# International Law and International Cyber Norms: A Continuum?

Liisi Adamson

# *Chapter 2*

# International Law and International Cyber Norms

## *A Continuum?*

Liisi Adamson

The international community has recognized the need for "rules of the road" in cyberspace not only for individuals and private sector actors but also for states. The issue of responsible state behavior in the context of international peace and security was raised by the Russian Federation already in 1998 when it called for an international dialogue under the auspices of the United Nations (UN) (UNGA 1998; UNGA 1999). Over the past two decades that regulatory discussion pertaining to cyberspace has evolved from a possible multilateral treaty to application of existing international law, and to the development and application of cyber norms.

Norms of responsible state behavior in cyberspace, or more commonly noted as *cyber norms*, have developed into a very broad research focus that can be part of various different discourses in the realm of cybersecurity. Norms, in general, can be found everywhere, from everyday interactions to norms that have been codified as law. Yet, in the interactions between states as well as in the academic discourse cyber norms and international law are often perceived as two different tracks of regulatory approaches. Mainly inspired by the work of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter UN GGE), norms in cyberspace are increasingly approached as nonbinding and voluntary in nature. The latter aspect is often interpreted as being a pathway to easier consensus in a challenging realm. At the same time, international law is portrayed as a binding source of normative behavior, application of which often leads to contestation among states.[1]

This chapter argues that norms and international law are not detached from each other. Instead, they are mutually reinforcing and ought to not be seen as two completely different parallel discourses. At the same time, not all norms are to be seen as international laws. Instead, norms of responsible state behavior ought to be seen in terms of continuums. A first continuum focuses on the spectrum from nonbinding norms to hard law. A second continuum emphasizes the specificity of norms.

Thus, the article first elaborates on the move to international law in the cybersecurity and state behavior discourse from a historical perspective. Second, the article then explains the origins of the cyber-norms discourse and how the norms discourse was and is seen as an easier avenue to achieve consensus on after the contesting approaches to application of international law. However, the opaque nature of the concept of nonbinding, voluntary norms in the context of cybersecurity can hamper the implementation of said norms. Furthermore, one could argue that cyber norms now mean everything and nothing at all. Last, the article argues that the binary dialogue of international law *versus* norms could be undermining the whole discourse. Instead, norms and international law ought to be seen as building on each other.

## RULES OF THE ROAD: THE MOVE FROM INTERNATIONAL LAW TO CYBER NORMS

The origins of the *cyber-norms* discourse can be found in a proposal for an United Nations General Assembly (UNGA) resolution by Russian Federation to the UN First Committee—the Disarmament and Security Committee, which later was adopted as the first resolution in the series pertaining to “Developments in the field of information and telecommunications in the context of international security” (UNGA 1999). In 1998, Russia claimed that the world had entered through the development and application of new information technologies and means of telecommunication qualitatively a new stage of scientific and technological revolution. While this revolution had brought about many positive developments, it was essential to consider, even if at the time only potential in nature, the threats that such rapid growth of dependency on information and telecommunications technologies (hereinafter ICTs) could present. Russia put forth that ICTs could be used for purposes incompatible with the objectives of maintaining international peace and security and such technologies could breach several established international law principles, such as nonuse of force, non-intervention, and respect for human rights and freedoms. Thus, Russian foreign minister Igor Ivanov concluded that “such a threat requires that preventive measures be taken today” (UNGA 1998). The international community could not permit the emergence of a “fundamentally new area of international confrontation, which may lead to an escalation of the arms race based on the latest developments of the scientific and technological revolution" (UNGA 1998). Carried by the possible arms race and conflict mind-set, the proposal called for a ban on information weapons to prevent information wars, as information weapons could have the destructive effect comparable to weapons of mass destruction (UNGA 1998). Hence, the issue of international regulation of ICTs was raised in the context of possible future conflicts among states,[2] and Russia was the first country to link international law and information security in the context of international peace and security.

Even though the 1998 Russian proposal to discuss information security-related issues in an international setting had merit, the rest of the international community was not immediately drawn to the idea to deliberate the regulation of ICTs. The Russian proposal was perceived as an invitation to negotiate a potential multilateral treaty to stop the proliferation of information weapons and prevent information wars.[3] The United States, a historically technologically powerful country, entered the republican Bush administration era in 2001. Due to different policy priorities in the early 2000s and the skepticism toward Russian proposals, considerations for responsible state behavior were deadlocked. The West was not interested in discussing a possible treaty to regulate behavior or curtailing developments in cyberspace. It was only six years later, in 2004, when the resolution served as a basis for convening the first session of the UN GGE under the chair of Russia. The task for the expert group was to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them. Even though it was the first UN GGE convened under the aegis of the 1998 "Russian" resolution, it yielded no real outcome (UNGA 2005).

## The Catalyst

A broader discussion on the regulation of cyberspace started a little over a decade ago. The catalyst for a deeper regulatory discussion was the denial-of-service (hereinafter DoS) and distributed-denial-of-service (hereinafter DDoS) attacks against the Estonian government, e-services and financial sector in April–May 2007 (Tikk et al. 2010, 14–35). This incident made it visible to the international community how vulnerable ICT-reliant states can be (Aaviksoo 2010). Although there was no physical damage to the servers, systems, and X-road infrastructure,[4] the DoS and DDoS attacks halted the functioning of several governmental vital services, which at the very least caused financial damage, but more importantly showed where digital states are vulnerable. Moreover, due to the supposed involvement of a neighboring government, this was also the first time tensions between states moved to a completely new realm of actions.[5] If the attacks had been attributed to Russia as a state, it would have been a clear indication that cyber operations have moved qualitatively to a different level and have become politicized. The 2007 Estonia attacks showed that there is a new possible domain for interstate conflict, which was promptly proven during the 2008 Georgia–Russia war. A rise in state-sponsored offensive activity in cyberspace led to calls for a secure and stable cyberspace in multiple avenues.[6]

Besides the diplomatic process among states under the aegis of the UN, the Estonian incident in 2007 and Iranian Stuxnet incident in 2010 also led to the start of the *Tallinn Manual* process.[7] It was one of the first academic initiatives and focused on putting forth an interpretation of existing international law pertaining to conflict and laws of war (*jus ad bellum* and *jus in bello*). The focus on conflict was understandable due to the catastrophic picture that was painted by policy makers and academics alike of the effects that cyber incidents could have.[8] Stuxnet had after all signified another qualitative leap from politically motivated operations to offensive state-sponsored cyber operations. It also raised questions of low-intensity conflict (Buchan 2012; O'Connell 2012) and assured the academics working on the normative framework for cyber operations and laws of armed conflict. Even though Stuxnet was never attributed to a state, the technical analysis left no doubt that at the very least, the offensive operation was backed by a nation-state (De Falco 2012), which once again emphasized the necessity to address the application of international law in cyberspace. The *Tallinn Manual* project was spearheaded by then newly created NATO Cooperative Cyber Defence Centre of Excellence, a NATO-accredited cyber defence hub, established in Tallinn, Estonia, in 2008. Ever since, the NATO CCD COE has become one of the strongest academic voices in the discussion revolving around the application of international law to cyberspace and operations.

After 2007, the conflict-focused regulatory discourse rebooted the UN GGE process, which convened after a five-year hiatus for their 2009–2010 session under the chair of Russia. Even though the United States, Russia's strategic contestant and another cyber power, still did not want to discuss the negotiation of a cybersecurity treaty, the new Obama administration broke the deadlock in discussions and shifted conversation from a possible multilateral treaty to responsible state behavior. Since 2009, the Obama administration advocated a general approach that favored the development of multilateral norms for responsible state behavior in cyberspace. The Cyberspace Policy adopted in 2009 emphasized that the "United States cannot succeed in securing cyberspace if it works in isolation" (The White House 2009, iv), which was a contrast to the policy of Obama's predecessor. The policy continued stating that "international norms are critical to establishing a secure and thriving digital infrastructure" (The White House 2009, 20). The Obama administration adopted an outward-looking and "norms-based" approach to international regulation of cyberspace, which paved the way for a cyber-norms discourse, including in the framework of the UN GGE.

The UN GGE has been a high-level diplomatic avenue for the discussion of responsible state behavior in cyberspace, where the strategic contestants United States and Russia among others are pushing forward their views and value systems. More than half of the world's countries—115 as of 2018—have sponsored the 1998 Russian resolution,[9] which indicates their support for and prioritization of the issue. However, the original resolution also asks states to provide the committee with their views pertaining to the developments in the field of ICTs in the context of international security. This call is reiterated annually. Here, less than half of the world's countries—seventy states as of 2018 have replied to this call.[10] In the face of criticism pertaining to the representation issues and the fact that the UN GGE is a closed process with limited outcome,[11] the UN GGE has adopted three reports, in 2010, 2013, and 2015, which are considered cumulative in their recommendations.

## The Progress

The task for the 2009/2010 UN GGE was identical to the previous UN GGE in 2004/2005: to study both the threats in the sphere of information security as well as suggest cooperative measures to strengthen the security of global information and communication systems. This time the UN GGE identified several motives for disruption, sources of threats as well as objectives. The 2009/2010 session resulted in a consensus report outlining the main threats stemming from the development and use of ICTs to international peace and security, such as the terrorist use of ICTs, ICTs as instruments of warfare and intelligence, attribution issues, use of proxies, protection of critical infrastructures, ICT supply chain security, and ICT capacity and security differences among states (UNGA 2010). Ever since, the UN GGE has become one of the most important avenues for regulatory discussion pertaining to the maintenance of international peace and security and the development and use of ICTs.[12] Bringing together strategic contestants, agile tech adopters and developing countries, the UN GGE has offered a venue to discuss which threats result from the development and the use of ICTs to international peace and security and how to prevent and mitigate such threats through the application of norms, international law, confidence-building measures[13] and capacity-building measures.[14]

During the hiatus year of the UN GGE, Russian Federation attempted to propose another opportunity for a negotiation of a cybersecurity treaty. Namely, in 2011, the Russian Ministry of Foreign Affairs put forth a Draft Convention on International Information Security (The Ministry of Foreign Affairs of the Russian Federation 2011). The general values and ideas of the convention were the same as in the original 1998 resolution proposal. The overall aim of the convention was to prevent "possible uses of information and communication technology for purposes not compatible with ensuring international stability and security" (The Ministry of Foreign Affairs of the Russian Federation 2011). With a heavy focus on sovereignty and the governance of a "sovereign information space," the convention did not find support among the like-minded Western allies. The Obama administration was still focusing on international norms and application of international law for responsible state behavior in cyberspace.

The following 2013 UN GGE report was heralded as a qualitative leap forward in regulating state behavior in cyberspace (Wolter 2013). Its major contribution lies in the fact that the group was able to conclude that international law, and in particular the UN Charter, applies to cyberspace and the activities therein (UNGA 2013, para. 19). The year 2013 was also the first time when the UN GGE included a section in its report on "Recommendations on norms, rules and principles of responsible behavior by States," which were seen as norms deriving from existing international law. Even though the report concluded that unique attributes of ICTs might warrant the development of additional norms over time, the main focus lied still with international law (UNGA 2013, para. 16). The report named a number of international law norms and principles that states ought to abide by ranging from sovereignty, including the international norms and principles that flow from sovereignty, to human rights and state responsibility (UNGA 2013, para. 19–23). This was a big step in the thus far binary discussion on whether international law applies or not. Together with the *Tallinn Manual on the International Law Applicable to Cyber Warfare* published in 2013 (Schmitt 2013), high hopes were put on international law to provide the normative framework applicable to states' cyberspace activities. The norms discussion continued in connection to international law. To keep the momentum, the UNGA decided to gather another UN GGE as soon as possible.

## The Turn

The 2015 iteration of the UN GGE was tasked with analyzing the specific application of international law principles elaborated in the 2013 report. However, this turned out to be a contested area of study, as states' understanding and interpretations of international law in general already vary greatly,[15] let alone in the context of cyberspace and responsible state behavior. The application and interpretation of international law reflect different value systems that states have. These fundamental differences necessitated an approach that would allow the group to not address the disputed issues regarding international law. In an effort to make progress on previous groups' work, the UN

GGE turned to a new construct to get past the contestation: general nonbinding, voluntary norms, rules, and principles for the responsible behavior of states. The latter, that is, norms as a concept, which had been in 2013 report deriving from international law and thus, deeply connected to it, was now presented as a different source for guidance regarding responsible state behavior than international law. This was reflected in the fact that international law and norms, rules and principles were now two different sections in the UN GGE report (UNGA 2015b, sec. III and VI). Moreover, the new norms, rules, and principles section reflected to a great extent (with some exceptions) already existing international law (for further elaboration, see UNODA 2017). The UN GGE, however, did not put forth any conceptualization regarding the relationship between the proposed recommendations of norms and international law. Yet, this conceptual opaqueness seemed to not be a concern. The U.S.-led voluntary, nonbinding norms approach, as argued by some, was a way sidestep the question of a possible cybersecurity treaty amid conflicting views on the application of international law, and at the same time allowed states to articulate issues that require more normative guidance than international law currently offers (Tikk et al. 2018b, 20–21). Outside the UN GGE, despite the fact that norms were seen as voluntary and nonbinding in the context and framework of the UN GGE, the following academic (Crandall et al. 2015; Finnemore 2017, 2011; Finnemore et al. 2016) as well as policy[16] discussion saw *cyber norms* the same way as the UN GGE. Thus, the narrative created by the UN GGE of norms as an alternative to binding international law had carried over to the wider cyber-norms debate.

However, the eleven recommendations for cyber norms (UNGA 2015, para. 13) proposed by the UN GGE in 2015 reflect to a great extent already existing international law. The implementation guide for said norms was left as a task for the following UN GGE that commenced its work in 2016. In 2017, however, the UN GGE failed to reach consensus. For the first time, two countries—the United States and Cuba—explained their views as to the failure of the closed and nontransparent process. The United States argued that the process failed over states' unwillingness to clarify how specific aspects of international law, such as law of the armed conflict or state responsibility, apply to cyberspace. Furthermore, the United States saw the lesser extent of the agreement in the 2017 UN GGE as backtracking the progress that had been made with previous reports (Markoff 2017). Cuba, on the other hand, argued that reinterpreting law of armed conflict would legitimize cyberspace as a domain for military conflict, giving thereby state-sponsored cyber operations a green light (Cuba's Representative Office Abroad 2017).

While the progress at the UN GGE stalled due to strategic, value, and interpretation differences, the international dialogue outside of the UN GGE continued. The year 2017 also marked the publication of *Tallinn Manual*

*2.0 on International Law Applicable to Cyber Operations*, which this time focused on peacetime operations as well as provided a revised look at the law applicable during conflict (NATO CCD COE 2017). The second iteration of creating the interpretative guidelines attracted over fifty states in the Hague Process. This was, however, in a merely consultative, not substantively contributing role.[17] The states participating in the Hague Process did not put forth their official positions on the interpretation of international law.[18] Thus, the *Tallinn Manual* represents an academic process focusing solely on the application of international law. The policy action in the parallel track has moved from application of international law and norms deriving therefrom to a dialogue focusing on international law and *cyber norms* without a clear understanding what the status and meaning of the latter vis-à-vis the former is. This has led to methodological and conceptual opaqueness.

## INTERNATIONAL NORMS

The political, as well as academic focus on *international cyber norms,* aims at reconciling the contestation among different views. Even though the vision and characteristics, how peace and security ought to be achieved in cyberspace have divided the discourse into multiple views[19] they still share the understanding that cyberspace and activities therein need regulation. Yet, the focus on cyber norms that the international community has seen since 2013 and especially after the 2015 UN GGE session is no silver bullet for fundamental differences among stakeholders. Different understandings of the development, role, and form of norms have created diverging views as to the necessity and utility of norms for cyberspace and norms for responsible state behavior. At the same time, the initiatives for creating or developing the norms discourse have not been able to unequivocally explain what norms are, why norms are needed, what type of norms are considered and how this discourse is or is not different from the international law discourse that has been going on for the past decade.[20] The Western approach highlights regulation through existing legal and other regulative frameworks. Yet, they fail at providing an understanding of the application and context-specific interpretation of said frameworks. At the same time, latching on to the novelty argument surrounding cyberspace activity, the Sino-Russian coalition is lobbying for a new multilateral cyber-specific legislation. Different approaches to the regulation to cyberspace reflect that the inherent differences in the state approaches pertain not only to norms, laws, and cyberspace, but toward a legal, strategic, and regulatory culture, as well as the understanding of the existing world order in a wider sense (Roberts 2017).

The definition of what an international cyber norm is depends on the disciplinary perspective of the person who poses the question. Those firmly believing in the adequacy and sufficiency of existing international law do not necessarily comprehend the utility of norms in a more general sense, especially in their nonbinding, voluntary form (Grigsby 2017) and at times conflate norms and cyber norms automatically with international law (Schmitt et al. 2014; Schmitt 2018). Defining a norm from the legal perspective entails mostly a strict view of norms as laws established by treaties or customary international law. From a more philosophical perspective, norms could be understood, for example, as social norms or ethical norms. From the international relations and especially constructivist perspective, international norms are defined as shared expectations or standards of appropriate behavior accepted by and applied in a certain community of actors with a given identity (Martinsson 2011, 2; Khagram et al. 2002, 4; Klotz 1995, para. 14; Katzenstein 1996, para. 5).

Norms can take different forms, as there is no single definition or one particular form of norms. According to one categorization, norms can be either constitutive or regulative. Some norms can have a constitutive effect, which means that they will specify what actions will cause others to recognize a particular entity (Katzenstein 1996, 5). For example, the Montevideo Convention establishes what entities can be considered states (Seventh International Conference of American States 1933). Its criteria have come to be accepted as the international norm on what constitutes a state. Regulative norms, on the other hand, are standards for the proper behavior for an entity with particular identity (Jepperson et al. 1996, 54). This entails in the context of responsible behavior of states in cyberspace, for example, standards defining what a properly conforming state would do in particular circumstances. Thus, regulative norms can prescribe or proscribe behavior for already constituted entities. These norms establish expectations how those defined entities will behave in varying circumstances (Jepperson et al. 1996, 54). This article focuses on responsible behavior of states. According to this categorization, the article would look into states and the regulative norms that prescribe, regulate, and constrain states' behavior in cyberspace.

## Continuums of Norms

Yet, instead of binary approaches, this article proposes to address norms in terms of continuums.[21] The first continuum ranges from norms that have been codified into hard laws to soft law to voluntary, nonbinding norms. Generally, laws are expressions of norms that the international community accepts. States conform their behavior to laws because of the wide acceptance of the underlying norms (Sloss 2006, 170). Moreover, international law often also serves an expressive function. States become a party to a treaty or engage in discussions to express their support for the emerging norm (Sloss 2006, 187).[22] International law provides a baseline to evaluate behavior—whether it conforms to the expectation of appropriate behavior in the international community or not—and threatens consequences for noncompliance. The aim of international law norms, as well as other regulative norms, is to induce a certain behavior. International law facilitates this behavior by delivering the framework and vocabulary that enables international politics among the international community (Klabbers 2017, 18).

International law is to a large extent comprised of hard norms. Treaty law and customary international law are the most binding forms of international law that also means that upon breaching the obligations therein state responsibility and sanctions mechanisms could apply. However, international law increasingly encompasses a substantive body of soft norms as well (Terpan 2015; Chinkin 1989). The body of international law is increasingly seen as a continuum between law and non-law, as formal law ascertainment has not managed to offer solutions to various legal phenomena in the international arena or offer them fast enough. Thereby, norms enshrined in soft instruments, as opposed to hard instruments such as treaties, belong to the continuum between hard and soft norms (D'Aspremont 2011, 128–29). On the other end of the bindingness spectrum[23] are completely legally nonbinding, voluntary norms, which does not mean that they might not be binding socially or morally and call for corresponding consequences once breached. The recommendations for norms made by the UN GGE in 2015 were from the outset framed as being nonbinding, voluntary norms. The Code of Conduct proposed by the Shanghai Cooperation Organization similarly frames the norms in the document in voluntary terms (UNGA 2011, 2015a). At the same time, the UN Charter, the applicability of which was confirmed by UN GGE in 2013 in the norms, rules, and principles section of the report comprises solely of hard norms as accepted by the international community (UNGA 2013, para. 19).

The second continuum that needs to be considered moves on the scale from general standards to specific rules. Norms can be understood as general standards, which are often goal-oriented and allow discretion for interpretation and do not prescribe specific action, which is needed to conform by the standard. Specific rules, however, allow for very limited discretion and set red lines in order to convey an obligation to achieve a certain outcome through certain means and measures (Wolfrum 2010, para. 65 ff). Thus, rules work well in circumstances when there is no solidarity or there is limited trust among the community. At the same time, the issue to be regulated occurs often. On the other hand, standards fulfill their intended outcome in opposite circumstances. Since standards are open-ended and allow for discretion, they require trust and solidarity among the community. When the issue to be regulated occurs rarely, that is, single isolated incidents, standards alongside trust ensure that given the circumstances, the actors will balance all relevant interests while making the decision on how to act (Koskenniemi 2019).

When it comes to the UN GGE norms, majority of them seem from the outset to be rather specific, that is, they have been cast in ICT-specific terms. Even though they pertain to specific "siloed" categories, such as cooperation (UNGA 2015b, para. A, D, H, J), due diligence of transit states (UNGA 2015b, para. C), critical infrastructure protection (UNGA 2015b, para. F, G), human rights protection (UNGA 2015b, para. E), and protection of CERTs (UNGA 2015b, para. K), they are essentially cast in the form of standards, providing no further guidance than the basic goal-oriented obligation set forth in the norm.

For example, the UN GGE 2015 report put forth a norm that state should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (UNGA 2015b, para. 13[C]). Even though it is made ICT specific through the addition of "using ICTs," it still puts forth a general obligation of due diligence in cyberspace. The latter is a standard in itself, which means that the ICT specificity of it has created marginal additional value. The use of general standards applies to norms in the SCO's Code of Conduct's as well. Even content wise specific norms' proposals for the protection of the public core of the Internet[24] or the norm against the manipulation of the integrity of financial data[25] are inherently standards. Thus, considering the uncertainty and the novelty of activities in cyberspace, the push for standards instead of rules makes somewhat sense. Standards are useful when stakes and the cost for errors are high. This has been inherently the case in cyberspace. However, considering the state of the regulatory debate surrounding cyberspace, political contestation, and the lack of trust and solidarity among the international community, the likelihood of implementation and purposeful functioning of these standards is small.

Thus, even though the concept of norms has grown to be used in the cybersecurity discourse as indicating only voluntary and nonbinding nature, the view of norms ought to be much wider. Yet, even when options are abundant and clarity would help with reducing uncertainty, participants in different norms discussions are reluctant to define what they mean by norms. They are often conjoined with the notion of responsible state behavior. Norms are seen as a tool to limit the malicious or negligent behavior of actors and incentivize desired behavior, thereby defining and explaining acceptable and unacceptable behavior.[26] If binding international law is not clear or its application is contested due to grave political differences, norms of different nature may offer an avenue for striving toward predictable behavior of states, creating trust and stability.

Hence, the article sees cyber norms for responsible state behavior in the broadest sense as legally relevant expectations, in the form of rules or standards, regarding appropriate behavior in cyberspace among the international community. Yet, norms in and of themselves do not guarantee compliance. All emergent norms must compete with existing or even countervailing ones, as norms are not created in a vacuum. Whereas new norms do not guarantee action nor do they determinate the results of said norm, they can legitimize new types of action (Jepperson et al. 1996, 56). At the same time, if complied with, norms also channel, constrain, and constitute action. As such, norms are "a fundamental component of both the international system and actors' definitions of their interests" (Klotz 1995, 15). Cyber norms regulate or the very least guide, depending on their nature, the behavior of states in cyberspace (Iasiello 2016, 31–32).

## Different Shades of Norms

Norms are not all equal, nor are they created, implemented, or interpreted equally. Norms may be different in terms of the sphere that they are established in. For example, the UN GGE has proposed global norms applicable to all. At the same time, norms agreed upon in the SCO (e.g., see Shanghai Cooperation Organization 2019), OSCE, ASEAN Regional Forum (hereinafter ARF) are regional norms. Additionally, there can be a wide variety of domestic norms that each state can enact. Norms vary also in terms of their content. As shown above, norms can be specific, for example, pertain to a particular part of critical infrastructure such as the submarine cables or they can be general and address the whole cyberspace and activities therein. One of such norms is the cooperation norm in the UN GGE 2015 report. It establishes that "States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security" (UNGA 2015b, para. 13(a)). This norm is a blanket suggestion for states to cooperate, leaving a wide room for interpretation.

The interpretation of norms adds another layer of complexity. As norms are expectations of behavior in a certain community, there might be differences of opinion with respect to the existence of the norms, that is, whether there exists a norm at all. For example, for some countries reporting of ICT incidents might be a norm, for others it might not. There might also be difference of opinion, when it comes to applicability of a norm. In this instance, there is an agreement that there is a norm, but disagreement about its application. For example, some characterized the Stuxnet attack on Iranian nuclear facility as an armed attack, which would have allowed Iran to use self-defence measures under UN Charter Article 51. At the same time, there were also those, who asserted that the attack did not reach the level of use of force in order to be considered an armed attack. As such, it remained a below-the-threshold operation which would have prevented Iran from acting in self-defence. In this case, there is an agreement that states have the right to act in self-defence, if there is an armed attack. However, there is disagreement whether the cyber-attack reached the threshold of an armed attack or not. Third, there might be variations of application of the norm, that is, interpretation of how to apply the norm in a particular case. This would be the case, for example, with the UN GGE 2015 report recommended norms, as there is no uniform interpretation guidance, all states can interpret them as they wish.

What connects this fragmented picture of norms is that they are all created through interaction among different actors in the international community. This is especially true when it comes to international norms. As the international level does not have a single authority who could prescribe or proscribe norms upon the international community, it is generally understood that most international norms for states are created through the interaction of states.[27] This does not mean that all international norms are created by states. Yet, considering that states are still the main subjects of international law, creating binding norms regulating their behavior still belongs to the purview of states. However, norm-creation in a broad sense is not just the prerogative of states or powerful states for that matter. Non-state actors and states alike can act as norm entrepreneurs. This has been particularly evident in the cybersecurity discourse.[28] It is then up to states to decide whether these norms, created or championed by non-state actors or nonbinding and voluntary, are legally relevant for them or not. As a result, some of those soft or voluntary, nonbinding norms created in the interaction among states or put forth by non-state actors can harden and become binding treaty or customary law, backed by responsibility and liability mechanisms in occurrence of noncompliance.

## THE FUTURE

The policy action regarding "the rules of the road" has not dealt with norms in such detail, rather the calls for promoting voluntary, nonbinding norms have become ubiquitous and opaque without clear understanding of what are the norms that are being promoted, how they should be implemented and what is the impact of such calls. The intricacies and different "shades" of norms are not always apparent.

On the one hand, the conceptual opaqueness created by the UN GGE and carried forward by states allows for room of manoeuvre. The conceptual and terminological opaqueness serves the interest of those who want to maintain the regulatory grey areas. States not agreeing on the binding rules of the road and instead focusing on developing voluntary, nonbinding cyber norms make use of the permissive system of international law. When the rule is what is not prohibited is permitted, states can make use of the grey areas with no direct violations of international law.[29] Legal uncertainty and ambiguity surrounding the existence, content, and interpretation of a normative framework for activities in cyberspace is thus instrumentalized by states for their own benefit (Mačak 2017, 887).

In addition, cyber norms, as put forth by the UN GGE and promoted by states, have been framed as voluntary, nonbinding, and thus qualitatively different from international law norms. This means that there is no framework for implementing and enforcing them, which often leads to calls for the end of cyber norms (Grigsby 2017; Tikk et al. 2018a; van de Velde 2018; Soesanto et al. 2017) and for getting "past" cyber norms (Hampson et al. 2017; Segal 2017). Thus, norms, which were and are seen as a way out of the contestation regarding international law, are seen by many in rather grim tones due to their voluntary nature. Regardless of enforceability and their binding or nonbinding nature, norms establish expectations in the international community and delineate what is acceptable and unacceptable behavior. Norms influence state behavior (Sloss 2006; for an opposite view, see Goldsmith and Posner 2005). Even though cyber norms that are considered voluntary, nonbinding do not allow for legal consequences, such as countermeasures or self-defence, there are several other more political responses (such as retorsion, naming, and shaming that leads to reputation loss [Sloss 2006, 194], economic and diplomatic consequences) that can be more effective than legal consequences the use of which is highly regulated (Adamson et al. 2017).

The conceptual opaqueness regarding norms, international law, and their relationship is reflected in the cyber norms discourse by the fact that cyber norms now have come to mean everything and at the same time nothing at all. From the UN GGE interpretation, the previously existing connection between international law and norms has been significantly downplayed, indicating that norms are something different than international law. At first, states and academics alike were enthusiastic of the flexibility and vagueness of the concept of norms of responsible state behavior framing it as generally a good thing that promises progress for the establishment of rules of the road in cyberspace. Norms were perceived as being more malleable than hard laws. Yet, increasingly the concept of *cyber norms* acts as a "sponge for meaning, soaking up whatever content is nearby."[30]

Moreover, putting forth cyber norms as standards, implementation of which relies on overall solidarity and trust among the international community, might turn out to be a futile effort. Considering the contestation and strategic behavior surrounding regulatory efforts, the continued increase of offensive cyber activities, and the rise of political attributions instead of legal ones, it is clear that there is significant lack of trust in the international community. Without trust, however, there is no meaningful way to apply the agreed-upon standards or hope for reciprocated behavior on others' part. At the same time, there is no space nor political will to create red lines rules, as cyberspace activity is largely unpredictable due to exponential technological development. Thus, the challenge here is to create actionable norms, whether standards or rules, in and for a highly unpredictable, contested, and strategic environment.

While there is a push forward on the progress regarding international legal norms applicable in cyberspace, states do not necessarily interpret cyber norms as legal norms, emphasizing often separately the adherence to international law and the support for norms for responsible state behavior in cyberspace. The latest *National Cyber Strategy of the United States of America*, for example, states that "International law and voluntary non-binding norms of responsible state behavior in cyberspace provide stabilizing, security-enhancing standards that define acceptable behavior to all states and promote greater predictability and stability in cyberspace" (The White House 2018, 20). This clearly shows that for the United States, norms and international law are as regulatory frameworks two complementary, yet conceptually separate things. Without defining the relationship between international law and international norms of behavior that have been created and are created, the opaqueness might lead to fragmentation and eventually unclear guidance for state behavior. This runs contrary to the object and purpose of cyber norms and norms in general, as norms are supposed to provide clarity, stability, and predictability.

It is apt to recall that norms and international law influence, condition, and develop dependent on each other. Voluntary, nonbinding norms do not undermine existing binding hard norms. On the contrary, laws yield a deeper support for the ideas reflected by norms. Cyber norms, even if seen in a voluntary, nonbinding form, are grounded in international law and at the same time, eventually, norms are going to have an impact on the interpretation and development of international law as well. There is no regulatory vacuum or norm vacuum when it comes to cyberspace. New norms build on already existing regulatory order. Thus, as norms build on and influence other norms, it is a fallacy to depict the norms and international law as being detached from each other, as is a fallacy to equate international law and cyber norms.

The UN GGE-proposed recommendations of future norms are clearly grounded in existing international law (see further, UNODA 2017). It is often used as a point of criticism, yet the norms could also be seen as ICT-specific iteration of standards known and accepted in general international law. Existing international law provides the new norms legitimacy and might thus invite a normative pull toward the norms. Denying then the applicability of norms, which are informed by existing international law, means indirectly denying the applicability of international law to cyberspace activities. This contravenes then the accepted and endorsed view that existing international law applies in cyberspace (UNGA 2013). Similarly, relying only on binding international law and denying the impact of other norms, which are not characterized by their binding nature, means denying the ethos and underlying fundamental values carried by those norms. Thus, norms and international law need to be grounded in each other.

In October 2018, both the United States and Russia put forward their vision for the next UN GGE in the UN 1st Committee in the form of draft resolutions. Russia and allies were emphasizing the need for a more open-ended UN GGE process and pushed the international community to accept a draft resolution containing a Code of Conduct 3.0 that integrated the content of previous reports of the UN GGE and the Code of Conduct previously presented by the Shanghai Cooperation Organization (UNGA 2018a). This was a clear move toward politically binding norms.[31] The United States and like-minded states continued with the known format of UN GGE and the dual logic of international law and norms, rules and principles of responsible behavior of states. As a novelty, the US draft resolution emphasized the need for UN GGE-participating states to clarify through national contributions how international law applies in cyberspace.[32] Thus far, a few countries, such as the United Kingdom, Estonia, and France, have put forth such declarations. While the progress of regulation for responsible state behavior is welcomed, the conceptual ambiguity continues, hampering the understanding and implementation of already agreed-upon norms and leading to the question whether the norms, in the eyes of the states, are legally relevant or not. If the answer would be no, then it is questionable, what would be the utility and possible impact of such standards. If the norms are considered legally relevant, it would mean that even if they are framed as voluntary, nonbinding, they are still to be considered as connected to international law, informing the cyberspace-specific application thereof. However, if the UN GGE, as a pioneer in the cyber-norms debate continues to promote the conceptual opaqueness, it might lead states to turn inward[33] and look at domestic solutions to international cybersecurity issues instead of embracing the international normative toolbox. Nevertheless, there is hope that the two parallel and hopefully complementary processes—the UN GGE and the Open-Ended Working Group—in the UN manage to make progress and stride toward further clarity regarding responsible behavior in cyberspace in the years to come.

## CONCLUSION

Calls for responsible behavior of states in cyberspace and rules of the road in said space have become ubiquitous. Out of the work of the UN GGE a distinct discourse on cyber norms has emerged. First developed as a response to contestation regarding international law, cyber norms have gradually obtained a rather opaque meaning.

This chapter argued that even though the UN GGE has moved from discussing international law norms to discussing international law and norms, rules and principles, the two are not detached from each other. Norms in general ought to be seen in several continuums, where norms have the potential to move and change when it comes to their binding nature and specificity. Having a "siloed" understanding of norms, meaning considering one type of norms detached from others is detrimental to the international community's understanding of what shapes state behavior. For example, hard norms in the form of international law might not always be the most effective forms of regulating behavior, as they are often accompanied by grave political differences. All norms pertaining to an issue-area ought to be seen as an ecosystem, where norms are mutually reinforcing, sometimes contesting, yet in general inform and influence the application of each other. Thus, when it comes to cyber norms, norms and application of international law to cyberspace cannot be seen as two parallel tracks of regulatory interventions. Norms are not necessarily an easier avenue to achieve consensus amid disagreement on the application of international law. Norms, even in voluntary, nonbinding form, are a powerful tool to change and regulate behavior, but not when they mean everything and nothing at all.

## NOTES

1. Most notably, international law was also a point of contestation in the 2016/2017 iteration of the UN GGE, which did not adopt a consensus report (Markoff 2017; Cuba's Representative Office Abroad 2017).

2. Interestingly, Russia raised the issue of regulation of ICTs in the Disarmament and Security Committee, but not in the UN Sixth Committee, which addresses the development of international law and other legal issues. Especially because the issues that Russia wanted to discuss among states pertained not only to international conflict and sovereignty, but also to terrorist and criminal use of such technologies.

3. The perception was created by point 3(c) in the draft resolution proposal, which called for "advisability of developing legal regimes to prohibit the development, production or use of particularly dangerous forms of information weapons, and of taking measures to combat information terrorism and crime, including the establishment of an international system (centre) for monitoring threats to the security of

global information and telecommunications systems." The Russians defined information weapon in their proposal as a weapon "the destructive effect of which may be comparable to that of weapons of mass destruction." Information war was understood as "actions taken by one country to damage the information resources and systems of another country while at the same time protecting its own infrastructure" (UNGA 1998).

4. The X-road is the data exchange layer for information systems. It is a technological and organizational environment enabling a secure Internet-based data exchange between information systems. X-road is the backbone of all Estonian e-services (Estonian Information System Authority 2018).

5. In his foreword, President Toomas Hendrik Ilves noted that the 2007 attacks in Estonia, even though mild in retrospect, considering our current capacity and capabilities, were the first time "one could apply the Clausewitzean dictum: War is the continuation of policy by other means" (NATO CCD COE 2017, xxiii).

6. For example, UN GGE process, Shanghai Cooperation Organization Code of Conduct process and Organization for Security and Co-Operation's proposals for stabilizing confidence-building measures to be applied among adversaries.

7. The first edition of the Tallinn Manual was published in 2013 with the second iteration published in 2017 (NATO CCD COE 2017; Schmitt 2013).

8. These ranged mostly from nuclear disasters to Cyber Pearl Harbor. Leon E. Panetta stated that "[t]he collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability" (Panetta 2012; Clarke and Knake 2012; Farwell and Rohozinski 2012, 2011).

9. Table of sponsorship of the UN I Committee Resolution 2006–2018 (compiled by the author, available upon request).

10. Table of replies from governments 1999–2017 (compiled by the author, available upon request). Of the cyber powers, Russia has never presented their views on the matter after putting forth the first proposal. The United States has presented their views three times and China four times.

11. Only thirty-eight countries in the world have been part of this process over fourteen years of having UN GGE's. Six countries have been part of all five UN GGE's (China, France, Germany, Russia, United Kingdom, and United States). (Table of membership of the UN GGE 2004–2017, compiled by the author, available upon request.)

12. UN GGE has had five iterations and three of them had a substantial outcome in the form of a consensus report. UN GGE is increasingly also perceived as an avenue of diplomatic negotiations in an issue which lends itself to increasingly contested views on how cyberspace ought to be regulated.

13. Confidence-building measures (CBMs) are a set of practical measures aimed at enhancing interstate cooperation, transparency, predictability, and stability in order to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs. This entails for example exchanging white papers, strategy documents and national views on cyber matters, sharing information and implementing legislation that would allow to do so, encouraging responsible disclosure of ICT vulnerabilities,

and nominating a national point of contact to facilitate dialogue between states on cyber matters. CBMs are often employed among adversaries to increase transparency and thereby maintain peace and security (UNGA 2015b, 9; OSCE 2013, 2016).

14. UN GGE understands capacity-building measures as measures that "provide technical or other assistance to build capacity in security ICTs in countries requiring and requesting assistance" (UNGA 2015b, paras 19–23).

15. For an overview of different approaches to International Law, see Roberts (2017).

16. The language on international law and voluntary, nonbinding norms for responsible state behavior in cyberspace has been increasingly adopted in several multilateral settings (see G7 2017, 2016; US Department of State 2016; NATO 2016a, 2016b; Australian Minister for Foreign Affairs 2017).

17. The Netherlands facilitated the consultation process between the States and NATO CCD COE (NATO CCD COE 2016).

18. Thus far, only United Kingdom, Estonia, and France have officially explained how principles and rules of international law apply in cyberspace according to their understanding (Wright 2019; Kaljulaid 2019; Ministère des Armées 2019).

19. Most notably the like-minded Western view and the Sino-Russo vision of the future of cyberspace.

20. For a solid effort in understanding the different aspects and forms of cyber norms, see Osula and Rõigas (2016).

21. This chapter addresses only the two most pertinent continuums for cyber norms' purpose. For more specific general categorizations of norms, see Bodansky (2004).

22. A good example here is Sweden's actions during the negotiation of the nuclear nonproliferation treaty. It had nothing to gain security wise in signing the Treaty on the Non-Proliferation of Nuclear Weapons; however, it primarily ratified it to express its support for the emerging nonproliferation norm.

23. Bindingness spectrum then ranges from hard laws, which are norms codified in written form and noncompliance with said norms is backed by sanctions, to voluntary, nonbinding norms.

24. The norm pertains to the protection of core logical and physical ICT infrastructure from unwarranted state interventions (Broeders 2015, 2017).

25. The norm is a specific norm for the protection of a specific critical infrastructure component (Maurer, Levite, and Perkovich 2017).

26. On the explanatory power of norms, see Björkdahl (2002, 11 ff).

27. As only states have the formal authority to craft new international legal regimes and authoritatively interpret existing international law (Shaw 2017, 155 ff).

28. This has been particularly visible for example regarding the norm entrepreneurship of Microsoft and Siemens, but also in the work of the Global Commission on the Stability of Cyberspace (see further McKay et al. 2014; Charney et al. 2016; Smith 2017; Microsoft et al. 2018; Airbus et al. 2018; GCSC 2018a, 2018b).

29. PCIJ, SS Lotus, 1927, Publ. PCIJ, Series A, no. 10. (Klabbers 2017, 25).

30. The problematique is inspired by James Shires and Max Smeets' analysis of similar tendencies when it comes to the word "cyber" (Shires and Smeets 2017; see also Futter 2018).

31. UNGA resolutions are not legally binding on states.

32. The draft resolution envisages an annex to the report containing "national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by States" (UNGA 2018b, para. 3).

33. After the non-report outcome of the 2016/2017 UN GGE, US put forth that violations of norms need to be responded to and violators need to be held accountable. It recognized that this may not be achievable through the UN framework, which is why the United States is focusing on imposing consequences, also with like-minded partners and "call out bad behavior and impose costs on our adversaries." The same was echoed by the latest US national cybersecurity strategy (The White House 2017, 2018).

## BIBLIOGRAPHY

Aaviksoo, Jaak. 2010. "Cyberattacks Against Estonia Raised Awareness of Cyberthreats." *Defence Against Terrorism Review* 3 (2): 13–22.

Adamson, Liisi, and Eneken Tikk. 2017. "The International Law Playbook of Consequences: From Acts of Retorsion to Countermeasures." Background Paper for the workshop "Writing the International Playbook of Cyber-Consequences." The Hague.

Airbus, IBM, Siemens, Allianz, Munich Security Conference, SGS, Daimler, NXP, and T-Mobile. 2018. "Charter of Trust: For a Secure Digital World."

Australian Minister for Foreign Affairs. 2017. "Joint Statement: Australia-Japan-United States Trilateral Strategic Dialogue." August 7, 2017.

Björkdahl, Annika. 2002. "Norms in International Relations: Some Conceptual and Methodological Reflections." *Cambridge Review of International Affairs* 15 (1): 9–23.

Bodansky, Daniel. 2004. "Rules vs. Standards in International Environmental Law." *Proceedings of the ASIL Annual Meeting* 98: 275–280.

Broeders, Dennis. 2015. *The Public Core of the Internet, An International Agenda for Internet Governance*. 1st ed. Amsterdam: Amsterdam University Press.

Broeders, Dennis. 2017. "Defining the Protection of 'the Public Core of the Internet' as a National Interest." 190. ORF Issue Brief. https://doi.org/10.1080/23738871.2017.1403640.

Buchan, Russell. 2012. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict & Security Law* 17 (2): 211–227.

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," June: 1–20. https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms%7B_%7DvFinal.pdf.

Chinkin, Christine M. 1989. "The Challenge of Soft Law: Development and Change in International Law." *International and Comparative Law Quarterly* 38: 850–866.

Clarke, Richard A., and Robert K. Knake. 2012. *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco.

Crandall, Matthew, and Collin Allan. 2015. “Small States and Big Ideas: Estonia’s Battle for Cybersecurity Norms.” *Contemporary Security Policy* 36 (2): 346–368.

Cuba’s Representative Office Abroad. 2017. “71 UNGA: Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” June 23, 2017. http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.

D’Aspremont, Jean. 2011. *Formalism and the Sources of International Law: A Theory of the Ascertainment of Legal Rules*. Oxford: Oxford University Press.

Estonian Information System Authority. 2018. “Data Exchange Layer X-Tee.” https://www.ria.ee/en/state-information-system/x-tee.html.

Falco, Marco De. 2012. “Stuxnet Facts Report. A Technical and Strategic Analysis.” Tallinn.

Farwell, James P., and Rafal Rohozinski. 2011. “Stuxnet and the Future of Cyber War.” *Survival* 53 (1): 23–40.

Farwell, James P., and Rafal Rohozinski. 2012. “The New Reality of Cyber War.” *Survival* 54 (4): 107–120.

Finnemore, Martha, and Duncan B. Hollis. 2016. “Constructing Norms for Global Cybersecurity.” *American Journal of International Law* 110 (3): 425–479.

Finnemore, Martha. 2011. “Cultivating International Cyber Norms.” *America’s Cyber Future Security and Prosperity in the Information Age* II: 87–102.

Finnemore, Martha. 2017. “Cybersecurity and the Concept of Norms.” *Carnegie Endowment for International Peace*. http://carnegieendowment.org/files/Finnemore_web_final.pdf.

Futter, Andrew. 2018. “‘Cyber’ Semantics: Why We Should Retire the Latest Buzzword in Security Studies.” *Journal of Cyber Policy* 3 (2): 201–216.

G7. 2016. “Principles and Action on Cyber.” May 27, 2016.

G7. 2017. “Declaration on Responsible States Behaviour in Cyberspace.” Lucca, April 11, 2017.

GCSC (Global Commission on the Stability of Cyberspace). 2018a. “Global Commission Urges Protecting Electoral Infrastructure.” May 24, 2018. https://cyberstability.org/research/global-commission-urges-protecting-electoral-infrastructure/.

GCSC (Global Commission on the Stability of Cyberspace). 2018b. “Global Commission Proposes a Definition of the Public Core of the Internet.” June 27, 2018. https://cyberstability.org/research/global-commission-proposes-definition-of-the-public-core-of-the-internet/.

Goldsmith, Jack L., and Eric A. Posner. 2005. *The Limits of International Law*. New York: Oxford University Press.

Grigsby, Alex. 2017. “The End of Cyber Norms.” *Survival* 59 (6): 109–122. https://doi.org/10.1080/00396338.2017.1399730.

Hampson, Fen Osler, and Michael Sulmeyer. 2017. *Getting Beyond Norms: New Approaches to International Cyber Security Challenges*. Centre for International Governance Innovation.

Iasiello, Emilio. 2016. “What Happens If Cyber Norms Are Agreed To?” *Georgetown Journal of International Affairs: International Engagement on Cyber VI, Assessing Cyber Strategy* 18 (3): 30–37.

Jepperson, Ronald L., Alexander Wendt, and Peter J. Katzenstein. 1996. “Norms, Identity, and Culture in National Security.” In *The Culture of National Security: Norms and Identity in World Politics*, edited by Peter J. Katzenstein, 33–75. New York: Columbia University Press.

Kaljulaid, Kersti. 2019. “President of Estonia: International Law Applies Also in Cyber Space.” Keynote speech CyCon 2019, May 29, 2019. https://www.president.ee/en/meedia/press-releases/15243-president-of-estonia-international-law-applies-also-in-cyber-space/index.html.

Katzenstein, Peter J. 1996. *The Culture of National Security: Norms and Identity in World Politics*. Edited by Peter J. Katzenstein. New York: Columbia University Press.

Khagram, Sanjeev, James V. Riker, and Kathryn Sikkink. 2002. *Restructuring World Politics: Transnational Social Movements, Networks and Norms*. Minneapolis: University of Minnesota Press.

Klabbers, Jan. 2017. *International Law*. 2nd ed. Cambridge: Cambridge University Press.

Klotz, Audie. 1995. *Norms in International Relations: The Struggle Against Apartheid*. Ithaca: Cornell University Press.

Koskenniemi, Martti. 2019. “International Cyber Law: Does It Exist and Do We Need It?” European Cyber Diplomacy Dialogue, EU Cyber Direct.

Mačak, Kubo. 2017. “From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers.” *Leiden Journal of International Law*, September 2016: 1–23. https://doi.org/10.1017/S0922156517000358.

Markoff, Michele G. 2017. “Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.” US Department of State Releases and Remarks. June 23, 2017.

Martinsson, Johanna. 2011. “Global Norms: Creation, Diffusion, and Limits.” CommGAP Discussion Papers. Washington, DC.

Maurer, Tim, Ariel Levite, and George Perkovich. 2017. “Toward a Global Norm Against Manipulating the Integrity of Financial Data.” White Paper. Carnegie Endowment for International Peace.

Mckay, Angela, Jan Neutze, Paul Nicholas, and Kevin Sullivan. 2014. “International Cybersecurity Norms,” 24. https://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/.

Microsoft et al. 2018. “Cybersecurity Tech Accord.” 2018. https://cybertechaccord.org/accord/.

Ministère des Armées (French Ministry of Defense). 2019. “Communiqué_La France s’engage à promouvoir un cyberespace stable, fondé sur la confiance et le respect du droit international.” September 9, 2019. https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international.

NATO CCD COE. 2016. "Over 50 States Consult Tallinn Manual 2.0." 2016. https://ccdcoe.org/over-50-states-consult-tallinn-manual-20.html.

NATO CCD COE. 2017. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, edited by Michael N. Schmitt. Cambridge: Cambridge University Press.

NATO. 2016a. "Cyber Defence Pledge." July 8, 2016.

NATO. 2016b. "Warsaw Summit Communiqué." July 9, 2016.

O'Connell, Mary Ellen. 2012. "Cyber Security Without Cyber War." *Journal of Conflict & Security Law* 17 (2): 187–209.

OSCE. 2013. *Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.*

OSCE. 2016. *Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.*

Osula, Anna-Maria, and Henry Rõigas. 2016. *International Cyber Norms*. https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf.

Panetta, Leon E. 2012. "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security." US Department of Defense. 2012. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Roberts, Anthea. 2017. *Is International Law International?* Oxford: Oxford University Press.

Schmitt, Michael N. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Edited by Michael N. Schmitt. Cambridge: Cambridge University Press.

Schmitt, Michael N. 2018. "International Cyber Norms: Reflections on the Path Ahead." *Netherlands Military Law Review*. https://puc.overheid.nl/mrt/doc/PUC_248171_11/1/

Schmitt, Michael N., and Liis Vihul. 2014. "The Nature of International Law Cyber Norms." 5. The Tallinn Papers. Tallinn. https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn Paper No 5 Schmitt and Vihul.pdf.

Segal, Adam. 2017. "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?" Council on Foreign Relations. https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

Seventh International Conference of American States. 1933. *Montevideo Convention on the Rights and Duties of States*. https://doi.org/10.1007/s13398-014-0173-7.2.

Shanghai Cooperation Organization. 2009. *Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security*. https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf.

Shaw, Malcolm N. 2017. *International Law*. 8th ed. Cambridge: Cambridge University Press.

Shires, James, and Max Smeets. 2017. "The Word Cyber Now Means Everything—And Nothing At All." *Future Tense*, 2017. http://www.slate.com/blogs/future_tense/2017/12/01/the_word_cyber_has_lost_all_meaning.html.

Sloss, David. 2006. "Do International Norms Influence State Behavior?" *George Washington International Law Review* 159: 159–207.

Smith, Brad. 2017. "The Need for a Digital Geneva Convention." Microsoft on the Issues. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Soesanto, Stefan, and D'Incau Fosca. 2017. "The UN GGE Is Dead: Time to Fall Forward." European Council on Foreign Relations. https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

Terpan, Fabien. 2015. "Soft Law in the European Union—The Changing Nature of EU Law." *European Law Journal* 21 (1): 68–96.

The Ministry of Foreign Affairs of the Russian Federation. 2011. *Convention on International Information Security (Concept).* http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publish.

The White House. 2009. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." https://www.energy.gov/sites/prod/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf.

The White House. 2017. "Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017." 2017. https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/.

The White House. 2018. "National Cyber Strategy of the United States of America." Washington. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Tikk, Eneken, and Mika Kerttunen. 2018a. "Cyber Treaty Is Coming : Что Делать ?" Tartu.

Tikk, Eneken, and Mika Kerttunen. 2018b. "Parabasis: Cyber-Diplomacy in Stalemate." Oslo.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. 2010. *International Cyber Incidents—Legal Considerations*. Tallinn: NATO CCD COE Publications.

UNGA (United Nations General Assembly). 1998. "Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary- General." A/C.1/53/3. 1998.

UNGA (United Nations General Assembly). 1999. *A/RES/53/70 Developments in the Field of Information and Telecommunications in the Context of International Security.*

UNGA (United Nations General Assembly). 2005. *A/60/202 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Report of the Secretary-General.*

UNGA (United Nations General Assembly). 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.*

UNGA (United Nations General Assembly). 2011. *A/66/359 49656 Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General.*

UNGA (United Nations General Assembly). 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.*

UNGA (United Nations General Assembly). 2015a. *A/69/723 Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General.*

UNGA (United Nations General Assembly). 2015b. *A/70/174 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications n the Context of International Security.*

UNGA (United Nations General Assembly). 2018a. *A/C.1/73/L.27, Developments in the Field of Information and Telecommunications in the Context of International Security: Draft Resolution*, October 22, 2018.

UNGA (United Nations General Assembly). 2018b. *A/C.1./73/L.37, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, October 18, 2018.

UNODA. 2017. *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary*. New York: UNODA.

US Department of State. 2016. "Joint Statement on Third Annual Nordic-Baltic + U.S. Cyber Consultations." September 16, 2016.

Velde, James van de. 2018. "Why Cyber Norms Are Dumb and Serve Russian Interests." *The Cipher Brief*, June 6, 2018.

Wolfrum, Rüdiger. 2010. "General International Law (Principles, Rules, and Standards)." *Max Planck Encyclopedia of Public International Law*. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1408

Wolter, Detlev. 2013. "The UN Takes a Big Step Forward on Cybersecurity." *Arms Control Today* 43 (7): 25–29.

Wright, Jeremy. 2019. "Cyber and International Law in the 21st Century." Speech on May 23, 2019. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

# Governing Cyberspace