The End of the Road for the UN GGE Process and the Future Regulation of Cyberspace

Henriksen, Anders

Published in:
Journal of Cybersecurity

DOI:
10.1093/cybsec/tyy009

Publication date:
2019

Document version
Publisher's PDF, also known as Version of record

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2019, 1–9
doi: 10.1093/cybsec/tyy009
Research paper

Research paper

The end of the road for the UN GGE process: The future regulation of cyberspace

Anders Henriksen*

Faculty of Law, University of Copenhagen, Karen Blixens Plads 16, DK–2300 Copenhagen S, Denmark

*Corresponding author: E-mail: anders.henriksen@jur.ku.dk

Received 5 July 2018; revised 17 September 2018; accepted 13 November 2018

Abstract

In June 2017, the fifth and so far last of the UN Group of Governmental Experts (UN GGE) were unable to agree on a consensus report that would have brought additional clarity to how international law regulates cyberspace. The article discusses why the UN GGE process seemed to have now reached a dead-end. It argues that the discussion about how Information and Communication Technology (ICT) should be regulated is as much about strategy, politics and ideological differences as it is about law. For the time being, states have too diverging interests and normative preferences for consensus on anything but the most basic of legal findings to arise. The article also offers some suggestions about what the future holds with regard to the regulation of cyberspace. It argues that the collapse of the UN GGE process is likely to lead to a shift away from ambitious global initiatives and towards regional agreements between "like-minded states". In turn, we may well see the gradual emergence of a fragmented international normative structure for ICT. It is also likely that nonstate actors will begin to play a more central role in the efforts to bring legal clarity to the governance of ICT.

Key words: cyber governance; regulation; UN GGE; international law

Introduction

As our societies become ever more dependent on information and communication technology (ICT), ensuring international agreement on what is proper and what is not proper behavior in cyberspace has become one of the most important policy issues of our time. In fact, since the digital world has increasingly become a scene of confrontation and potential conflict among states, norms – both formal and informal – appears to now be the preferred regulatory course for seeking to create stability and safety in cyberspace [1]. In an anarchical cyberspace without "rules of the road" and shared expectations of behavior, stronger states will be free to impose their will on weaker states and minor incidents may escalate and spin out of control.

Since the challenges of ICT was first brought to the attention of the UN General Assembly in the late 1990s, the so-called "UN GGE process" has been the primary avenue for interstate dialogue about the international legal regulation of cyberspace.[1] To use the well-known terminology of Martha Finnemore and Kathryn Sikkink, for purposes of international law, the UN GGE framework has been the main "organizational platform" for states seeking to act as

1 Cyber security is discussed in a range of international fora, including in different UN fora. Reference should also be made to the two-phased UN sponsored *World Summit on the Information Society* (WSIS) held in Geneva in 2003 and in Tunis in 2005. In December 2015, a High-Level meeting of the General Assembly was organized to review the implementation of the documents that had been produced in the course of the WSIS process. For an overview of the various organizational "cyber-platforms" at the UN, see Maurer T. *Cyber Norm Emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-Security*, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011. https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security (20 November 2018, date last accessed). See also the overview in Nye JS Jr, The Regime Complex for Managing Global Cyber Activities, *Global Commission on Internet Governance, Paper Series* 2013, 1. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf (20 November 2018, date last accessed).

"norm entrepreneurs" in cyberspace [2]. Here, "Groups of Governmental Experts" (GGE) (assisted by the UN's Office for Disarmament Affairs) set up by the UN Secretary General to study the "Developments in the Field of Information and Telecommunications in the Context of International Security" have discussed how best to approach the many challenges the new technologies raise. While the process was off to a slow start and the first group of experts was not able to reach agreement on a consensus report, subsequent groups were more successful and over the course of the next decade agreement was reached on a range of noteworthy findings. Among other things, it became clear that everyone agreed that cyberspace is not an unregulated space, where states are free to behave as they please. Rather, as a point of departure at least, it is governed by the same international legal principles that govern the "physical" spaces. But the question of "how exactly" those principles apply to ICT proved much harder to answer. And in June 2017, the fifth and so far final group of governmental experts realized that they had reached a dead-end and could not agree on another report that would have brought additional clarity on the application of international law to cyberspace.

The purpose of this article is two-fold. First, it will explore why the fifth and so far last UN GGE failed. Why was it not possible for states to bring additional legal clarity to how international law applies in cyberspace? Secondly, the article will try to predict what the future has in store *vis-à-vis* the regulation of ICT. How will states now try to bring legal clarity to cyberspace? What will be the main processes and actors?

The article argues that the breakdown of the UN GGE process was actually fairly predictable [3]. After all, despite what many international lawyers seem to believe, the discussion about how ICT should be regulated is as much about strategy, politics and ideological differences (if not more so) than it is about law. And at present, states' interests and normative preferences are simply too diverse for consensus on anything but the most basic of such issues to arise. The article also argues that we should not expect cyberspace to be regulated by a uniform international legal regime anytime soon. The frustrated UN GGE process reflects how difficult it has become for states to agree on some of the most important issues of our time and it is likely to lead to a shift away from ambitious global initiatives and towards regional agreements between "like-minded states". Thus, we may well see the gradual emergence of a fragmented international normative structure for ICT. The article also predicts that non-state actors will begin to take a more central rule in the efforts to bring legal clarity to the governance of ICT.

Since the issue of norms – both informal and formal – feature prominently in the debate about cyber governance,[2] it is worth noting that the present article focuses on the formal norms that one finds in the sphere of international law.

The article proceeds as follows: Section 2 provides an overview of the UN GGE process as well as its most important legal findings. Section 3 explains why the process came to a dead-end by situating the debate about the regulation of cyberspace in a wider strategic and ideological context. Section 4 offers some thoughts about where the efforts to regulate cyberspace will go now before Section 5 offers a brief conclusion.

The UN GGE process

The UN GGE process up until the collapse of the fifth group of experts

The rapid developments in information and communication technology (ICT) was first brought to the attention of one of the main organs in the United Nations in 1998, when Russia introduced a draft resolution in the First Committee of the General Assembly. The resolution – adopted without a vote – noted how new technologies could be used in a destabilizing fashion and therefore affect the security of States. It also invited Member States to inform the Secretary-General of their views on, *inter alia*, the "advisability" of developing international principles to enhance the security of global ICT systems and to assist in fighting information terrorism and criminality (A/Res/53/70 (1999)). In the following years, Russia introduced more or less similar draft proposals (A/Res/54/49 (1999); A/Res/55/28 (2000); A/Res/56/19 (2001)) and in January 2002, the General Assembly asked the Secretary-General to establish a group of governmental experts to report on international concepts for "strengthening the security of global information and telecommunications systems" (A/Res.56/19 (2002)). This first group of experts – officially titled the "United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (more commonly referred to as the "Group of Governmental Experts" or "UN GGE") – consisted of 15 members selected on the basis of an equitable geographical distribution. While it was the ambition of this first group of experts to submit a consensus report that goal turned out to be too optimistic and a final report was never adopted.

The failure of the first GGE did not dissuade the UN and its Member States, however, and by the end of 2005, the Secretary-General set-up a second group of experts to continue the study of ICT threats and possible cooperative measures (Res. A/60/45 (2005)). When the group of experts met in 2009, the 2007 cyberattacks on Estonia and Russia's campaign of cyber-activities in its 2008 conflict with Georgia had heightened awareness among states about the risk of conflict in cyberspace. The Estonian attacks also illustrated how the absence of international agreement on the most basic governing principles in cyberspace increased the risk that a cyber-incident – whether intended or not – could potentially spiral out of control and lead to a damaging conflict. Unlike the first group of experts, this second group managed to reach agreement on a short 2010 consensus report with a set of very rudimentary findings and recommendations (A/Res/65/2001 (2010)). The report noted how states were developing ICTs as "instruments of warfare and intelligence, and for political purposes" and it stipulated how uncertainties about attribution and the absence of common understanding about acceptable behaviour created a risk of instability and misperception. As for the regulation of cyberspace, the report merely noted that norms could be developed over time in order to supplement existing norms and that further dialogue was needed. Procedurally, the report was dealt with in the First Committee's next periodic meeting in the fall of 2010. As other reports adopted by consensus, it was interpreted as reflecting unanimity.

Although the 2010 report did not bring much legal clarity, the mere fact that the experts were able to agree on a report was considered a positive sign and a cause for optimism. Thus, in December

2 "Norms" are usually understood to be widely accepted ways of behaving among members of a certain group. Norms may take many forms and there are different ways of classifying norms. One can distinguish, for example, between cultural and social norms, and informal and formal norms. It is within the group of formal norms we find those accepted ways of behavior that have been created in law-making processes – either domestically or internationally – and thus take the form of law.

2011, the General Assembly set up a third group of experts and this time the group was specifically asked to discuss "norms, rules or principles of responsible behaviour of States" (A/Res/66/24 (2011)). By then, the 2010 Stuxnet-attack on the Iranian nuclear program had uncovered what a targeted covert cyber-operation could accomplish. In 2009, at the initiative of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in Tallinn (Estonia), a working group of independent (Western) legal experts had also begun drafting what would later become known as the first Tallinn Manual on the international law governing cyber warfare. In June 2013, the third UN GGE submitted a consensus report stressing how common "understandings on norms, rules and principles applicable to the use of ICTs" can help advance peace and security (A/Res/68/98 (2013)). More substantively, the report noted that international law and in particular the Charter of the United Nations, as well as the principles of state sovereignty apply to state conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territories. While vague and rudimentary, these findings reflected an emerging consensus that cyberspace is subject to the same general principles of international law that govern the more physical domains. As we return to later, this had been the official position of the United States since 2011, when it presented its International Strategy for Cyberspace. Other states had been more hesitant and China in particular, had consistently stressed how difficult it is to apply international law to ICT [4]. A few months prior to the publication of the 2013 report, the international working group of academic experts set up by NATO to draft a manual for cyber warfare published the "Tallinn Manual on the International Law applicable to Cyber Warfare" – also known as the first Tallinn manual. Here, the experts had unanimously concluded that the general principles in international law for governing the resort to the use of force (*jus ad bellum*) and the legal principles governing the conduct of hostilities (*jus in bello*) apply to cyber operations and that the relevant issue is not "if" but instead "how" such law applies [5]. One more finding in the 2013 report is worth mentioning. The group of experts agreed that human rights and fundamental freedoms apply in ICT. Later in the same year, the General Assembly adopted a resolution on "the right to privacy in the digital age" that recognized the "global and open nature of the Internet" and how "the same rights that people have offline must also be protected online" (A/Res/68/167 (2013)).

In December 2013, a fourth group of governmental experts was created (A/Res/68/243, 2013)) and in July 2015 the group submitted a consensus report that elaborated on some of the findings in the two previous GGE reports. The report explicitly referred to the UN resolutions on the right to privacy in the digital age and offered a list of nonexhaustive views on how international law applies to the use of ICTs by States. Among other things, the experts noted that states have jurisdiction over the ICT infrastructure located within their territory; that they must observe the principles of sovereignty, sovereign equality, the settlement of disputes by peaceful means and nonintervention in the internal affairs of other States. The report also stated that existing obligations under international law are applicable to state uses of ICTs, and that states must comply with their obligations under international law to respect and protect human rights and fundamental freedoms. With regard to the UN Charter, the experts affirmed that it "applies in its entirety" and noted "the inherent right of States to take measures consistent with international law and as recognized in the Charter". The report also stated, however, that there was a "need for further study on this matter". Other noticeable points in the report included its reference to "the principles of humanity, necessity, proportionality and distinction" and the obligation on states not to "use proxies to commit internationally wrongful acts using ICTs" and to "ensure that their territory is not used by non-State actors to commit such acts" (A/Res/70/174, 2015)). The 2015 report was able to keep the interstate conversion on the regulation of cyberspace on track but the discussions had not been easy and a number of important issues were notably absent from the consensus report. Most importantly, despite the vague reference to "the principles of humanity, necessity, proportionality and distinction" cited above, the report did not explicitly state that international humanitarian law potentially applies to cyber-activities.

The fifth and final group of experts

In December 2015, a fifth Group of Experts was created with the hope – among Western states in particular – that yet another round of expert discussions could add clarity to the regulation of cyberspace (A/Res/70/237, 2015)). This time, however, the discussions proved much more difficult and in June 2017, the experts failed to agree on a draft for a consensus report. It appears to have been Cuba and apparently also China and Russia that decided not to accept the draft. Officially, at least, the problem seems to be explicit references in the draft report to the potential applicability of the right to self-defence, the general international law principles of countermeasures and international humanitarian law. In a statement issued after the unsuccessful discussions were concluded, the Cuban representative stated that he was concerned with "the pretension of some ... to convert cyberspace into a theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs". He objected to statements in the draft report that in his mind sought to "establish equivalence between the malicious use of ICTs and the concept of "armed attack ... which attempts to justify the alleged applicability in this context of the right to self-defense". Allegedly, this constituted a "fatal blow to the collective security and peacekeeping architecture established in the Charter of the United Nations", essentially turning the field into a "Law of the Jungle", in "which the interests of the most powerful States would always prevail to the detriment of the most vulnerable". The Cuban representative also highlighted the draft report's references to the law of armed conflict because it "would legitimize a scenario of war and military actions in the context of ICT" [6].

Cuba's official objection to the potential application of the right to self-defense and countermeasures to activities in cyberspace is difficult to accept [7]. After all, as noted above, previous reports had stated that the Charter applies to activities in the ICT environment. The 2015 report explicitly referred to "the inherent right of States to take measures consistent with international law and as recognized in the Charter" and the right to self-defense is, of course, an integral part of the Charter. References to the right to self-defense and the principles of countermeasures in relation to hostile acts in cyberspace are also found in a November 2015 declaration by the G20 [8] and in an April 2017 declaration by the G7 [9]. In the academic literature, the claim that cyber activities may – if sufficiently grave and serious – trigger a right to self-defense or to countermeasures is far from controversial [5, 10].

On the surface, at least, the reluctance by states like Cuba and China to accept that international humanitarian law may apply to activities in cyberspace is less surprising. As already noted, there were no explicit references to humanitarian law in the GGE's 2015 report and that was not a coincidence. As we shall return to below,

in its official statements about how to regulate cyberspace, China has sought to adopt a pacifist view and frequently voiced its alleged concern about the application of the "military paradigm" to cyberattacks. China has stated that there is a risk that this will aggravate "the arms race and militarization in cyberspace". Thus, China's official stance is that the "application of existing laws of armed conflict to cyberspace requires further scrutiny" [11, 12].

Regardless of why China has decided to publicly voice its concern about an undue "militarization" of cyberspace, such a concern is not totally unwarranted. After all, many states have integrated their new cyber-capabilities – at times termed "cyber commands" – into the military chain of command. In addition, as noted elsewhere, even though no one has yet (by November 2018) been killed or even injured in a cyberattack, the debate about ICT security and cyber threats has been dominated by worst-case scenarios of "cyber-armageddons", "cyber Pearl Harbors" and airplanes falling from the sky.[3] The preoccupation with catastrophic cyberattacks against critical infrastructure may well have deflected attention away from what should be of most concern to at least Western states: so-called "below the use of force threshold" operations that consist of various forms of espionage, manipulation of data, criminal activities and different and novel forms of coercion that cause little physical destruction [13].

This, however, should not lead one to rule out the possibility that international humanitarian law could become of relevance to activities in cyberspace. This also appears to be the position of the International Committee of the Red Cross (ICRC). In a November 2017 statement to the United Nations, the ICRC stated that "there is no question that IHL applies to and restricts the use of cyber capabilities as means and methods of warfare during armed conflicts". The ICRC also stressed that by "asserting that IHL applies to cyber operations, the ICRC is in no way condoning cyber warfare, nor is it condoning the militarization of cyberspace" [14]. Indeed, as we shall return to in the following section, it may very well be that a state like China's reluctance to accept the potential applicability of international humanitarian law to harmful cyber-activities has more to do with longer term strategic calculations and a desire to slow the pace of reaching international consensus than bona fide interpretations of international law.

The strategic and ideological context surrounding cyber security

The link between law and strategy

To understand why the overall consensus that international law applies to ICT has yet to materialize into agreement among states on the concrete application of particular legal principles, one must take account of the wider strategic and ideological context. The debate about how international law applies to cyberspace is not merely an academic exercise in legal interpretation but also – if not primarily – about trying to reconcile colliding strategic interests and clashing ideological worldviews [3].[4] For all manners and purposes, the outcome of the debate will determine how states can use modern ICT to further their political agendas, including their foreign policy goals. The discussion is, in other words, to a large extent about how the traditional concepts and tools of statecraft should be applied to the present and future digital age [15]. This, of course, has not been lost on the states, and the major states in particular are actively seeking to promote those norms and legal interpretations they believe will serve their long-term strategic interests.[5]

We have already seen how the Chinese seek to use international law and legal interpretation as a way to prevent the potential application of international humanitarian law to cyber-activities. China traditionally adopts a restrictive position on the legality of using force and it would be natural if it utilized legal interpretations to try to counterbalance American posture in cyberspace [4]. In the cyber security debate, China's traditional support for the UN is reflected in the fact that the Chinese would like the UN to take the leading role in developing consensus on the regulation of ICT. Beijing has therefore been very critical of the Tallinn Manual process that it considers an American NATO effort to maintain US dominance in the information age. To some extent, at least, Russia is a Chinese "ally" when it comes to using international law to counter American dominance of ICT. Moscow worries about the prospects of a "cyber arms race" and it has therefore tried to push for an international agreement modeled on earlier arms control agreements [16, 17]. To Russia, such an agreement may help "level the playing field". Thus, when Russia brought the issue of ICT to the UN, it introduced its resolution in the General Assembly's First Committee on Disarmament and International Security. While Russia acknowledges that international law applies to ICT, it also argues that new laws and institutions are required to ensure long-term stability.

The most dominant power in cyberspace is, of course, the USA. The Americans rely on international law to maintain their superior position and to prevent other states from engaging in what it perceives to be disruptive activities. To the USA, the promotion of cyber-norms is a way to create predictability and to deter hostile cyber-acts [18]. From the beginning, the USA has consistently sought to resist the creation of new legal constraints – such as those proposed by the Chinese and the Russians – that would limit American cyber capabilities. Thus, it has (so far) managed to steer away from any serious talks about adopting new treaties or new standards for regulating cyberspace. As noted previously, the American position is that cyberspace should be regulated by the existing legal principles. This was reflected in the US reaction to the failure of the fifth UN GGE to agree on another consensus report, where, after the negotiations, the American representative reiterated the US view that the task of the GGE was not to discuss "if" international law applies to the use of ICTs', but merely "how" [19]. This is also the position of the UK [20].

The USA has also been very active in seeking to counter industrial espionage and the theft of intellectual property. For example, while the Russians as noted earlier introduced their resolutions on ICT in the GA's First Committee on Disarmament and International Security, the Americans instead introduces its resolutions in the Second Committee on Economic and Financial issues and the Third Committee on Social, Cultural and Humanitarian affairs. The USA has also worked tirelessly to persuade China to accept a norm

3 For a provocative view, see Rid, T. *Cyber War Will Not Take Place*. New York.: Oxford University Press, 2014; A classic example of a fairly alarmist view is offered in Clarke, R, Knake, R.K. *Cyber War: The Next Threat to National Security and What To Do About It*. New York: HarperCollins Publishers, 2010.

4 It should be noted that the lack of disagreement may also reflect a split between developed and developing states over the issue of some sort of technology transfer and assistance with regard to building cyber capabilities, see Nye (n 21), p. 7–8.

5 For an overview of states' approaches, see Global Commission on the Stability of Cyber Space (GCSC), *Briefings from the Research Advisory Group*, New Delhi, India, November 2017. https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf (11 September 2018, date last accessed).

prohibiting economic espionage and in September 2015 the American efforts paid off when President Obama signed an agreement on commercial espionage with Chinese president Jinping [21]. In addition, the US government has brought criminal indictments against Chinese nationals suspected of engaging in cyber espionage activities deemed harmful to the USA.

The strategic dimension of the legal debate is reflected in the reluctance by some states to publicly state their positions on the regulation of cyberspace. Some states appear to believe that it is not – at present at least – in their strategic interests to be very active participants in the creation of a very detailed regulation of ICT. This could either be because they want to see where the technology is going before they form their legal opinions or – more cynically – because they think it is in their interest to stall progress and maintain the existing legal uncertainties. After all, legal ambiguity may allow for more flexibility. There would, for example, appear to be an element of this form of "fence sitting" to the Chinese approach to the regulation of cyberspace.

In reaction to the June 2017 UN GGE disappointment, the American representative noted that the US had come to the "unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles believe their states are free to act in or through cyberspace to achieve their political ends with no limit on their actions" and that this is "a dangerous and unsupportable view" [19]. Although the US representative did not name states like China and Russia, the insinuation was quite clear. Frustration with what appears to be intentional obstruction by at least certain states was also noticeable in remarks delivered in the First Committee's discussions of the lack of a fifth UN GGE consensus report in October 2017 by the German Representative [22].

In practice, of course, the strategic approaches adopted by states to the discussion of how cyberspace is or ought to be regulated under international law coincide with their respective ICT strengths and weaknesses. This is not surprising, and Professor Matthew Waxman has illustrated how, for example, less powerful states always try to use norms and legal interpretations to try to "level the playing field" [23]. We should therefore only expect that states with powerful offensive cyber capabilities and correspondingly low vulnerabilities to cyberattacks will try to push for a regulation that differs from what will be advanced by states with comparatively limited capabilities and high vulnerabilities. In addition, as noted above, since Western states, like the USA, are particularly vulnerable to industrial espionage they have been very active in pushing for legal bans on such forms of activities.

The regulation of cyberspace and ideological differences about internet openness

Some of the obstacles to reaching common ground on how to regulate ICT stems from fundamentally different ideological attitudes towards Internet openness and fundamental freedoms. Simply put, states disagree about whether the free flow of information in cyberspace is primarily a "good" that is worth protecting or if it is mainly a threat that must be curbed. In the West, of course, cyberspace is considered an important tool for spreading – and at times even securing – human rights, such as the freedom of expression. To Western states, the debate about how to regulate ICT concerns "cyber security" and identifying the right way to include participation from the many different actors who has a stake in the peaceful use of cyberspace. In other parts of the world, however, notions of Internet freedom is greeted with much less enthusiasm. In places like Russia, China and in many states in the Middle East, an open cyberspace is (rightly) considered a threat to existing governing structures [17]. Here, the debate is not framed as one about "cyber security" but instead about "information security" centered around state sovereignty. As Christopher A. Ford has noted, one simply cannot divorce Russia and China's proposals to ban or regulate cyber weapons from their desire to maintain domestic political control over information. The fears harbored by these states about cyberattacks are inseparable from their deeper concern about political subversions that may be associated with the free flow of information [17]. In China, the concern about freedom of information has led to the creation of the so-called "Great Firewall of China", which essentially seeks to cut off the Chinese part of the Internet from the rest of the system.

The ideological differences were on clear display at the International Telecommunications Union's (ITU) World Conference on International Telecommunications (WCIT) in Dubai (UAE) in 2012. Here, many Western states refused to sign treaty amendments to the 1988 International Telecommunications Regulations due to concerns that the new provisions would give governments to great a role in governing cyberspace [24]. Some of the "government friendly states" push their ideological views through the so-called Shanghai Cooperation Organization (SCO) that is composed of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan. In September 2011, the SCO submitted an International Code of Conduct for Information Security to the UN Secretary-General. Among the noticeable elements of the Code is the statement that states refrain from using information and communication networks "to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability". The Code also stresses how states must ensure that other states cannot exploit a dominant position within ICT "to undermine States' right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security". The Code refers to the right to "seek, receive and impart information" but it also states how it may be necessary to make "certain restrictions" in order to ensure "respect of the rights or reputations of others" and for "the protection of national security or of public order (*ordre public*), or of public health or morals" (SCO Code of Conduct, 2011).[6]

It should be noted that states do not always fit neatly into the different categories of having either "strong" or "weak" cyber-capabilities or of being either "pro-Internet freedom" or "anti-Internet freedom". Often, a state has multiple "identities" [1]. For instance, on the surface at least, the Snowden revelations illustrate that ideological disagreements about privacy and state surveillance may arise within a group of otherwise ideologically likeminded states. NSA's activities reminded less powerful liberal states that their ideological interests in the future governance of cyberspace may not always coincide with those of the USA. In addition, it also bears noting that different institutional priorities within the states may complicate their ability to adopt and pursue a single strategic priority.

6 An updated Code of Conduct was submitted to the Secretary-General in January 2015, see *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*, se A/69/723.

What now?

Future efforts to agree on how to regulate cyberspace

When seen in a historical perspective, the difficulties by states to reach broad international agreement on how international law applies to ICT are not particularly extraordinary. After all, it usually takes substantial time and effort for states to reach common ground on how to approach and regulate novel technologies and emerging means of coercion. This is particularly the case for technologies with features that challenge existing categories. It is nevertheless tempting to conclude that the stalemate in the inter-state discussions about how to govern cyberspace is yet another illustration of how difficult it has become for the major states to cooperate and agree on legally binding regulation of issues of major importance to an ever more interconnected and globalized international society. The rise of more powerful and assertive states like China, and the comparatively diminishing influence and power of the West, has, after all, led to an increase in interstate competition and more pronounced rivalry between the most powerful states about who gets to dictate international affairs and what the legal norms should be. At present, in what the UN Secretary-General recently characterized as a "deteriorating international security environment" where the system is becoming more multipolar [25], states are loosing the appetite for embarking on highly ambitious efforts to create legally binding global agreements on important contemporary issues. Instead, they opt for either less ambitious nonbinding global political agreements or legally binding regional agreement with like-minded states. It is tempting to strike a parallel between the lack of agreement about how to govern cyberspace and the developments in international trade law where little progress has been made since the ninth (and so far last) round of WTO negotiations was initiated in Doha back in 2001. In their trade relations, states seem to have largely given up on ambitious global deals and instead seek out regional partners.

Regardless of whether the disagreements among the experts in the fifth UN GGE reflects a larger pattern or not, it seems likely that the June 2017 disappointment has put a halt to serious global efforts to find common ground among all the major powers on how, exactly, ICT should be regulated – at least for the foreseeable future. At present, states like the USA and China are so powerful in cyberspace they act as "gatekeepers", essentially deciding when meaningful international agreement will emerge [1]. Thus, reaching meaningful international agreement on ICT governance requires participation from both states and their different strategic ambitions and worldviews means that we are unlikely to see a uniform legal regime for cyberspace emerge anytime soon.

This, however, does not mean that individual states will just abandon their roles as "norm entrepreneurs" and stop pushing their respective views on how ICT should be regulated. Rather, states will pursue their normative agendas through other processes, before other fora and by other means.

In a recent process-oriented analysis of cyber-norms, Martha Finnemore and Duncan Hollis illustrate how the creation of such norms – whether legally binding or not – is a complex task that depends on a range of choices about not just the content of the desired norm but also about the target of the norm and the process by which the norm will be created [1]. Thus, the debate about the future governance of cyberspace concerns not just what the regulation should look like but also who gets to set the norms and how these norms will be set.

The attempt to predict what the future has in store *vis-à-vis* the regulation of cyberspace after the collapse of the UN GGE process can be broken down into distinct expectations about, respectively, what the main processes and institutions will be, who the primary protagonists may be, and, finally, what the content of the future regulation will look like.

Processes and the turn toward regionalization

As noted previously, cyber governance appears to remain a fragmented area of international law for the foreseeable future. The lack of progress before the UN GGE is likely to lead to an increasing focus on "regional" initiatives with "like-minded" states. In response to the June 2017 failure at the UN GGE, an adviser for US Homeland Security stated that it was now "time to consider other approaches" and that the USA will "also work with smaller groups of likeminded partners" and "pursue bilateral agreements when needed". So while "not abandoning our multilateral efforts, the United States will move forward internationally in meaningful bilateral efforts" [26]. As already noted, a range of regional fora already exists. China and Russia has created the Shanghai Cooperation Organization, which submitted a Code of Conduct for Information Security to the UN process. In Europe, in 2014 the Council of Europe adopted the Cyber Crime Convention. In 2016, members of the Organization for Security and Cooperation in Europe (OSCE) established a series of voluntary confidence-building measures (CBMs) to improve cyber stability, including a mechanism for sharing national cyber strategies and other forms of information [27]. The EU may also begin to more actively seek to fulfill its strategic ambition of promoting a "rules-based global order" (European Union Global Strategy) by taking up a more visible role in relation to the creation of acceptable cyber-norms. The EU already plays an important role within privacy and data protection and in September 2017, the EU Commission announced a "cybersecurity package", including a "Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU". On a more practical day-to-day level, of course, there is already extensive regional cooperation among national Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs).

As a result of the likely turn toward regional fora we are, of course, likely to see more regional agreements. There are obvious downsides to such a trend. The overall regulation of ICT may end up consisting of a range of legal sub-systems of varying normative depth with the result that different regions develop competing "silos" of norms [1]. Given the global nature of the Internet, this is highly unfortunate. A stronger emphasis on regional agreements may also lead states to abandon efforts to reach more complicated but also much-needed universal agreement on the regulation of ICT.

There are, however, also advantages to a more regional approach to cyber regulation. Regional agreements could, for example, be a way of avoiding time-consuming obstruction of negotiations by certain state and therefore in all likelihood be a faster way to "operationalize" certain norms. The expected turn toward regionalization may also enable states to cooperate in those areas where they agree, while remaining in disagreements in others. More selective regional approaches may also enable states to reach agreement on not just the "low-hanging fruits" but potentially also the more complex issues that stand in the way of reaching global agreement. Thus, we could see a shift away from very broad and "shallow" global instrument that have to accommodate the interests of all states toward more narrow but also "deeper" instruments, which merely have to take account of the interests of fewer states. Increasing regional cooperation could also force some states, in particular smaller states, to consider who their allies actually are in the debate about the

regulation of cyberspace: what states are "like-minded"? As already noted, when it comes to strategy, capabilities and ideological preferences, states often have multiple identities.

Two other "process-trends" are likely to flow from the collapse of the UN GGE process. First, we may well see more "bilateral agreements" on ICT, such as the 2015 agreement on commercial espionage between the USA and China. As already noted, the American efforts to limit Chinese industrial espionage paid of in September 2015 when then-President Obama signed an agreement with Chinese President Xi. Under the agreement, neither states' "government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors" [21].

Secondly, we should expect that states begin to try to influence the discussion about the regulation of cyberspace by unilaterally stating their legal views and interpretations in official documents such as national cyber strategies. Over time, such pronouncements could also help develop international law by consolidating emerging *opinio juris*. In March 2018, for example, the British Attorney General sought to lay out the UK's position on applying international law to cyberspace [20].

The increasing role of nonstate actors

The processes listed above all have states as the primary protagonists. However, as states struggle to reach common ground, it is likely that various nonstate actors will begin to take on a greater role in the efforts to bring legal clarity to the regulation of ICT. While it is true that only states can create legally binding instruments under international law, nonstate actors can play an important role in the law-making process [28]. One of the ways nonstate actors can play a bigger role is by engaging states. Thus, we may well see new collaborative initiatives between states and think tanks and research institutions. A prime example was the so-called "Hague Process", where more than 50 states submitted their observations to a draft version of the second edition of the Tallinn Manual that was published in 2017. Another example is the "Global Conference on Cyber Space" (GCCS), an annual Internet policy event where state representatives meet up with other actors to engage in discussion about various issues, including norms for responsible behavior in cyberspace. The GCCS was initiated to establish internationally agreed "rules of the road" for behavior in cyberspace and to create a more focused and inclusive dialogue between all those with a stake in the Internet. In recent years, we have seen the emergence of a range of different high-level academic fora that serve as suitable "vehicles" for the debate about cyber regulation. The "Global Commission for the Stability of Cyberspace" (GCSC), for example, was initiated by the Dutch Government in collaboration with The Hague Center for Strategic Studies and the East-West Institute to develop proposals for norms and policies to enhance international security and stability and guide responsible state and nonstate behavior in cyberspace.[7]

The "tech industry" may also now decide that it should take on more responsibility for creating an international legal framework for ICT or at least help establish clear expectations of what is acceptable state behavior. Certain steps have already been taken. In December 2014, Microsoft published a paper with six "initial cybersecurity norms" on how states could try to limit conflict in cyberspace [29]. In July 2016, the tech giant issued a follow-up paper on how the suggested norms should be implemented [30]. Unlike the 2014 paper, it addressed not only state behavior but also that of the industry itself. In February 2017, Microsoft proposed a much-discussed "Digital Geneva Convention" to protect cyberspace. The purpose of this "Convention" is to "commit" states to protect "civilians from nation-state attacks in times of peace". When presenting its proposal, Microsoft drew parallels to the ICRC's active involvement in the Geneva Conventions and stated how "protection against nation-state cyberattacks requires the active assistance of technology companies". Since the industry "play's a unique role as the internet's first responders", it should commit to "collective action that will make the internet a safer place" [31]. Here, reference should also be made to the Cybersecurity Tech Accords that is a public 2017 commitment by 40 global tech companies to improve the security, stability and resilience of cyberspace. In the Accords, the companies not only promise to strive to protect all users from cyberattacks and to design, develop and deliver products and services that prioritizes security, privacy, integrity and reliability, but also to support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.

Finally, there is the "academic literature", where the discussions about how international law applies to activities in cyberspace are likely to proceed at full throttle. There is already a booming literature on "cyber-law" and one would expect the many scholarly contributions to have some sort of effect on the future regulation of ICT. The best examples may well be the two Tallinn Manuals on international law applicable to cyber-operations publshed in 2013 and 2017 respectively.

The content of the regulation

Finally, there is the all-important question of the content of the desired norms. What should we expect that prescribed behavior in cyberspace will be? What will states be allowed to do with ICT and what will they not be allowed to do? Here, two points should be made. The first is that, as time passes, states are likely to become increasingly comfortable with stating their legal positions about how cyberspace is – or should be – governed. Most ICTs are fairly novel inventions and there is still a substantial amount of uncertainty about the exact nature of the threats in cyberspace. There is also still fairly little relevant jurisprudence from courts, whether national or international. But as more harmful cyber incidents take place, more information about the new technologies becomes available and courts begin to render decisions, states will find it easier to make the required legal interpretations. In other words, in the coming years, in part aided by courts, we should generally expect that more states become sufficiently comfortable about the new technologies that they will come down from the fence and state their legal positions.

7 See also East-West Institute, Promoting International Cyber Norms: A New Advocacy Forum, A report from the EastWest Institute Breakthrough Group on Promoting Measures of Restraint in Cyber Armaments, December 2015. https://www.eastwest.ngo/idea/slowing-cyber-arms-race (20 November 2018, date last accessed). In 2014, the two-year Global Commission on Internet Governance (GCIG) was initiated by the Centre for International Governance Innovation and Chatham House to make recommendations on the future governance of the internet, see the overview on https://www.cigionline.org/initiatives/global-commission-internet-governance (20 November 2018, date last accessed). The final report of the GCIG was published in June 2016, see One Internet, 21 June 2016. https://www.cigionline.org/publications/one-internet (20 November 2018, date last accessed).

The second point is that, while it may still be too early to predict how all aspects of ICT will be regulated, the conversation should begin from the premise that various norms of different character already exists in cyberspace. As Finnemore and Hollis [1] notes, cyberspace is not a "blank slate". For one thing, as we saw in Section 2, despite its inability to continue the interstate conversation and the differences about the applicability of international humanitarian law, the UN GGE process "did" manage to provide some of the broader answers. Thus, in the third and fourth experts reports the most important states did go on the official record and stated the following: (i) that states have jurisdiction over the ICT infrastructure that is located within their territory; (ii) that the UN Charter applies in its entirety; (iii) that the principles of sovereign equality and peaceful settlement of international disputes as well as the prohibition of the use of force, and nonintervention are of central importance; (iii) that states must respect human rights and fundamental freedoms in cyberspace; (iv) that the same rights that people have offline are protected online; (v) that states must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts; and (vi) that states must meet their international obligations regarding internationally wrongful acts attributable to them under international law. So, although the concrete task of "translating" these core principles into concrete rules for ICT remains fraught with contention, the already established principles provide a solid point of departure. This was also emphasized by the Secretary-General in his recent May 2018 "Agenda for Disarmament" where it was noted that the UN GGE process made overall progress on, among other things, "norms, rules and principles of responsible behaviour of States" and that states should implement what was already agreed upon [25].

Finally, of course, there are the many other legal instruments, technical protocols and best practices that abound in and around cyberspace. All these instruments also form a basis upon which states can continue their discussions of how international law should govern cyberspace.

Conclusion

To understand why the UN GGE process reached a dead-end in June 2017, one must consider the discussions among the governmental experts in a wider strategic and ideological context. The debate about how cyberspace should be regulated is highly politicized and states are actively pushing norms and legal interpretations that coincide with their strategic and ideological preferences. For time being, such preferences simply cannot be reconciled. The collapse of the UN GGE is therefore also a clear indication that we are unlikely to witness the emergence of a single legal regime for the regulation of ICT in the foreseeable future. In fact, the June 2017 disappointment will probably only accelerate the creation of a more regionalized and fragmented regulation of cyberspace. States' ICT activities will therefore continue to be governed by a host of different instruments, some legally binding and some not. But the stalemate at the UN does not spell the end of states' efforts to bring more legal clarity to the field; it just means they will turn their attention to other fora and processes. A host of nonstate actors are now likely to begin to assume a greater role in the continuing debate about law and cyberspace. While the UN GGE process did not deliver much more than the most basic of legal finding, it is upon these findings the debate about the future regulation of ICT should – and will – proceed.

References

1. Finnemore M, Hollis B. Constructing norms for global cybersecurity. *Am J Int L* 2016;**110**:425–79.
2. Finnemore M, Sikkink K. International norm dynamics and political change'. Int *Organ* 1998;**52**:887–917.
3. Henriksen A. Politics and the development of legal norms in cyberspace. In: Friis K, Ringsmose J (eds), *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. Routledge, 2016, 151–64.
4. Ku J. How China's views on the law of jus ad bellum will shape its legal approach to cyberwarfare, 2017. Aegis Series Paper, 1707. https://www.hoover.org/research/how-chinas-views-law-jus-ad-bellum-will-shape-its-legal-approach-cyberwarfare (24 November 2018, date last accessed).
5. Schmitt, MN (ed.). *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013.
6. Rodriguez M. Declaration by, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, New York, June 23, 2017.
7. Schmitt M, Vihul L. International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, 2017. https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ (24 November 2018, date last accessed).
8. G20 Communiqué Antalya Summit, 15–16 November 2015. https://www.consilium.europa.eu/en/press/press-releases/2015/11/16/g20-summit-antalya-communique/ (24 November 2018, date last accessed).
9. G7 Declaration on Responsible States Behavior in Cyberspace, Lucca, 11 April 2017. https://www.mofa.go.jp/files/000246367.pdf (24 November 2018, date last accesssed).
10. Schmitt, MN (ed). *The Tallinn Manual on the International Law Applicable to Cyber Operations*. New York: Cambridge University Press, 2017.
11. Xinmin M. Key issues and future development of international cyberspace law. *CQISS* 2016;**2**:119–33.
12. Macak K. From cyber norms to cyber rules: re-engaging states as law-makers. *Leiden J Int L* (published online 18 July 2017).
13. Lewis J. Fighting the Wrong Enemy: aka the Stalemate in Cybersecurity, *the Cipher Brief*, 2017. https://www.thecipherbrief.com/column/expert-view/fighting-the-wrong-enemy-aka-the-stalemate-in-cybersecurity (24 November 2018, date last accessed).
14. ICRC, Weapons: Statement of the ICRC to the United Nations, 2017. https://www.icrc.org/en/document/weapons-statement-icrc-united-nations-unag-2017 (24 November 2018, date last accessed).
15. Burns WJ, Cohen J. The rules of the brave new cyberworld. *Foreign Policy* 2017. http://foreignpolicy.com/2017/02/16/the-rules-of-the-brave-new-cyberworld/ 24 November 2018; date last accessed).
16. Komov S, Korotkov S, Dylewski I. Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law. *Disarmament Forum* 2007;**3**:35–43.
17. Ford CA. The trouble with cyber arms control. *The New Atlantis* 2010; Fall: 52–67.
18. Lotrionte C. A better defense: examining the united states' new norms-based approach to cyber deterrence. *Georgetown J Int Affairs* 2013;**14**: 75–88.
19. US Explanation of Position, United States Mission to the United Nations, 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, June 23, 2017.
20. UK Attorney General, Speech: Cyber and International Law in the 21st Century (23 May 2018). https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (24 November 2018, date last accessed).
21. Fact Sheet, President Xi Jinping's State Visit to the United States, 25 September 2015. https://obamawhitehouse.archives.gov/the-press-office/

2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (24 November 2018, date last accessed).

22. Fitschen T. Statement by Ambassador Dr Thomas Fitschen, Director for the United Nations, Cyber Foreign Policy and Counter-Terrorism, Federal Foreign Office of Germany. http://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com17/statements/23Oct_Germany.pdf (24 November 2018, date last accessed).
23. Waxman MC. Cyber-attacks and the use of force: back to the future of article 2(4). *Yale J Int L* 2011;**36**:421–59.
24. Center for Democracy and Technology, Consensus Crumbles as Nations Split on Internet Governance, 2012. https://cdt.org/press/consensus-crumbles-as-nations-split-on-internet-governance/ (24 November 2018, date last accessed).
25. UNSG, Securing Our Common Future: An Agenda for Disarmament, 24 May 2018, p. 3–4. https://www.un.org/disarmament/publications/more/securing-our-common-future/ (24 November 2018, date last accessed).
26. Bossert T. Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week, 2017. https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/ (24 November 2018, date last accessed).
27. OECD, Decision No. 1202 OSCE Confidence-Building Measures to reduce the Risks of Conflict Stemming from the use of Information and Communication Technologies, 10 March 2016. https://www.osce.org/pc/227281? download=true (24 November 2018, date last accessed).
28. Boyle A, Chinkin C. *The Making of International Law*. New York: Oxford University Press, 2017.
29. Microsoft, International Cybersecurity Norms: Reducing conflict in an Internet-dependent world. December 2014. https://www.microsoft.com/en-us/cybersecurity/content-hub/reducing-conflict-in-Internet-dependent-world (24 November 2018, date last accessed).
30. Microsoft, From Articulation to Implementation: Enabling progress on cybersecurity norms, June 2016. https://www.microsoft.com/en-us/cybersecurity/content-hub/enabling-progress-on-cybersecurity-norms (24 November 2018, date last accessed).
31. Smith B. The need for a Digital Geneva Convention, 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ (24 November 2018, date last accessed)