers 2020, 112). Moreover, for countries like China and Russia, sovereignty is not the same for all states: the sovereignty of great states is of a different order than those of smaller states. Great power status is paired with exceptionalism. In the eyes of both Russia and China, the *Pax Americana* was built on American exceptionalism—"do as I say, don't do as I do." Their (rise to) great power status will likewise be built on the idea of exceptionalism, which in turn will influence their views and role in disrupting, reforming, and building the future world order (Broeders, Adamson, and Creemers 2019). The cyber order will be shaped by great power politics, which is currently and for the foreseeable future in flux.

It is also interesting to see how less powerful states seek to navigate the power divides in cyberspace, aligning themselves with one power block on some issues, while choosing to align themselves with a competing power block on others. In this volume, Shires (2020) looks at states in the Middle East—a complex region with multiple allegiances on different issues—and shows how "their regulations, laws, and participation in international institutions places them with Russia, China, and other proponents of cyber sovereignty; on the other, their private sector cybersecurity collaborations, intelligence relationships, and offensive cyber operations are closely aligned with the USA and Europe" (Shires 2020, 205–206). For many countries then determining their position on security, international law, and norms is often an undertaking characterized by a degree of ambiguity.

In the practice of everyday cyber diplomacy, the inequality between sovereign states often means that smaller states favor and support the development of a rules-based order, engaging, for example, in cyber-norms entrepreneurship (Adamson and Homburger 2019), while larger states engage with these processes but allow themselves at least a certain degree of strategic ambiguity. Russia and the United States may be the primary instigators of the UN processes that seek to define how international law applies in cyberspace and which cyber norms could help shape state behavior, they are also the states that shift the posts on these issues through their actual behavior and advances in national (military) doctrine and operations. In terms of espionage (NSA mass surveillance, Chinese economic espionage, Russian digital sabotage), the “militarization” of cyberspace (building up military cyber commands) and the return of information operations (Russian influence operations, most notably interference with the 2016 US presidential election) it has been state practice, not laws and rules, that set the tone. Development in military cyber doctrine in some of the top-tier countries also points in the direction of a more aggressive posture in cyberspace. For example, the US Department of Defence (DoD) cyber strategy states that US cyber forces are in “persistent engagement” with their adversaries and, therefore, need to “defend forward” and “continuously contest” those adversaries, creating more possibilities for escalation of cyber conflict, even though the intention may be the opposite (Healey 2019). States interpreting the actions and intentions of other states erroneously is a classic source of instability as it can lead to the unintended escalation of conflict, a dynamic captured by the idea of the classic security dilemma (Jervis 1978). As Buchanan (2016) has shown, cyberspace provides an excellent context for what he calls a cybersecurity dilemma, highlighting how misinterpretation and escalation of conflict in cyberspace may emerge easily. Therefore, stability in cyberspace may be best served by consciously preparing for the moment that states wrongly interpret the actions of their adversaries. In addition to international law and cyber norms, the world also needs Confidence Building Measures (CBMs) as the third part of the triptych to avoid (unwanted) escalation of conflict in cyberspace (Kavanagh and Crespo 2019). Even though they are widely considered to be vital, CBMs mainly play a useful role when the escalation of (cyber) conflict is *un*-intentional (Pawlak 2016, 135). When states intentionally seek to escalate a conflict, CBMs are useless: in that case the red phone may ring, but will not be picked up. In spite of the realities of power politics, a rules-based order—international law foremost and to certain degree norms—is still the most promising route to stability in cyberspace. International law does not always prevent hostilities; however, states but it does provide a benchmark by which to judge and call out state behavior that is in breach of laws and norms.

NEGOTIATING CHANGE

Finding a framework that applies to the problems at hand in cyberspace is not easy, however. Even though cyberspace does not change the world beyond recognition, it does present severe challenges for international governance.

The regional level has gained in importance when it comes to issues of international peace and security in relation to cyberspace. The ASEAN Regional Forum (ASF) has been an active player in the international debate about cyber stability and norms (Heinl 2018) and announced in November 2019 the start of an ASEAN working group on the implementation of the UN cyber norms. Likewise, the work done in the Organisation for Security and Co-operation in Europe (OSCE)—especially in the field of CBMs—and the Organisation of American States (OAS) has been valuable in and of itself, but also as a means to continue the conversation about international cyber stability when the UN GGE process ground to a temporary halt in 2017 (Ott and Osula 2019). As a military alliance that spans the Atlantic, NATO's role in the cyber domain is more complicated. There is no clear mandate for the organization itself on the operational level, even though the alliance does recognize the importance of cyberspace as an operational domain of warfare. Operational cyber power rests with the member states and the differences within the alliance in terms of operational capacity are vast. NATO houses both top-tier cyber powers like the United States and the United Kingdom as well as states that have hardly developed any military or foreign intelligence capacity to operate in cyberspace. At the Wales summit in 2014, NATO declared cyber defense a core part of collective defense, meaning that a cyberattack could trigger Article 5, the collective defense clause, of the treaty. In this volume, Hill and Marsan (2020) sketch how NATO as a multilateral organization is charting a course to help its member states build their cyber defense capabilities, both individually and collectively, and also seeks to contribute to building a legal and normative framework in which cyber capabilities can be deployed and contested.

Cyberspace may have been named the fifth domain of warfare by states but the actual day-to-day operation of that domain is only to a very limited amount a state affair. Cyberspace's rise to global dominance was to a very large extent a private affair driven by businesses and the technical community laying the groundwork of the logical and technical infrastructure. Most states regarded its development with a benign neglect until cyberspace also became a foundational value for the national economy and society (Mueller 2010; DeNardis 2014; Broeders 2015). With the growth of cyberspace, the stakes of states have risen, but so did the stakes of the private sector and the technical community. Both "communities"—whose interests sometimes overlap and align but who also frequently find themselves at opposite ends of Internet governance debates—have massive interests in how cyberspace develops both in a technical sense as well as in a socioeconomic and political sense. Whether cyberspace is seen as a domain of warfare, whether notions of sovereignty are overlaid on a global system of information exchange, whether privacy regulations have extraterritorial effects, and whether governments are going to expect, request, and/or direct Internet companies and ISPs to enforce national policies matters a great deal to globally operating tech companies. Both in terms of their business models and opportunities and in terms of their (corporate) identities. Some companies have been seeking ways to insert themselves into the political debates about global Internet governance, especially into the field of international security which is traditionally closed to all actors other than states.

In this volume, Eggenschwiler and Kulesza (2020) analyze a number of corporate and multistakeholder initiatives that aim to influence the global debate about responsible behavior of states in cyberspace. Private initiatives coming from, for example, Microsoft and Siemens and global fora such as the Global Commission on the Stability of Cyberspace, which recently published its final report (GCSC 2019), aim to influence state and corporate behavior in cyberspace. Two chapters in this volume, Hurel and Lobato (2020) and Gorwa and Peez (2020), dive deeper into Microsoft's role as a norms entrepreneur. Microsoft has been at the forefront of corporate involved in the cyber-norms process which has for now culminated in its (informal) co-authorship of the French government initiative of the *Paris Call for Trust and Security in Cyberspace* which was launched in November 2018 and its sponsorship of the recently founded Cyber Peace Institute.[2] Hurel and Lobato (2020) analyze Microsoft's internal structures and complexities to gain insight in the how and why of Microsoft's engagement with the international norms processes. They also raise an interesting question with regard to where a global corporation's allegiance lies (in addition to its shareholders). How does Microsoft balance the interest of its global user base with the interest of the United States, its home country? When push comes to shove—and it might very well in these times of geopolitical strife—what will carry more weight: its global user base or the interest of its home government? Gorwa and Peez (2020) make an in-depth analysis of the Microsoft-led initiative of the Cyber Security Tech Accord (CTA). The CTA is focused on corporate self-regulation—partly in response to government pushback to Microsoft's earlier high-profile "Digital Geneva Convention" initiative—and has been backed by over 120 companies. They argue that Microsoft's CTA initiative served to brush up their reputation on data protection after the damage done by the Snowden revelations about their involvement with the NSA surveillance. The success of the accord in terms of the growing body of signatories is at least partially explained by their assessment that "the Accord offers all the PR potential and heavyweight legitimacy and very little of the normative obligation of the international legal language" (Gorwa and Peez 2020, 277). However, their characterization of Microsoft as a "quasi-diplomatic entity" (based on Hurel and Lobato 2018) ultimately points back into the direction of the diplomatic tables where the seats are taken by states.

The reports of the GGE's death in 2017 seem to have been greatly exaggerated given that the sixth round of the process has started in December

2019. The fact that twenty-five UN member states will again meet to discuss the application of international law to the cyber domain and cyber norms is in itself not a guarantee for success, although sources say that the 2017 round found quite a lot of common ground, in addition to the disputes that eventually blocked consensus. As the General Assembly of the UN thickened the diplomatic cyber plot by also voting through the Russian resolution that called for the installation of an Open-Ended Working Group (OEWG), the revival of the UN GGE is in no way "business as usual." Russia has claimed the moral high ground and played the card of international political legitimacy. The Russian delegation built its case for the OEWG on the principle that it is open to the participation of all states and renounced the UN GGE as "the practice of club agreements that should be sent into the annals of history" (cited in Kurowska 2019). As one of the permanent members of the Security Council, Russia is assured of a seat in that club, but given their sponsorship of the OEWG resolution the stakes are high. The parallel tracks have ushered in a state of Mutually Assured Diplomacy: it is more than likely that either both processes yield a result or that both will fail (Broeders 2019). If one fails on account of one political camp, the other camp is likely to respond in kind and derail the other process. This will complicate an already difficult process. Getting agreement on how existing international law applies to cyberspace—generally agreed to be the stumbling block of the 2017 GGE round—now has to be navigated in two processes that are at once separate and joined at the hip. Add in the new geopolitics of technical Internet governance and rising tensions about the permanent state of "unpeace" in cyberspace and those working on the diplomatic challenges of cyberspace stability and Internet governance have their work cut out for them.

NOTES

[1] Article 13 F of UNGA 2015: "A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."

[2] See also: https://cyberpeaceinstitute.org/

BIBLIOGRAPHY

Adamson, L. 2020. "International Law and International Cyber Norms: A Continuum?" In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Adamson, L. and Z. Homburger. 2019. "Let Them Roar: Small States as Cyber Norm Entrepreneurs." *European Foreign Affairs Review* 24 (2): 217–234.

Betz, D. and T. Stevens. 2011. *Cyberspace and the State. Towards a Strategy for Cyber-Power*. Abingdon: Routledge for the IISS.

Boeke, S. and D. Broeders. 2018. "The Demilitarisation of Cyber Conflict." *Survival* 60 (6): 73–90.

Broeders, D. 2015. *The Public Core of the Internet. An International Agenda for Internet Governance*. Amsterdam: Amsterdam University Press.

Broeders, D. 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.

Broeders, D. 2019. "Mutually Assured Diplomacy: Governance, 'unpeace' and Diplomacy in Cyberspace." *Global Policy—Digital Debates 2019* 6: 26–29.

Broeders, D., L. Adamson and R. Creemers. 2019. *Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace*. The Hague Program for Cyber Norms Policy Brief. November 2019.

Broeders, D., S. Boeke and I. Georgieva. 2019. *Foreign Intelligence in the Digital Age. Navigating a State of "unpeace."* The Hague Program for Cyber Norms Policy Brief. September 2019.

Buchanan, B. 2016. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford: Oxford University Press.

Creemers, R. 2020. "China's Conception of Cyber Sovereignty: Rhetoric and Realization." In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Deibert, R. 2013. *Black Code. Inside the Battle for Cyberspace*. Toronto: Signal.

DeNardis, L. 2014. *The Global War for Internet Governance*. New Haven and London: Yale University Press.

Efrony, D. and Y. Shany. 2018. "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice." *American Journal of International Law* 112 (4): 583–657.

Eggenschwiler, J. and J. Kulesza. 2020. "Non-State Actors as Shapers of Customary Standards of Responsible Behaviour in Cyberspace." In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Finnemore, M. and D. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *The American Journal of International Law* 110: 425–479.

Finnemore, M. and K. Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52: 887–917.

GCSC. 2019. *Advancing Cyberstability*. Final Report of the Global Commission on the Stability of Cyberspace, November 2019.

Georgieva, I. 2020a. "The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace." *Contemporary Security Policy* 41 (1): 33–54.

Georgieva, I. 2020b. "The Power of Norms Meets Normative Power: On the International Cyber Norm of Bulk Collection, the Normative Power of Intelligence Agencies and How These Meet." In *Governing Cyberspace: Behaviour, Power* *and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Gorwa, R. and A. Peez. 2020. "Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord." In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Greenberg, A. 2018. "The Code That Crashed the World." *Wired*, September 2018: 53–63.

Grigsby, A. 2017. "The End of Cyber Norms." *Survival* 59 (6): 109–122.

Healey, J. 2019. "The Implications of Persistent (and Permanent) Engagement in Cyberspace." *Journal of Cybersecurity* 5 (1): 1–15.

Heinl, C. 2018. "Cyber Dynamics and World Order: Enhancing International Cyber Stability." *Irish Studies in International Affairs* 29: 53–72.

Hill, S. and N. Marsan. 2020. "International Law in Cyber Space: Leveraging NATO's Multilateralism, Adaptation and Commitment to Cooperative Security." In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Hoffman, G. 2020. "Cybersecurity Norm-Building and Signaling with China." In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Hurel, L.M. and L.C. Lobato. 2020. "*Cyber-Norms Entrepreneurship?* Understanding Microsoft's Advocacy on Cybersecurity." In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Inkster, N. 2016. *China's Cyber Power*, Adelphi 456. Abingdon: Routledge for the IISS.

Jervis, R. 1978. "Cooperation under the Security Dilemma". *World Politics* 30 (2): 167–214.

Katzenstein, P., ed. 1996. *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press.

Kavanagh, C. and L. Crespo. 2019. "Confidence Building Measures and ICT." *European Foreign Affairs Review* 24 (2): 187–202.

Kello, L. 2017. *The Virtual Weapon and International Order*. New Haven and London: Yale University Press.

Klimburg, A. 2017. *The Darkening Web. The War for Cyberspace*. New York: Penguin Press.

Klimburg, A. and L. Faesen. 2020. "A Balance of Power in Cyberspace." In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Kurowska, X. 2019. *The Politics of Cyber Norms: Beyond Norm Construction Towards Strategic Narrative Contestation*. EU Cyber Direct: Research in Focus.

Kurowska, X. 2020. "What Does Russia Want in Cyber Diplomacy? A Primer." In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Maurer, T. 2018. *Cyber Mercenaries. The State, Hackers and Power*. Cambridge: Cambridge University Press.

Maurer, T. 2019. “A Dose of Realism: The Contestation and Politics of Cyber Norms.” *Hague Journal on the Rule of Law*, First Online: September 17, 2019.

Mueller, M. 2010. *Networks and States. The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.

Nye, J. 2014. *The Regime Complex for Managing Global Cyber Activities*. Global Commission on Internet Governance Paper Series, Paper No. 1.

Ott, N. and A. Osula. 2019. “The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level.” In *2019 11th International Conference on Cyber Conflict: Silent Battle*, edited by T. Minarik et al., 321–346. Tallinn: CCDCOE.

Pawlak, P. 2016. “Confidence-Building Measures in Cyberspace: Current Debates and Rrends.” In *International Cyber Norms. Legal, Policy & Industry Perspectives*, edited by A. Osula and H. Rõigas, 129–153. Tallinn: CCDCOE.

Roguski, P. 2020. “Violations of Territorial Sovereignty in Cyberspace—An Intrusion-based Approach.” In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Schmitt, M., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schmitt, M., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Segal, A. 2016. *The Hacked World Order. How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.* New York: Public Affairs.

Shires, J. 2020. “Ambiguity and Appropriation: Cybersecurity and Cybercrime in Egypt and the Gulf.” In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

Taddeo, M. 2017. “Deterrence by Norms to Stop Interstate Cyber Attacks.” *Minds & Machines* 27: 387-292.

Tsagourias, N. 2020. “Electorial Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace.” In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders and B. van den Berg. London: Rowman & Littlefield.

UNGA. 1999. A/RES/53/70 *Developments in the Field of Information and Telecommunications in the Context of International Security.* New York: UN.

UNGA. 2010. A/65/201 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: UN.

UNGA. 2013. A/68/98 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: UN.

UNGA. 2015. A/70/174 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: UN.

Governing Cyberspace

OPEN ACCESS

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