Chapter 18
Norms of Responsible State Behaviour in Cyberspace

Paul Meyer

Abstract Cyberspace has witnessed a 'militarisation' as a growing number of states engage in a variety of cyber operations directed against foreign entities. The rate of this militarisation has outstripped the diplomatic efforts undertaken to provide this unique environment with some 'rules of the road'. The primary mechanism for discussing possible norms of responsible state behaviour has been a series of UN Groups of Governmental Experts, which have produced three consensus reports over the last decade. The 2015 report recommended a series of principles and confidence-building measures to prevent conf1lict, but prospects for its implementation have receded as differences amongst states persist over how security concepts should be applied to cyberspace. Renewed efforts to promote responsible state behaviour will require greater engagement on the part of the private sector and civil society, both of which have a huge stake in sustaining cyber peace.

Keywords Confidence-building measures · Cyber conflict · Norms of responsible state behaviour · OSCE · United Nations

18.1 Introduction

18.1.1 Cyberspace: A Realm of Peace or War?

Cyberspace as a term was coined by William Gibson, a Vancouver-based writer of speculative fiction whose 1984 novel *Neuromancer* described it as "a consensual hallucination experienced daily by billions". Today, with over three billion users of the Internet, Gibson's projection has proven prescient, but few among current users would realise that this unique space has experienced, alongside exponential growth, a marked 'militarisation' in recent years. States, with their monopoly on organised

P. Meyer (✉)
Simon Fraser University, The Simons Foundation Canada, ICT4Peace, Vancouver, Canada
e-mail: pmeyer@sfu.ca

M. Christen et al. (eds.), *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology 21,
https://doi.org/10.1007/978-3-030-29053-5_18

armed force, have energetically turned their attention to cyberspace, declaring this environment to be a domain for 'war-fighting' and investing heavily in the development of capabilities for offensive as well as defensive cyber capabilities. According to the US Director of National Intelligence, over 30 states currently possess cyber-attack capabilities, and such attacks now figure prominently in the intelligence community's ranking of global threats faced by the United States. (Coats 2018). In this chapter, the gradual efforts of the international community to define an order for cyberspace are examined, and in particular the ongoing effort to develop norms of responsible state behaviour in this new and unique environment. After surveying the contributions of the chief national and multilateral actors and inputs from other cyber stakeholders, the chapter concludes with some ideas for bringing this complex international discussion of norms to a practical outcome.

While states have long engaged in electronic intelligence-gathering, the emergence of cyberspace as a perceived domain for inter-state warfare with the attendant establishment of specialised units within militaries to conduct it is relatively recent (see also Chap. 12). It was only 2009 when the US created a dedicated Cyber Command, but as this element has enjoyed a rapidly increasing share of the defence budget ever since, America has set the global pace for military engagement in cyberspace. Many militaries now boast cybersecurity units and increasingly acknowledge that their capabilities extend beyond purely the defence of national systems to include offensive cyber action. This 'militarisation' process has proceeded with little political or public debate and is now frequently depicted as an inevitable development.

Significantly, however the US military, in acknowledging a 'diplomatic risk' of being seen as 'militarising' cyberspace, asserts that this environment represents "a domain already militarised by our adversaries". Given that the United States is widely perceived as the author of the 'Stuxnet' cyber weapon directed against Iran—the first cyber payload providing for actual physical destruction—the allegation that others were to blame for the 'weaponisation' of cyberspace rings rather hollow. This assertion from Cyber Command suggests, however, a certain sensitivity as to how its overt pursuit of military "superiority in cyberspace" will be perceived by other users, both governmental and non-governmental (Cyber Command 2018: 10).

States have struggled with incorporating the new, potent technology represented by cyberspace and its most salient embodiment, the Internet, into existing frameworks of international affairs. Part of the reason for this lies in the initial use of cyber capabilities by the intelligence community. As this covert activity was shrouded in secrecy and entailed accessing information from foreign targets without alerting them to this fact (the so-called Computer Network Exploitation) there was little incentive for states to acknowledge these actions, let alone discuss reciprocal limits on them. Espionage has eluded any effort at more than tacit agreement amongst states. In contrast, states have long cooperated in the field of international security and have negotiated agreements to regulate military activity and control armaments.

To the degree that intrusive cyber operations emerged from the shadows of the intelligence sphere into the somewhat more transparent field of military establishments and capabilities, it became more feasible to treat such activity as a potential realm for international agreement.

In the event, it was a Russian-led initiative at the UN in 1998 to adopt a resolution on "Developments in the field of information and telecommunications in the context of international security" (UNGA 1999) that first brought the issue of "information security" before a diplomatic forum. This resolution, introduced in the First Committee of the General Assembly (the committee responsible for issues of disarmament and international security), raised the threat that these new technologies could be employed in ways that could "adversely affect the security of states".

18.1.2 The GGE Process: Early Failure and Initial Success

The Russian-initiated focus on this potential risk to international security was widely supported and led, 4 years later, to the authorisation of a UN Group of Governmental Experts (GGE) "to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them…" (UNGA 2002).

This GGE met in the 2004–05 period but was unable to agree on a consensus report (as required by UN procedures for such GGEs). The chief issues that reportedly divided the group were how to characterise the threat represented by state exploitation of information and communication technology (ICT) for military purposes; and whether the concept of security should be limited to the ICT infrastructure itself or be extended to include the content of the information conveyed. In particular, there was a dispute over whether information that was the subject of trans-border transmission should be controlled as a matter of national security (UNIDIR 2016: 6).

This initial failure to agree did not impede efforts at the UN to pursue consideration of the issues contained in the information security- international security nexus. A second GGE was convened in the 2009–2010 timeframe and on this occasion, the 15 experts were successful in producing a consensus report. The report affirmed that "Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century". It went on to enumerate a series of malicious and disruptive ICT-enabled activity including the fact that "States are developing ICTs as instruments of warfare and intelligence, and for political purposes." In response to these developments, the report recommended that states pursue cooperative measures. Specifically, the GGE recommended that states should "discuss norms pertaining to state use of ICTs, to reduce collective risk and protect critical national and international infrastructure" and consider "Confidence-building, stability and risk reduction measures to address the implications of state use of ICTs" (UNGA 2011: 8).

18.2 National Strategies for Cyberspace

18.2.1 The US Strategy for Cyberspace

The 2010 GGE report introduced the concept of norms for state conduct into the diplomatic discourse that hitherto had focused on state responses to malicious activity by non-state actors. The report also drew upon the past diplomatic tool box of arms control in advocating confidence-building and risk reduction measures. The United States was the first leading power to pick up on these suggestions in its *International Strategy for Cyberspace* issued by the Obama administration in May 2011. This policy document recognised the dangers that unchecked state cyber action could represent: "Cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace" (White House 2011: 4). This application of traditional national power in cyberspace was occurring in the absence of "clearly agreed-upon norms for acceptable state behaviour in cyberspace" (White House 2011: 9). To rectify this situation, the *Strategy* affirmed: "We will engage the international community in frank and urgent dialogue, to build consensus around principles of responsible behaviour in cyberspace" (White House 2011: 11).

The initiation of this urgent dialogue, however, proved elusive and the Obama administration experienced difficulty in translating its clear interest in developing "norms of responsible behaviour" into an actual diplomatic process to achieve this end. Initial follow-up action seemed to have been delegated to the United Kingdom, where then Foreign Secretary William Hague hosted an international cyberspace conference in London in November 2011. Secretary Hague characterised the conference as an opportunity to discuss norms of acceptable behaviour in cyberspace and to explore mechanisms for giving such standards "real political and diplomatic weight" (Hague 2011). In his chairman's summation of the conference discussions, he indicated: "All delegates agreed that the immediate next steps must be to take practical measures to develop shared understanding and agree common approaches and confidence-building measures. There was no appetite at this stage to expend effort on new legally-binding international instruments" (Hague 2011).

While Secretary Hague's conclusions may have reflected British preferences to a degree, there did appear a broad consensus that the "common approaches" for governing state behaviour in cyberspace should take the form of politically as opposed to legally binding measures. Early in the UN's polling of national views, influential states such as the US and the UK argued that in the realm of cyber conflict, legally binding agreements were superfluous as the laws of armed conflict would apply (Tikk and Kerttunen 2017: 20). Whether it was the time-intensive character of negotiating international legal instruments, the absence of adequate verification means or the risk of such efforts being rendered obsolete by a rapidly developing technology, states in general seemed more comfortable with the idea of political versus legal arrangements in this new environment.

18.2.2 Sino-Russian Code of Conduct

This approach was reinforced when Russia and China (alongside Tajikistan and Uzbekistan) submitted to the UN General Assembly in September 2011 a proposal for an *International Code of Conduct for Information Security.* Although these states generally advocated legally binding agreements in the realm of international security, in this case the sponsors decided to utilise the less demanding and more palatable form of politically binding measures represented by the *Code of Conduct.* At the same time, the conflict prevention dimension of the proposal was stressed by the sponsors. In his introduction of the proposal, the Chinese Ambassador Wang Qun stated that "countries should work to keep information and cyberspace from becoming a new battlefield, prevent an arms race in information and cyberspace and settle disputes on this front peacefully through dialogue" (Qun 2011).

The co-sponsors of the *Code* characterised it, therefore, as a collection of voluntary measures designed to maintain international stability and security. The chief undertaking would be a commitment by states "not to use Information and Communication Technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies" (Code 2011). This external security aspect was associated with other measures with far more of an internal security focus. The *Code* affirmed the rights of states "to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage". How such hostile actions would be defined could prove problematic, as what one state might view as a "disturbance", another might consider a simple exercise of freedom of expression. From a classic arms control perspective, the definitional challenges inherent in determining what constituted an "information weapon" or an "act of aggression" in cyberspace were also significant obstacles. At the same time, the Sino-Russian *Code* represented the first major diplomatic effort to provide a set of "norms of responsible state behaviour" as called for in the 2010 GGE report and the US 2011 *Strategy*.

In the event, China and Russia chose to proceed cautiously with their initiative, engaging over the next few years in consultations on the margins of UN General Assembly sessions but not seeking to bring the *Code* forward for adoption by that body. A revised *Code* was circulated by the co-sponsors in January 2015 that essentially eliminated the previous "arms control" aspect but retained the bulk of the measures directed at prohibiting cyber interference "in the internal affairs of other States or with the aim of undermining their political, economic and social stability" (Code 2015). The internal control orientation of the *Code* was further evident in its affirmation of the sovereign rights of states to protect "their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage". The Sino-Russian *Code of Conduct for Information Security* reflected, in its use of the term 'information security' over the prevalent terminology of 'cybersecurity', a fundamental conceptual difference with the West. Whereas 'cybersecurity' was seen as focusing on the integrity of the computer

systems comprising cyberspace, "information security" implied that the content of information transmitted should also be viewed through a security prism. This conceptual distinction continues to colour the preferred approaches of leading cyber powers in pursuing common norms of responsible state behaviour.

18.3 International Developments

18.3.1 GGE 2013

In parallel to these unilateral or plurilateral forays into suggesting norms to govern state conduct in cyberspace, the UN GGE process continued to act as a locus for multilateral cybersecurity diplomacy. A successful GGE report in 2013 contributed to the framing of the problem by flagging the increasingly sophisticated nature of malicious cyber activity and stressing "[T]the absence of common understandings on acceptable State behaviour with regard to the use of ICTs increases the risk to international peace and security" (GGE 2013: 7). The report established the principle that international law is applicable to cyberspace without attempting to delineate how it did so. In a counterbalancing finding, it also affirmed the applicability of the sovereignty principle to state cyber conduct and state jurisdiction over ICT infrastructure within its territory. The report stated that "States must not use proxies to commit internationally wrongful acts" (GGE 2013: 8) and indicated that states had the responsibility to ensure that non-state actors did not engage in such unlawful use of ICTs on their territory. The GGE reiterated the earlier call for states to consider "the development of practical confidence -building measures to help increase transparency, predictability and cooperation" and suggested a series of basic consultative and information-exchange measures towards this end (GGE 2013: 9).

18.3.2 GGE 2015

The UN-centric GGE process reached a culmination of sorts with the successful conclusion of an enlarged (20 experts) GGE in the summer of 2015. This GGE, explicitly building on its two predecessors, stated that "Voluntary, non-binding norms of responsible state behaviour can reduce risks to international peace, security and stability" while observing that "norms do not seek to limit or prohibit action that is otherwise consistent with international law" (GGE 2015: 7). The report provided the fullest elaboration to date of the "norms, rules and principles for the responsible behaviour of states" and the "confidence building measures" that formed the chief headings of the GGE reports. Importantly on the normative side, the report recommended that "A state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical

infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public" (GGE 2015: 8).

A further major restraint measure was set out to the effect that "States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another state. A state should not use authorised emergency response teams to engage in malicious international activity" (GGE 2015: 8).

In these two restraint measures, there is a clear connection with pre-existing obligations under international humanitarian law not to target civilians or crucial infrastructure for the public. It also mirrors recognition of a certain "protective status" for the computer emergency response teams akin to that accorded to medical personnel and facilities under international humanitarian law.

In addition to these restraint measures, the 2015 GGE report also recommended proactive steps such as encouraging states to report "ICT vulnerabilities and share associated information on available remedies to such vulnerabilities" (GGE 2015: 8). Given that this reporting concerns the very vulnerabilities that states have secretly harboured to develop targeted exploits, it would seem doubtful that states will undertake such cooperation anytime soon. After its enumeration of proposed measures, the report acknowledged that "while such measures may be essential to promote an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible" (GGE 2015: 8). The 2015 GGE may have elaborated the most practical set of measures to date, but its experts were aware that their proposals remained only recommendations, the implementation of which would depend on state capacity or willingness to adopt them.

Some of the underlying problems of the GGE process in generating recommended measures that states would actually embrace were made manifest in the subsequent GGE (at 25 experts, the largest yet) which operated in the 2016–17 timeframe yet failed to achieve a consensus report. Whereas there was considerable speculation as to the reasons for the failure of the latest GGE, it seems likely that it reflected basic disagreement among leading cyber powers as to the relationship between inter-state cyber conflict and the laws of armed conflict. In brief, whereas states such as the US and UK wanted to elaborate on the rules around cyber operations in the context of the laws of armed conflict others, namely Russia and China, balked at this direction. As one observer remarked: "Russian and Chinese diplomats wanted to concentrate their efforts on preventing cyber-based conflict in the first place, instead of setting the rules for something that should not be allowed to happen" (Grigsby 2017: 114). This fundamental divergence over the appropriateness of state-conducted cyber operations helps explain why defining responsible state behaviour has proven so difficult. As another analyst of the GGE concluded, "Authoritative guidance for responsible state behaviour in cyberspace remains farfetched, not just because of yawning technical capacity divides and the known difficulties of attribution of state behaviour in cyberspace, but also because the principal questions of the international cybersecurity discourse are far from settled politically" (Tikk and Kerttunen 2017: 5).

18.3.3 Regional Security Organisations and Cyber Confidence-Building Measures

Although the UN and its GGE process has been the primary focus of discussion of norms of responsible state behaviour in cyberspace, it has not been the only inter-governmental forum to have taken up this issue. Notably, the 57-member Organization for Security and Cooperation in Europe (OSCE) has been engaged since 2012 in an effort to develop cybersecurity confidence-building measures to "enhance cooperation, transparency, predictability, and stability to reduce the risks of misperception, escalation and conflict that may stem from the use of ICTs" (OSCE 2012).

In 2013, the OSCE was able to adopt a set of 11 confidence-building measures relating to cybersecurity information sharing and in 2016 it was able to add five additional measures including the protection of critical infrastructure and the establishment of protected channels of communication. It has been noted that the measures adopted by the OSCE are cast in more prescriptive language than the comparable measures identified by the UN GGE. The OSCE has also established an on-going working group for discussion relating to the implementation of the agreed confidence-building measures (Hitchens and Gallagher 2018: 6). Other regional organisations such as the AU, OAS, and ASEAN Regional Forum have considered cybersecurity confidence building measures over the last decade, although none have progressed as far as the OSCE in agreeing on a substantial package of measures. It remains to be seen whether the relative success of the OSCE in addressing the issue of international cybersecurity cooperation will be sustained in a context of deteriorating East-West relations, notably between leading OSCE member states Russia and the US.

18.4 Other Stakeholders

While the inter-governmental discussion of norms of responsible state behaviour proceeds with various degrees of progress, there is increasing engagement in its subject matter by other stakeholders. The private sector, civil society, academia and mere Internet users have legitimate reasons to be concerned with how states will conduct themselves in cyberspace. Beyond the fact that this special, human-created environment is overwhelmingly owned and operated by non-governmental entities, disruptive or destructive state activity in cyberspace could have serious detrimental effects on the interests of 'netizens' and humanity in general.

In recent years, several of these stakeholders have begun to express their views on what would constitute responsible state behaviour in cyberspace in an effort to influence the inter-governmental debate.

18.4.1 International Committee of the Red Cross

Given its role as a custodian of international humanitarian law, it is not surprising that the International Committee of the Red Cross (ICRC) has been monitoring state action in cyberspace and has begun to air its concerns. In its statement to the 2017 session of the UN General Assembly's First Committee, the ICRC drew attention to the upswing in major cyber-attacks including those "affecting the functioning of electricity networks, medical facilities and a nuclear power plant". Such attacks, the statement noted, "are a stark reminder of the vulnerability of essential civilian infrastructure to cyber-attacks and of the significant humanitarian consequences that may ensure". The ICRC affirmed that international humanitarian law "applies to and restricts the use of cyber capabilities as means and methods of warfare during armed conflicts. Crucially, IHL prohibits cyber-attacks against civilian objects or networks, and prohibits indiscriminate and disproportionate cyber-attack" (ICRC 2017: 3).

The ICRC, however, also wanted to make it clear that "by asserting that IHL applies to cyber operations, the ICRC is in no way condoning cyber warfare, nor is it condoning the militarisation of cyberspace. Any resort to force by a State, whether physical or through cyberspace, remains constrained by the UN Charter (*jus ad bellum*)" (ICRC 2017: 3). The ICRC expressed its regret over the failure of the 2016–2017 GGE to adopt a consensus report and called upon all states "to renew discussions in appropriate forums on the critical issues raised by cyberwarfare, with a view to finding common ground on the protection afforded by IHL to civilian use of cyber space" (ICRC 2017: 3).

18.4.2 Civil Society

At the same session of the UN General Assembly's First Committee that heard the position of the ICRC on the threats posed by irresponsible state behaviour in cyberspace, there was also a statement delivered by the *Women's International League for Peace and Freedom* on behalf of several civil society organisations. This statement was especially noteworthy as it went beyond affirming the applicability of international humanitarian law to state cyber operations to challenge the militarisation of cyberspace itself. Expressing its regret over the failure of the latest GGE, the civil society statement suggested that it was "an opportune moment to put forward a few basic questions: how much more militarised are we going to allow cyberspace to become? When and under whose authority did it pass from a civilian domain to the so-called 'fifth domain' of conflict, and how was that allowed to happen?" (WILPF 2017: 1). According to the civil society statement there was still time to "turn back the clock" on militarisation: "States can choose to elaborate methods to preserve cyber peace, rather than resign themselves to formulating the norms of cyber war" (WILPF 2017: 1). This statement argued in effect for a new orientation

for the future discussion of norms, one that would seek to reinforce the peace in cyberspace rather than merely set out the limits to warfare undertaken by states within it.

18.4.3 The Private Sector

A relevant sector that might have been expected to be at the forefront of the discussion of state conduct in cyberspace given its implications for its business model is that of the ICT industry.

The industry has largely been silent on issues of international cybersecurity policy, however, and not particularly engaged with the nascent inter-governmental discussion of norms of responsible state behaviour. An important exception to this general trend of the industry has been the Microsoft Corporation, which has for several years been advocating cooperative approaches and restraint measures for international cybersecurity. Its president, Brad Smith, has been outspoken in voicing alarm about the implications of irresponsible state conduct in cyberspace and the threat posed to civil interests. He has stated: "A cyber arms race is underway with nations developing and unleashing a new generation of weapons aimed at governments and civilians alike, putting at risk the critical data and digital-powered infrastructure that we all depend on for our daily lives" (Smith November 2017).

Smith has not shied away from blaming governments for the damaging consequences for society flowing from their practice of hoarding software vulnerabilities in order to use them on their adversaries via targeted "exploits". In the aftermath of the 'WannaCry' ransomware attacks of early May 2017, Smith wrote "this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem …We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage" (Smith May 2017).

These concerns have led Smith to propose a new international agreement that would set out standards for state cyber operations. In a keynote speech at a major industry conference, he explained "What we need now is a Digital Geneva Convention. We need a convention that will call on the world's governments to pledge that they will not engage in cyberattacks on the private sector, that they will not target civilian infrastructure, whether it's of the electrical or the economic or the political variety" (Smith February 2017). He went on to espouse the need for a neutral entity along the lines of the International Atomic Energy Agency or the ICRC to partner with governments in the development of such an accord. More broadly, he outlined prospects for the ICT industry as a whole to play a role as a "neutral Digital Switzerland on which everyone can depend and rely" (Smith February 2017).

Smith's advocacy on behalf of an international arrangement for responsible state behaviour and the engagement of the private sector in bringing such arrangements about seem to have yielded some further allies in the industry. In April 2018, 34

companies (including major actors such as Facebook, LinkedIn, Dell and Cisco) signed a 'Cybersecurity Tech Accord' which pledged to uphold four principles supportive of cybersecurity. The principles are to: (i) protect all of our users and customers everywhere; (ii) oppose cyberattacks on innocent citizens and enterprises from anywhere; (iii) empower users, customers and developers to strengthen cybersecurity protection and iv) partner with each other and with like-minded groups to enhance cybersecurity (Smith April 2018). Although these general principles are open to question and interpretation (e.g. who decides which citizens and enterprises are "innocent"?) they do represent some common ground on the part of leading firms in the ICT sector in espousing positions relevant to the future development of cyberspace and especially the trend towards its 'militarisation'.

18.5 Prospects and Proposals for Norms of Responsible State Behaviour

The failure of the 2016–2017 iteration of the GGE process has derailed to some degree the momentum that this process had developed in terms of agreed norms for state conduct in cyberspace. For some observers, the pursuit of agreed norms represents a "bridge too far" given the absence of shared ideological principles, and the more modest aim of accepting a few practical confidence-building measures is advocated instead (Grigsby 2017: 116–18). There has also been reference to the "cybersecurity dilemma" that generates fear amongst cyber powers and impedes cooperation, as intrusions into foreign networks are advantageous for both defensive and offensive purposes and thus promote "worse-case scenario" reactions by the intruded party (Buchanen 2016: 188). A general lack of transparency regarding policy and doctrine concerning offensive cyber operations in particular also constitutes an impediment to more cooperative approaches.

At the same time, the recommendations emerging from the GGE process, while falling short of the clear norms and rules of state conduct that some would have liked to see, still constitute an important step in that direction. As noted by one longtime observer: "In this reading, the 2015 GGE provides the international community with a very valuable roadmap to strengthening international cyber security". A roadmap that, for all of its utility in providing direction, leaves much of the distance to be completed as "There is hardly any state, even among those having participated in the OSCE and the GGE discussions, that to date fully implements all the GGE recommendations" (Tikk 2018: 7–8).

The UN Secretary General sees a future role for himself in the prevention and peaceful settlement of cyber conflict as well as in "foster[ing] a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace" (ODA 2018: 56). How exactly these contributions are to be realised is unstated in the Secretary General's *An Agenda for Disarmament*, but the UN is likely to retain a vital convening role for the norms discussions, especially

given the alignment between its universal membership and the universal nature of cyberspace. Member state action will remain crucial, however, in order to achieve progress in normative development, and unfortunately prospects for inter-state cooperation have become dimmer. The 2018 session of the General Assembly witnessed a bifurcation of future work on cyber security norms when two competing resolutions were adopted on divided votes. A Russian-led resolution established an Open-Ended Working Group (OEWG) to ensure "more democratic, inclusive and transparent" negotiations in developing "rules, norms and principles of responsible behaviour of states"; whereas a US-led resolution adhered to the traditional GGE format with limited membership (UNGA 2018). This splintering of the UN work on devising cyber security norms reflects the strained relations between the leading cyber powers and will further complicate the effort to identify and operationalise such norms at the universal level.

Even if states persist in disputes regarding the nature of the norms that should apply to state conduct in cyberspace, there are constructive proposals being generated by other stakeholders. The Swiss-based NGO ICT4Peace, for example, has suggested that the cooperative measures recommended by the UN GGE process (specifically the measures recommended in the 2015 GGE report) be taken up by states regardless of the future course of this UN mechanism. ICT4Peace has also engaged in cybersecurity capacity building and has promoted this as a crucial enabler for the developing world to participate effectively in international policy discussions.

Finally, we should expect to see a greater engagement by the private sector and civil society with the specialised forums where representatives of government debate these issues (see also Chap. 13). Heightened awareness of the damage to civil interests that offensive state cyber operations can cause, intentionally or inadvertently, is likely to foster greater lobbying efforts to press governments to support cooperative efforts and measures of restraint in cyberspace. The 'Digital Peace Now' campaign launched in September 2018 by Microsoft in cooperation with ICT4Peace and other NGOs is a manifestation of this reaction. Moves to accelerate an unregulated 'militarisation' of cyberspace are likely to call forth countervailing pressures to ensure that inter-state cyber conflict, if not precluded, is at least mitigated and subject to some form of reciprocal restraint. Diplomatic discussion and the negotiation of norms of responsible state behaviour are likely to continue to feature prominently in these efforts.

References

Buchanen B (2016) The Cybersecurity dilemma: hacking, trust and fear between nations. Oxford University Press, Oxford

Coats DR (13 Feb 2018) Worldwide threat assessment of the US Intelligence Community. www.dni.gov. Last access: 7 July 2019

Gibson W (1984) Neuromancer. Ace Books, New York

Grigsby A (2017) The end of cyber norms. Survival 59(6):109–122
Hague W (2 Nov 2011) Closing remarks London conference on Cyberspace. www.fco.gov.uk/en/news/latest-news/?view=Speech&id=685672482. Last access: 7 July 2019
Hitchens T, Gallagher NW (Mar 2018) Building confidence in the Cybersphere: a path to multilateral progress. Center for International and Security Studies, University of Maryland. www.cissm.umd.edu. Last access: 7 July 2019
International Committee of the Red Cross (10 Oct 2017) Statement to UN General Assembly First Committee – General Debate on all disarmament and international security agenda items
GGE (2013) United Nations General Assembly Group of Governmental Experts on Developments in the field of information and telecommunications in the context of international security. A/68/98 (24 June). http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf. Last access: 7 July 2019
GGE (2015) United Nations General Assembly Group of Governmental Experts on Developments in the field of information and telecommunications in the context of international security. A/70/174 (22 July). https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf. Last access: 7 July 2019
ODA (2018) Securing our common future: an agenda for disarmament. www.un.org/disarmament. Last access: 7 July 2019
OSCE (26 Apr 2012) Permanent Council Decision 1039. www.osce.org/pc/90169. Last access: 7 July 2019
OSCE (3 Dec 2013) Permanent Council Decision 1106. www.osce.org/pc/109168. Last access: 7 July 2019
OSCE (10 Mar 2016) Permanent Council Decision 1202. www.osce.org/pc/227281. Last access: 7 July 2019
Qun W (19 Oct 2011) Work to build a peaceful, secure and equitable information and cyber space. Statement to UN General Assembly First Committee. www.fmprc.gov.cn/eng/wjdt/zyjh/t869580.htm. Last access: 7 July 2019
Smith B (14 Feb 2017) The need for a Digital Geneva Convention. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention. Last access: 7 July 2019
Smith B (14 May 2017) The need for urgent action to keep people safe online: Lessons learned from last week's cyberattack. https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/. Last access: 7 July 2019
Smith B (10 Nov 2017) We need to modernize international agreements to create a safer digital world. https://blogs.microsoft.com/on-the-issues/2017/11/10/need-to-modernize-international-agreements-to-create-a-safer-digital-world. Last access: 7 July 2019
Smith B (17 Apr 2018) 34 companies stand up for cybersecurity with a tech accord. https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord. Last access: 7 July 2019
Tikk E, Kerttunen M (Dec 2017) The alleged demise of the UN GGE: an autopsy and eulogy. Cyberpolicy Institute. www.cpi.ee. 22 Aug 2018
Tikk E (2018) "Introduction" Voluntary, non-binding norms for responsible state behaviour in the use of information and communications technology: a commentary. www.un.org/disarmament. Last access: 7 July 2019
UNIDIR (2016) Report of the International security cyber issues workshop series. www.unidir.org. Last access: 7 July 2019
UNGA (4 Jan 1999) Developments in the field of information and telecommunications in the context of international security A/RES/53/70
UNGA (30 Dec 2002) Developments in the field of information and telecommunications in the context of international security A/RES/57/53
UNGA (14 Sep 2011) International Code of Conduct for information security A/66/359

UNGA (13 Jan 2015) International Code of Conduct for information security A/69/723
UNGA (11 Dec 2018) Developments in the field of information and telecommunications in the context of international security A/RES/73/27 and 2 Jan 2019 Advancing responsible state behaviour in cyberspace in the context of international security A/RES/73/266
US Cyber Command (2018) Achieve and maintain cyberspace superiority: command vision for US Cyber Command www.cybercom.mil. Last access: 7 July 2019
White House (May 2011) International strategy for cyberspace: prosperity, security and openness in a networked world. whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Last access: 7 July 2019
Women's International League for Peace and Freedom (10 Oct 2017) Civil society statement on cyber. UN General Assembly First Committee. www.reachingcriticalwill.org. Last access: 7 July 2019