V. Cyber arms control and resilience

ENEKEN TIKK

Introduction

The dialogue in the United Nations on arms control and information and communications technology (ICT) dates back to the late 1990s. In 1998, wary of the information warfare doctrines of the United States and the rapid proliferation of ICT, Russia decided to take the question of ICT as a threat to peace and security to the First Committee of the UN General Assembly (on disarmament and international security). This eventually resulted in the setting up of a group of governmental experts (GGE) on developments in the field of information and telecommunications in the context of international security, which met for the first time in 2004.

The international community's concern about the disruptive impacts of ICT has expanded dramatically since that time. The US Council for Foreign Relations and the Center for Strategic and International Studies (CSIS) have identified over 250 state-sponsored cyberattacks in the period 2005–18.[1] Their conclusions about the states involved are similar to dyadic analysis published in 2014 on the period 2000–14.[2] These findings implicate around 20 states, most of which have taken part in the GGE discussions.

After two decades of deliberations, however, there is little common ground between states on the nature of the threat and the measures required to address it. A central challenge that the UN discussions face is that states have fundamentally different approaches to the use and regulation of ICT. The two most influential viewpoints are those of Russia and the USA, but they approach the topic from different perspectives. Russia wants to contain the actors with the greatest cyber capabilities and control information flows within national borders. It advocates a multilateral regulatory process to address the use of ICT for military, terrorist and criminal purposes. The USA, which is among the most cyber-capable actors, frames the discussion around the actions of states or activities targeted at states, and less about domestic security and information threats. Thus, the USA argues that there is no need for additional regulation at the international level because the use of ICT by states is already covered by international law. The distance between the Russian and US positions has been a barrier to progress at the UN level and reflects broader divisions in the positions of different groups of states.

Adding further confusion to these processes is the distance between the issues being discussed at the UN level and the reality of state-sponsored

[1] Council on Foreign Relations, 'Cyber operations tracker'.

[2] Valeriano, B. and Maness, R. C., 'The dynamics of cyber conflict between rival antagonists, 2001–11', *Journal of Peace Research*, vol. 51, no. 3 (May 2014), pp. 347–60.

cyberattacks in recent years. The vast majority of known state-sponsored cyberattacks are instances of cyber espionage. Where cyberattacks have had noticeable effects, these have been relatively limited: defacement of websites, temporary disabling of the services and functions of a system, data destruction and, in a few cases, sabotage and physical damage.[3] However, achieving an accurate understanding of the extent and content of state-sponsored cyberattacks can be difficult as most countries lack independent capabilities for conducting effective detection and attribution. A further complication is that ICT is available to anyone and networks are often owned and operated by the private sector, which makes it difficult for governments to exercise control over their use, or even agree that it is feasible to do so.[4] Russia and the USA share a reluctance to offer any additional guarantees that they will not conduct cyber operations that remain below the threshold of the use of force. This leaves the vast majority of state-on-state cyber operations—such as espionage, denial of service and data destruction—unaddressed by the First Committee dialogue. Moreover, the discussion of ICT in the First Committee remains compartmentalized from many other issues related to the development and use of these technologies. Cybercrime, terrorist use of ICT, internet governance, surveillance, privacy and other human rights issues are excluded from the focus of the arms control dialogue.

This section first reviews recent developments in international discussions on the use of ICT by states in the First Committee of the UN General Assembly. It discusses states' diverging views on the threats to international peace and security resulting from ICT, and their consequent differences about measures to address such threats. It examines, in particular, the achievements and aspirations of the two key rivals in the international cyber arms control dialogue: Russia and the USA. After assessing the future of the international cybersecurity dialogue, it then situates it in relation to other regional and private sector efforts aimed at creating shared norms and increasing resilience in the cyber field. The section concludes with a generally pessimistic view of the likelihood of reaching agreement on definitive normative guidance on cybersecurity, but highlights what states can do to mitigate this failure.

International dialogue within United Nations frameworks

The international discussion on the use of ICT by states in the First Committee has taken place under a Russian-initiated series of UN General

[3] Council on Foreign Relations (note 1).

[4] United Nations, General Assembly, 'Developments in the field of information and telecommunications in the context of international security', Report of the Secretary-General, A/66/152, 15 July 2011.

Assembly resolutions on 'Developments in the field of information and telecommunications in the context of international security'.[5] Some states refer to these efforts as the international cybersecurity dialogue, others as international information security negotiations.

These resolutions have initiated two interlinked processes. First, every year UN member states are invited to inform the UN Secretary-General of their views on and assessments of issues related to information security and the advisability of developing relevant measures at the global level. Second, since 2004, GGEs have met to discuss these issues and to study the threat and measures to mitigate it. Three of the five GGEs have issued consensus reports (see table 9.3).

The GGE process

The first GGE was not able to achieve consensus on whether the development and use of ICT could constitute a threat to international peace and security. However, after cyberattacks against Estonia in 2007 and the use of cyber-attacks in the Russo-Georgian war in 2008, experts agreed to discuss the threat and ways to address it. Negotiations in the GGEs of 2009–10, 2012–13 and 2014–15 resulted in general acknowledgment of the threat and a shared conclusion that international law was applicable to issues of international information security.

By 2015 the fourth GGE had developed a four-tier structure of discussions: (*a*) the applicability of international law; (*b*) development of voluntary and non-binding norms, rules and principles of responsible behaviour of states; (*c*) confidence-building measures (CBMs); and (*d*) relevant capacity building.

The fifth GGE, in 2016–17, was tasked with clarifying how international law applies to the use of ICT by states.[6] However, incompatible national interests made it impossible to forge consensus, and it was unable to issue a consensus report as a result.[7] The chair of the group concluded that 'deep divisions remained on some aspects of how international law applies to the use of ICT by States'.[8]

The UN General Assembly did not adopt its usual resolution in 2017 and no substantive agenda was put forward for 2018. This left the international

[5] UN General Assembly resolutions on 'Developments in the field of information and telecommunications in the context of international security', 53/70 of 4 Dec. 1998; 54/49 of 1 Dec. 1999; 55/28 of 20 Nov. 2000; 56/19 of 29 Nov. 2001; 57/53 of 22 Nov. 2002; 58/32 of 8 Dec. 2003; 59/61 of 3 Dec. 2004; 60/45 of 8 Dec. 2005; 61/54 of 6 Dec. 2006; 62/17 of 5 Dec. 2007; 63/37 of 2 Dec. 2008; 64/25 of 2 Dec. 2009; 65/41 of 8 Dec. 2010; 66/24 of 2 Dec. 2011; 67/27 of 3 Dec. 2012; 68/243 of 27 Dec. 2013; 69/28 of 2 Dec. 2014; 70/237 of 23 Dec. 2015; 71/28 of 5 Dec. 2016; and 73/27 of 5 Dec. 2018.

[6] UN General Assembly Resolution 70/237 (note 5).

[7] United Nations, General Assembly, Group of governmental experts on developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, A/72/327, 14 Aug. 2017.

[8] United Nations, General Assembly, 72nd session, First Committee, 19th meeting, A/C.1/72/PV.19, 23 Oct. 2017, p. 2.

Table 9.3. Groups of governmental experts on developments in the field of information and telecommunications in the context of international security, 2004–17

Years	No. of members	Chair	Other participating states	Consensus report
2004–05	15	Russia	Belarus, Brazil, China, France, Germany, India, Jordan, Korea (South), Malaysia, Mali, Mexico, South Africa, UK, USA	Not issued
2009–10	15	Russia	Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, Korea (South), Qatar, South Africa, UK, USA	Issued[a]
2012–13	15	Australia	Argentina, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, UK, USA	Issued[b]
2014–15	20	Brazil	Belarus, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Korea (South), Malaysia, Mexico, Pakistan, Russia, Spain, UK, USA	Issued[c]
2016–17	25	Germany	Australia, Botswana, Brazil, Canada, China, Cuba, Egypt, Estonia, Finland, France, India, Indonesia, Japan, Kazakhstan, Kenya, Korea (South), Mexico, Netherlands, Russia, Senegal, Serbia, Switzerland, UK, USA	Not issued[d]

[a] United Nations, General Assembly, Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security, A/65/201, 30 July 2010.

[b] United Nations, General Assembly, Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security, A/68/98, 24 June 2013.

[c] United Nations, General Assembly, Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security, A/70/174, 22 July 2015.

[d] United Nations, General Assembly, 72nd session, First Committee, 19th meeting, A/C.1/72/PV.19, 23 Oct. 2017, pp. 1–3.

community wondering whether the cyber arms control agenda had run out of steam.

Two new General Assembly resolutions in 2018

The usual General Assembly resolution underwent a significant upgrade in 2018.[9] The resolution now lists a selection of norms, rules and principles recommended by the GGE. It establishes an open-ended working group (OEWG) to build on the work of the earlier GGEs. The OEWG will discuss the implementation of these norms and, if necessary, introduce changes

[9] UN General Assembly Resolution 73/27 (note 5).

to them or elaborate additional rules of behaviour. The OEWG, a General Assembly process, will convene diplomats to consider 'the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations'.[10] All interested states can now study and promote common understandings of: (*a*) existing and potential threats in the sphere of information security; (*b*) possible cooperative measures to address these threats; (*c*) how international law applies to the use of ICT by states; (*d*) CBMs; and (*e*) capacity building.

Russia is the sponsor of this process. It is committed to making the UN negotiation process on security in the use of ICT more democratic, inclusive and transparent.

The USA was strictly against both the content and format of the resolution.[11] Accordingly, the USA initiated a separate General Assembly resolution on 'Advancing responsible state behaviour in cyberspace in the context of international security'.[12] This resolution establishes a new, government expertise-based, GGE on this subject to build on the assessments and recommendations in the reports of the earlier GGEs, and 'to continue to study, with a view to promoting common understandings on and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security'. Such common understandings might include 'norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States'.[13]

The process has thus split into two threads, neither of which is a direct continuation of the original process of 1998–2017 (see figure 9.2). The Russian-sponsored OEWG aims for cyber or information arms control with legally binding instruments, whereas the new, US-sponsored GGE is focused on voluntary and non-binding norms in peacetime.

Russian and US intentions, concepts and definitions

The seemingly similar mandates of the two working formats should not be mistaken for unity on what needs to be achieved. In order to understand Russia's intentions for the OEWG, it is necessary to take account of its information security policy and doctrine. Over time, Russia has clarified its original call for a ban on information weapons as these weapons and their uses have come to be a reality.

[10] UN General Assembly Resolution 73/27 (note 5), para. 5.

[11] Wood, R. A., US delegation, Statement to the UN General Assembly First Committee, 29 Oct. 2018.

[12] UN General Assembly Resolution 73/266, 'Advancing responsible state behaviour in cyberspace in the context of international security', 22 Dec. 2018.

[13] UN General Assembly Resolution 73/266 (note 12), para. 3.

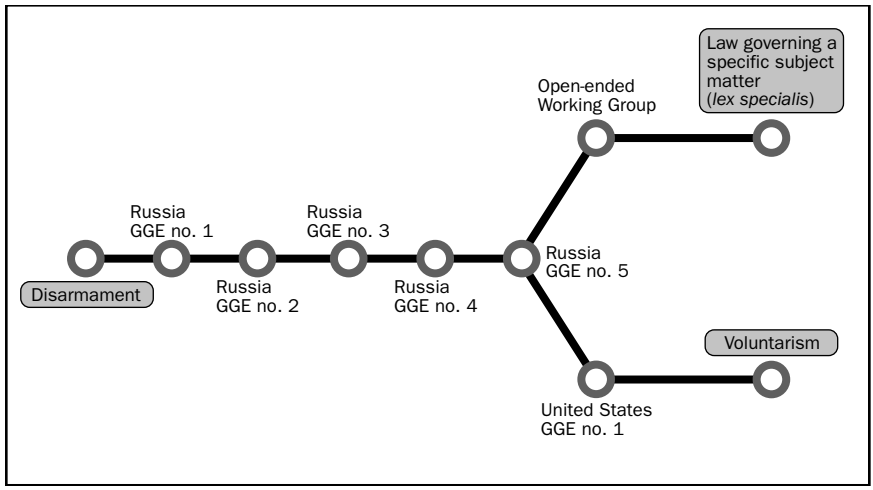

Figure 9.2. The international cybersecurity dialogue processes
GGE = group of governmental experts.

In the GGE process, Russia first defined information weapons as 'Means and methods used with a view to damaging another State's information resources, processes and systems; use of information to the detriment of a State's defence, administrative, political, social, economic or other vital systems, and the mass manipulation of a State's population with a view to destabilizing society and the State'.[14] More recently, leading Russian military officials have defined information weapons as capabilities to destroy an adversary's information systems or disable them temporarily. In particular, such weapons comprise: (*a*) electromagnetic weapons, such as radio jammers, electromagnetic pulsed weapons and directed energy weapons; (*b*) software weapons, such as computer viruses, computer worms, Trojan programs, hidden management utilities and so on; and (*c*) hardware weapons, such as bookmarks to permit unauthorized access to computer information, download and transmit it to an addressee and mount attacks against computer networks to modify or destroy information stored and circulating in them.[15]

Russia's information security doctrines have set a more nuanced agenda for the prohibition of the development, dissemination and use of information weapons. Russia's goal remains the formation of an international information

[14] United Nations, General Assembly, 'Developments in the field of information and telecommunications in the context of international security', Report of the Secretary-General, A/54/213, 10 Aug. 1999, p. 10.

[15] Dylevsky, I. N. et al., 'Political and military aspects of the Russian Federation's state policy on international information security', *Military Thought*, vol. 24, no. 1 (2015), pp. 7–16.

security system.[16] A specialized non-proliferation regime would form part of this system.[17] Russia has consistently argued for international law to be adapted to this end, but it has also stressed that this system must be created on the basis of universally recognized principles and rules of international law such as respect for national sovereignty, no use or threat of force in international relations, and the right of states to individual and collective defence.[18] This constitutes a potential dividing line between Russia and China, as China has rejected the applicability of international humanitarian law to cyberattacks, suggesting that the UN Charter contains an absolute prohibition on the use of force in cyberspace.[19]

It is also evident that Russia's reading of existing international law is not shared by many other states, as demonstrated by its joint proposals with the other members of the Shanghai Cooperation Organisation (SCO) in 2011 and 2015 for an international code of conduct on information security.[20] Both these proposals contained formulations that expanded the language of some familiar rules and standards of international law, but they gained little support. The 2018 General Assembly resolution on information security, however, makes direct reference to a long-forgotten 1981 General Assembly resolution, the Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States.[21] This declaration contains ideas that Russia and China have sought to socialize within the UN system: it speaks strongly of sovereignty and the principles of non-intervention and non-interference in the internal and external affairs of states being of 'the greatest importance for the maintenance of international peace and security'. It also refers to the notions of national identity and cultural heritage, and states' right to develop 'their system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations'. The latter is said to be based on, among other

[16] Information Security Doctrine of the Russian Federation, approved by Presidential Decree no. 646 of 5 Dec. 2016 (in Russian), paras 19 and 29 (b), (c), (d). An English translation is available at <http://interkomitet.com/foreign-policy/basic-documents/doctrine-of-information-security-of-the-russian-federation/>.

[17] Foundations of the State Policy of the Russian Federation on International Information Security in the Period up to 2020, approved 24 July 2013, no. 1753 (in Russian). See also Dylevsky et al. (note 15).

[18] Dylevsky et al. (note 15).

[19] United Nations, A/C.1/72/PV.19 (note 8), p. 14.

[20] United Nations, General Assembly, 'International code of conduct for information security', Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, 14 Sep. 2011; and United Nations, General Assembly, 'International code of conduct for information security', 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, A/69/723, 13 Jan. 2015. For a brief description and other details of the SCO see annex B, section II, in this volume.

[21] UN General Assembly Resolution 73/27 (note 5), opening para.; and UN General Assembly Resolution 36/103, 'Declaration on the inadmissibility of intervention and interference in the internal affairs of states', 9 Dec. 1981.

things, 'the relevant articles of the Universal Declaration of Human Rights and the principles of the new international information order'.[22]

Senior Russian officials have accused the West, especially the USA, of the development and dissemination of cyberweapons 'practically with no controls' with the result 'that instances of their unlawful use are multiplying'.[23] More recently, however, perhaps to underline that the precedent set by the USA is not lost on it, Russia has been observed using the same techniques and tools. This, in turn, inevitably changes the governing calculus for an international information security regime, as non-proliferation would now be likely to address primarily those countries that do not possess advanced ICT capabilities, as well as particularly hostile uses of ICT.

The USA has stood by the argument that the use of ICT by states is already sufficiently covered in international law. It remains strongly opposed to the kind of state regulation in the field of information flows favoured by Russia. In particular, the USA has emphasized the right to countermeasures and self-defence in the context of cyberattacks. The USA argues in favour of a policy of consequences, through which governments must seek to deter malicious non-state actors: the US Department of State has recommended that 'The United States should prepare a menu of options for swift, costly, and transparent consequences below the threshold of the use of force that it can impose, consistent with US obligations and commitments, following an incident that merits a strong response that can have downstream deterrent effects'.[24] More recently, the United Kingdom has expressed a view that, in the context of cybersecurity, sovereignty is just a principle and not a rule.[25] This view—which is in line with one earlier expressed by the staff judge advocate of the US Cyber Command—justifies infringements of sovereignty by cyber means.[26]

The 2018 US National Cyber Strategy seeks to 'preserve peace through strength' using two management mechanisms that provide a basis for responses to those state actions that are inconsistent with the US framework.[27] The administration of US President Donald J. Trump promises to 'promote a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state

[22] UN General Assembly Resolution 36/103 (note 21), para. 1(c).

[23] Dylevsky et al. (note 15).

[24] US Department of State, Office of the Coordinator for Cyber Issues, 'Recommendations to the President on deterring adversaries and better protecting the American people from cyber threats', 31 May 2018.

[25] Wright, J., British Attorney General, 'Cyber and international law in the 21st century', Speech, British Attorney General's Office, 23 May 2018.

[26] Corn, G. P. and Taylor, R., 'Sovereignty in the age of cyber', *AJIL Unbound*, vol. 111 (2017), pp. 207–12.

[27] White House, *National Cyber Strategy of the United States of America* (White House: Washington, DC, Sep. 2018), p. 20.

behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity'. The USA is ready to ensure that there are 'swift, costly and transparent consequences' for irresponsible, malicious and harmful behaviour. It considers that all instruments of national power are employable in this endeavour.[28] The cyber strategy of the US Department of Defense (DOD) promotes the development of military capacity to conduct cyberspace operations for both war fighting and countering malicious cyber actors. It also stresses that the DOD 'will reinforce voluntary, non-binding norms of responsible state behavior in cyberspace during peacetime'.[29]

Accordingly, despite their differences, both Russia and the USA were satisfied with the outcome of the 2014–15 GGE, particularly with the recommendation on 11 norms of responsible state behaviour.[30] While the GGE clearly stated that such norms, rules and principles are voluntary and non-binding and therefore not a move towards a new legal regime, the report can also be read as supporting the Russian proposition that there are gaps in international law that need to be addressed.

Hardly any country subscribes wholly to either the Russian or the US view. In voting against the OEWG, the US view was supported by the European Union (EU) member states and the remaining members of the Five Eyes intelligence-sharing alliance.[31] However, a statement in the General Assembly by French President Emmanuel Macron just days before the vote left little doubt about France's commitment to sovereignty.[32] In its discussions on the Dutch-initiated 'cyber diplomacy toolbox' (see below), the EU does not appear to be united on how a deterrence-first approach would fit with its otherwise robustness- and resilience-focused cybersecurity agenda.[33] Australia appears unconvinced by the British and US views on sovereignty.[34]

China continues to try to push the discussion on cybersecurity towards a greater emphasis on governance. While sharing Russia's views on sovereignty,

[28] White House (note 27), pp. 20–21.

[29] US Department of Defense (DOD), *Summary: 2018 Department of Defense Cyber Strategy* (DOD: Washington, DC, 2018), pp. 4–5.

[30] United Nations, General Assembly, Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security, A/70/174, 22 July 2015, para. 13.

[31] The Five Eyes alliance comprises Australia, Canada, New Zealand, the UK and the USA.

[32] United Nations, General Assembly, 73rd session, 6th plenary meeting, A/73/PV.6, 25 Sep. 2018, pp. 29–30.

[33] Council of the European Union, 'Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ("cyber diplomacy toolbox")', 10474/17, 19 June 2017.

[34] Australian Government, *2017 Foreign Policy White Paper: Opportunity Security Strength* (Department of Foreign Affairs and Trade: Canberra, Nov. 2017), p. 74. For an analysis of national views on international law based on a reading of their national policy and strategy documents see Väljataga, A., *Tracing* Opinio Juris *in National Cyber Security Strategy Documents* (NATO Cooperative Cyber Defence Centre of Excellence: Tallinn, 2018).

China has also made a case for international law, emphasizing that rules must be observed and responsibilities honoured.[35]

The burning question, however, is: which rules and whose responsibilities? In order to promote its political ambitions, Russia is trying to codify notions such as national identity, cultural heritage, media sphere and public order in the ICT environment. Western states, in turn, are pushing their reading of the law on state responsibility and of international humanitarian law. In the dialogue on international law, the China–Russia coalition usually applies a rules-based approach while the West takes policy-based positions. The former approach, according to one expert, regards the law as normatively strong but restricted in scope; the latter sees the law as normatively weak but wide in scope.[36]

The international dialogue as arms control?

The dialogue in the First Committee and the GGEs has used traditional arms control language. An increasing tendency to refer to conflict prevention and CBMs can be perceived between the 2010, 2013 and 2015 GGE reports. In logic similar to the logic of arms control, members of the GGEs have concluded that the proliferation and use of ICT in conflict could threaten international peace and security. They have proposed that ICT threats to peace and security need to be addressed through measures similar to those used in arms control: limitations on usage and development through normative measures and the prevention of conflicts and escalation through CBMs, as well as specific institutional arrangements.

However, these arms control methods have not been fully operationalized in the context of ICT. To date, there have been no negotiations on international instruments to reduce, limit or ban the development and use of military ICT capabilities. Nor has there been any authoritative guidance on how international law is or is not applicable in the above-mentioned situations, regardless of whether they are brought about by state or non-state actors using ICT for political purposes. Nor have GGE members inspected or scrutinized national cyber capabilities and activities. As a result, the GGE measures do not effectively target the issue of conflicts or the question of escalation and de-escalation. Instead, concepts of international law that some experts did not consider acceptable for their respective states have been moved to the report's section on voluntary and non-binding norms. In

[35] United Nations, General Assembly, 73rd session, 12th plenary meeting, A/73/PV.12, 28 Sep. 2018, p. 19.

[36] Koskenniemi, M., *From Apology to Utopia: The Structure of International Legal Argument* (Cambridge University Press: Cambridge, 2005), pp. 184–85.

the consensus-based process, for this to happen, it is sufficient for one expert to feel strongly against a particular legal concept.[37]

Despite the widespread allegations of state-sponsored cyber operations, the GGEs have also avoided taking a clear stand on preventing cyberattacks. Unresolved issues are the thresholds for the use of force and armed attack and the application of international humanitarian law. Russia's focus is on obtaining assurances about the use of force by cyber means, while the US focus remains on re-emphasizing the existing rules that are applicable in the context of hostilities.[38]

In sum, the five GGEs have achieved little on the issue of non-proliferation. The GGEs have, instead, embarked on issues such as lack of national capacity, deficiencies in resilience, and the absence of a common understanding of the potential and benefits of ICT. These, however, are not suitable for arms control measures. Nonetheless, the GGE process has gathered a curious international community around the dialogue, as many states are worried about the potential impact of ICT on their national security. Between 2006 and 2017, more than 110 states have sponsored Russia's General Assembly resolution. The OEWG proposal attracted further sympathetic states as the member states of the EU and the North Atlantic Treaty Organization (NATO) withdrew their support.[39] Since 1999, over 70 states have sent an assessment of the situation to the UN Secretary-General.[40]

The current status of the international dialogue

Until 2016–17 it had been assumed that each GGE accepted the premises and conclusions of its predecessors and that, therefore, some issues had been settled. Until 2013, Russia's original proposition that it was necessary to develop an international legal regime in order to prohibit the development, production or use of particularly dangerous forms of information weapons dominated proceedings.[41] To this end, states were consulted on how to develop international principles that would enhance the security of

[37] E.g. in the 2015 GGE report, differences on state responsibility and due diligence resulted in these topics being included in the section on norms, rules and principles. United Nations, A/70/174 (note 30), para. 13.

[38] United Nations, A/66/152 (note 4), p. 18.

[39] The Russian-sponsored UN General Assembly Resolution 73/27 (note 5) was passed by a vote of 119 in favour and 46 against, with 14 abstentions. The US-sponsored Resolution 73/266 (note 12) was passed by a vote of 138 in favour and 12 against, with 16 abstentions. United Nations, General Assembly, 73rd session, 45th plenary meeting, A/73/PV.45, 5 Dec. 2018, p. 4; and United Nations, General Assembly, 73rd session, 65th plenary meeting, A/73/PV.65, 21 Dec. 2018, p. 14.

[40] For a list of these countries see Tikk, E. and Kerttunen, M., *Parabasis: Cyber-diplomacy in Stalemate*, Norwegian Institute of International Affairs (NUPI) Report no. 5/18 (NUPI: Oslo, 2018), annex A.

[41] United Nations, General Assembly, 53rd session, First Committee, Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, A/C.1/53/3, 30 Sep. 1998, appendix, para. 3(c).

global information and telecommunications systems and help to combat information terrorism and criminality.[42]

In 2013, however, the GGE concluded that 'International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment'.[43] This was widely interpreted, especially in the West, as a decisive step towards accepting the authority of existing international law and a dismissal of the call for a special legal regime. However, the same report also states that:

> The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability. Common understandings on how such norms shall apply to State behaviour and the use of ICTs by States requires further study. Given the unique attributes of ICTs, additional norms could be developed over time.[44]

In the 2016–17 session of the GGE, some experts directly challenged the applicability of international law.[45] Hence, the issue of the applicability and sufficiency of international law in the context of state use of ICT has not been settled and remains at the core of the international information security dialogue.

The language in the GGE reports is significant in that it incorporates two different views on and expectations of the world. The first, from the West, regards the proliferation of ICT as positive and considers that existing international law is sufficient to guide state behaviour in cyberspace. The other view, from a group of countries led by China and Russia, regards digitization as a threat and prefers new normative guidance on state use and development of ICT. For many years, the GGE reports have been framed and worded in such a way that both views could be accommodated. As a result, the GGE reports offered little normative guidance to the international community.

Instead of condemning or restraining any particular conduct, the GGEs have opted to support the pursuit of voluntary, non-binding norms, rules and principles and for selective reiteration of concepts of international law. Although most states have welcomed this approach, it does little to change problematic behaviour. Offered on a strictly non-binding and voluntary basis, the norms approach brings no predictability to international cyber affairs and creates further uncertainty about the authority of international law. The UN High Representative for Disarmament Affairs, Izumi Nakamitsu, is optimistic

[42] UN General Assembly Resolution 53/70 (note 5).

[43] United Nations, General Assembly, Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security, A/68/98, 24 June 2013, para. 19.

[44] United Nations, A/68/98 (note 43), para. 16.

[45] United Nations, General Assembly, 72nd session, First Committee, 7th meeting, A/C.1/72/PV.7, 9 Oct. 2017, p. 21.

that the consensus reports have laid the foundations for preventing and mitigating offensive cyber operations, but she also continues to emphasize that the current framework is non-binding.[46]

Other acute, non-cyber-related risks between Russia and the USA have been addressed through bilateral arms control measures, such as the establishment of a Russian–US hotline, with the intention of avoiding a major war. Following this logic, Russia has proposed military-to-military dialogue and negotiations to prevent accidental cyber conflict between Russia and the USA. So far, the USA has not responded.[47]

The future of the United Nations process

The setting up of an OEWG is a clear advance of Russia's aim to create a non-proliferation cyber regime sealed by an international agreement. The OEWG is built around the premise of chronic cyber confrontation. It is a strong manifestation of the return of a bipolar world order. Behind this move is the Russian belief that it will be able to convince the world of the threats linked to digitization and excess dependence on ICT. The significance of the passage of a resolution on establishing an OEWG is the opportunities it provides for wider dissemination of a more cautious approach to ICT.

In the future, the GGE and the OEWG will need to choose between or become reconciled with the different standpoints, perspectives and interests of Russia and the USA, as well as agile countries keen to adopt advanced technologies and some developing countries that might be less keen. States have proffered many views on the various threats and measures that could be considered in both forums. These range from discussions on a new legal regime and specific bans, via exchanges of views on patterns of state behaviour to taking the matter to the UN Security Council.

Cuba, for example, remains determined that there should be 'urgent action within the framework of the United Nations in order to prevent the covert and illegal use by individuals, organizations and States of other nations' computer systems to attack other countries, because of its potential to provoke international conflicts'.[48] According to Egypt,

> Cybersecurity has become a vital field affecting all aspects of daily life and the safety and stability of the strategic facilities and infrastructure of every State. Developing consensus-based international standards to ensure that this space is not used for

[46] United Nations, General Assembly, 72nd session, First Committee, 10th meeting, A/C.1/72/PV.10, 11 Oct. 2017, p. 3.

[47] Streltsov, A. and Smirnov A., [Russian–US cooperation in the sphere of international information security: Suggestions regarding priority areas], *Mezhdunarodnaya zhizn*, Nov. 2017, pp. 72–81 (in Russian).

[48] United Nations, General Assembly, 72nd session, First Committee, 3rd meeting, A/C.1/72/PV.3, 3 Oct. 2017, p. 15.

destructive purposes that undermine international peace and security is one of the most important issues confronting the United Nations today.[49]

The International Committee of the Red Cross (ICRC) has noted the challenges of compliance with international humanitarian law raised by new cyber capabilities and has called for urgent international debate on such means of warfare.[50] Finland has called for an exchange of views on serious cyberattacks below the threshold of an armed attack—on both their prevention and the tools available to states that are victims of such attacks.[51] Estonian President Kersti Kaljulaid has said that 'all cybersecurity and artificial intelligence issues should be brought to the UN Security Council table, because international law in this area is clearly lagging behind'.[52]

France has proposed further steps to control exports of offensive cyber tools and techniques with a view to limiting their proliferation in cyberspace and more elaborate measures to prevent non-state actors from carrying out offensive activities in cyberspace.[53] Brazil maintains that the international community must examine the need to develop a specific legal framework that would include prohibitions on offensive first-use, tampering with the supply chain, intentionally introducing vulnerabilities into systems or networks, and compromising the information security of other states.[54] The Caribbean Community (CARICOM) has suggested even more explicitly that if the UN is serious about disarmament, it must also be serious about addressing cybersecurity as 'Increased cybersecurity has the potential to stymie the illicit manufacture, transfer and circulation of illegal weapons'.[55]

The road ahead promises to be more inclusive and transparent. The OEWG process is open to all states. The UN Office for Disarmament Affairs (UNODA) will support the GGE by collaborating with relevant regional organizations to convene a series of consultations that will share views on the issues within the GGE's mandate in advance of its sessions. In addition, the chair of the GGE will organize consultative meetings to enable all UN member states to engage in interactive discussions and share their views, which the chair will then

[49] United Nations, General Assembly, 72nd session, First Committee, 4th meeting, A/C.1/72/PV.4, 4 Oct. 2017, p. 11.

[50] United Nations, General Assembly, 72nd session, First Committee, 9th meeting, A/C.1/72/PV.9, 10 Oct. 2017, p. 7.

[51] United Nations, General Assembly, 72nd session, First Committee, 20th meeting, A/C.1/72/PV.20, 23 Oct. 2017, p. 11.

[52] Quoted in Aaresild, A., 'Eesti ÜRO julgeolekunõukokku—mis sõnumiga?' [Estonian membership of the UN Security Council—what message?], Opinion Festival, Paide, 20 Sep. 2018 (author's translation). See also Baltic News Service, 'President: Estonia can raise issue of cyber security on UN Security Council', Eesti Rahvusringhääling, 12 Aug. 2018.

[53] United Nations, A/C.1/72/PV.20 (note 51), p. 15.

[54] United Nations, A/C.1/72/PV.19 (note 8), p. 23.

[55] United Nations, General Assembly, 72nd session, First Committee, 6th meeting, A/C.1/72/PV.6, 6 Oct. 2017, p. 23.

convey to the GGE for consideration.[56] The prospect of more transparency and inclusion, however, should not be regarded with excess optimism. States entering these dialogues must have a clear understanding of what they want and what they will be able to achieve there. If not, governments and their experts risk becoming pawns in the strategic security confrontation between Russia and the USA.

The governing norms approach is not a sufficient answer to the totality of concerns that the international community has expressed with regard to the development and use of ICT. In the next stage of the dialogue it is therefore possible that attempts at top-down arms control or normative voluntarism will be met by and confronted with further national concerns about the interpretation and implementation of international law and ideas on the remedies achieved by increased resilience as a bottom-up approach. It is possible that this could lead to a clash of frames and processes at the UN level.

Regional, national and corporate processes

Several regional organizations have made significant headway in comparison with the UN dialogue. There have also been important national and corporate initiatives.

Efforts by regional organizations

In 2018 the General Data Protection Regulation (GDPR) and Network and the Information Security Directive (NIS Directive) came into force in the EU.[57] These upgraded regional measures on data breaches and intrusions into systems. In addition, a Dutch initiative on coordinated EU cyber diplomacy is under way following the adoption of the 'cyber diplomacy toolbox', a joint EU diplomatic response to cyber operations.[58] With this step, the EU approach can be read as moving from preventive and regulatory to responsive and retaliatory.[59]

In 2013 and 2016 the Organization for Security and Co-operation in Europe (OSCE) adopted a set of CBMs to reduce the risk of conflict arising from the

[56] UN General Assembly Resolution 73/266 (note 12), para. 5.

[57] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, L 119, 4 May 2016; and Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *Official Journal of the European Union*, L 194, 19 July 2016.

[58] Council of the European Union (note 33).

[59] See e.g. the comment by Estonia in United Nations, A/C.1/72/PV.20 (note 51), p. 12.

use of ICTs.[60] It focused on their implementation in 2017 and 2018. Among the measures are exchanges of threat assessments, cooperation between national cybersecurity authorities, risk consultations, information sharing, joint capacity building, and transparency in national policies and legislation. A 2016 analysis of states' implementation of the OSCE CBMs found high implementation rates in the Nordic countries and underscored the role of incident response teams in confidence building.[61]

NATO has made a decisive move to develop its capability for cyber operations. It now considers cyberspace to be among the conflict domains in which it is facing 'challenges and threats from all strategic directions'.[62] NATO has reaffirmed its commitment to act in accordance with international law and 'agreed how to integrate sovereign cyber effects [i.e. the military cyber organizations of individual member states] . . . into Alliance operations and missions, in the framework of strong political oversight'.[63] The USA, the UK, the Netherlands and Estonia are among the NATO members that are likely to lend their capabilities. NATO is also building a Cyberspace Operations Centre at its headquarters in Mons, Belgium.[64] Given the differences over the applicability of international law in cyberspace among its member states, NATO will face challenges reconciling the capabilities offered with international law. Cybersecurity is also an area of NATO and EU cooperation.[65]

The Association of Southeast Asian Nations (ASEAN) has taken steps to improve cybersecurity in the region, and to improve national cyber capacity in particular. In the context of norm development, Singapore has taken the lead in implementing the GGE's 2015 recommendations as well as developing specific ASEAN norms. In 2018 the ASEAN leaders enshrined their commitment to cooperate on cyber affairs in general and the norms process in particular in a joint statement with the USA.[66]

[60] Organization for Security and Co-operation in Europe (OSCE), Permanent Council, 'Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies', Decision no. 1106, PC.DEC/1106, 3 Dec. 2013; and OSCE, Permanent Council, 'OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies', Decision no. 1202, PC.DEC/1202, 10 Mar. 2016.

[61] OSCE and University of Florence Department of Political and Social Sciences, *Analysis of the Implementation of the Initial Set of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies* (Firenze University Press: Florence, 2017).

[62] North Atlantic Treaty Organization, North Atlantic Council, 'Brussels summit declaration', NATO Press Release no. (2018) 074, 11 July 2018, para. 2.

[63] North Atlantic Treaty Organization (note 62), para. 20.

[64] North Atlantic Treaty Organization (note 62), para. 29.

[65] North Atlantic Treaty Organization and European Union, 'Joint declaration on EU–NATO cooperation', NATO Press Release no. (2018) 095, 10 July 2018.

[66] ASEAN–United States leaders' statement on cybersecurity cooperation, Singapore, 15 Nov. 2018.

National and corporate initiatives

National and corporate initiatives have emerged in support of specific agendas and goals.

The London Process is a series of global conferences on cyberspace held biennially since 2011. These events bring together representatives of governments, the private sector and civil society to discuss and promote practical cooperation in cyberspace, to enhance cyber capacity building and to discuss norms on responsible behaviour in cyberspace. The statements of the conference chairs encapsulate various principles and conclusions on responsible state behaviour in cyberspace. The chair's statement on the 2017 conference, held in New Delhi, India, has been assessed as a regression from previous commitments.[67]

Since hosting the 2015 conference of the London Process in The Hague, the Netherlands has acquired a prominent position in the international cyber community by hosting and funding several influential cybersecurity activities. The Global Commission on the Stability of Cyberspace (GCSC) has worked to develop proposals on norms and policies to enhance international security and stability and guide responsible state and non-state behaviour in cyberspace.[68] The Global Forum on Cyber Expertise, a global platform for countries, international organizations and private sector companies to exchange best practices and expertise on cyber capacity building, is also based in The Hague.[69]

The Netherlands is also funding The Hague Process on the Tallinn Manual. The manual was a result of a series of academic discussions on how international law could be applied to cyber operations, hosted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia.[70] In 2015 the Dutch Ministry of Foreign Affairs decided to fund a process that would make the findings of the book available to audiences worldwide. This led to a series of courses on the international law applicable to cyber operations based on a new edition of the manual.[71]

The 2018 World Internet Conference in Wuzhen, China, issued the Wuzhen Outlook, which confirmed a 'rough consensus' that 'The cyberspace

[67] Global Conference on Cyberspace (GCCS) 2017, 'Chair's statement–summary', 24 Nov. 2017; and Kaspar, L., 'GCCS2017: A cyberspace free, open and secure (but mostly secure)', Global Partners Digital, 29 Nov. 2017.

[68] Global Commission on the Stability of Cyberspace, 'The commission'.

[69] Global Forum on Cyber Expertise, 'Framework document', 16 Apr. 2016.

[70] Schmitt, M. N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Operations* (Cambridge University Press: Cambridge, 2013).

[71] Schmitt, M. N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press: Cambridge, 2017).

governance framework will continue to evolve and the shared governance system must be improved'.[72]

Although the two issues of internet governance and international cybersecurity are kept carefully apart in the GGEs, they keep merging in other settings. The Netherlands has also noted 'the constructive and fruitful discussions that took place [in the 2016–17 GGE] on the protection of the general functionality of the Internet'.[73]

France is promoting its own international cybersecurity agenda. Since November 2018, more than 60 states, including all the EU member states, have pledged their support for a new international agreement on setting standards on cyberweapons and the use of the internet by signing the Paris Call for Trust and Security in Cyberspace.[74] Russia, China and the USA are not among the signatories.

The US technology company Microsoft has sponsored a process to promote a Digital Geneva Convention. This calls on governments 'to protect civilians on the internet in times of peace' and promotes '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'.[75] While this initiative has not acquired governmental support, it has caught the attention of some states and led to inquiries by the ICRC about the protection of civilians from cyberattacks.[76]

However, other than their proliferation, there are few noticeable trends and little meeting of minds in all these efforts.

National resilience and corporate responsibility

An essential clue to what states are doing in a situation where universal and effective normative solutions are unlikely to be achieved can be derived from the USA's 2011 submission to the First Committee: 'The tasks of Member States are twofold: domestic and international. Securing national information infrastructures is a responsibility Governments must lead on domestically, in coordination with relevant civil society stakeholders.'[77] The GGEs have also outlined national cybersecurity standards and how states

[72] World Internet Conference, Organizing Committee, High-level Advisory Council, 'Wuzhen Outlook 2018', 9 Nov. 2018, point 5.

[73] United Nations, A/C.1/72/PV.19 (note 8), p. 24.

[74] Paris Call for Trust and Security in Cyberspace, Paris, 12 Nov. 2018; French Ministry for Europe and Foreign Affairs, 'Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace'; and Agence France-Presse, '"Paris call": 51 states vow support for global rules on cyberweapons', France 24, 12 Nov. 2018.

[75] Smith, B., President, Microsoft, 'The need for a digital Geneva Convention', Keynote address, RSA conference, San Francisco, CA, 14 Feb. 2017.

[76] International Committee of the Red Cross (ICRC), 'Digital technology and war', 27 June 2017.

[77] United Nations, A/66/152 (note 4), p. 15.

might cooperate on implementing such standards, for example, on protecting critical infrastructure, ensuring the integrity of the supply chain, preventing the proliferation of malicious ICT tools and techniques, and sharing information.[78]

The 2018 dialogue in the General Assembly also marked a potential move away from cybersecurity and towards a more inclusive and comprehensive dialogue on cyber-related issues. The UN Secretary-General, António Guterres, seems to be guiding the international dialogue towards harnessing technology in support of the Sustainable Development Goals. He has referred to the impacts of new technologies on warfare as 'a direct threat to our common responsibility to guarantee peace and security'.[79] According to Guterres:

> The prospect of machines with the discretion and power to take human life is morally repugnant. Heaven forbid, a new war could very well include a massive cyberattack that targets not only military capacities, but also critical civilian infrastructure. . . .
>
> More work on those issues, aimed at building trust between and within nations, will be needed if we are to ensure the responsible use of new technologies.[80]

The UN Secretary-General's Strategy on New Technologies points out that the scale and pervasiveness of cyber insecurity and actors adopting offensive postures could 'weaken the delicate balance and system of reciprocity that underpins much of the contemporary international security architecture'.[81] In particular, the goal of the strategy is to 'define how the United Nations system will support the use of these technologies to accelerate the achievement of the 2030 Sustainable Development Agenda and to facilitate their alignment with the values enshrined in the UN Charter, the Universal Declaration of Human Rights and the norms and standards of International Laws'.[82]

A potential development embedded in this message is the possibility of a more consolidated international dialogue on the relationship between new technologies and international development, peace, stability and security. The High-level Panel on Digital Cooperation, established by Guterres in July 2018, could become an essential platform for this international dialogue.[83]

Regardless of the level of operational capabilities and interests, there is a strong argument that responsibility for cybersecurity within a state rests entirely with that state. The Non-Aligned Movement, for instance, in its condemnation of any cyberattack or threat of cyberattack against peaceful nuclear facilities as a grave violation of the principles in the UN Charter and

[78] United Nations, A/C.1/72/PV.20 (note 51), p. 11.
[79] United Nations, A/73/PV.6 (note 32), pp. 3–4.
[80] United Nations, A/73/PV.6 (note 32).
[81] United Nations, *UN Secretary-General's Strategy on New Technologies* (United Nations: New York, Sep. 2018), p. 9.
[82] United Nations (note 81), p. 3.
[83] United Nations, 'Secretary-General's High-level Panel on Digital Cooperation', [n.d.].

international law, recognizes that the primary responsibility for nuclear safety rests with individual states.[84]

Consequently, having and implementing a national cybersecurity strategy is an essential feature of the informational self-determination of states. Without one, governments leave their populations and the ICT environment wide open to foreign influence. So far, 106 states have adopted national information security or cybersecurity policies and strategies that explicitly focus on the development of national capacity—the legal and institutional frameworks, capabilities and mechanisms that, among other things, protect critical infrastructure and combat cybercrime and develop skills, competences and performance.[85] Tracking the development of national strategies allows anticipation of the issues—such as privacy, human rights, cooperation and national responsibility—that are likely to be reintroduced into the UN dialogue agenda in the future.[86]

Conclusions

The discussions in the First Committee, and now in the UN General Assembly as a whole, on international cybersecurity and information security have become highly complex and opaque. The UN cybersecurity dialogue is likely to remain strongly polarized for the foreseeable future, allowing for only non-essential solutions. There is no short-term or simple remedy for cyberattacks by states or non-state actors. Indeed, the prevailing outlook, particularly among those focused on voluntary and non-binding norms, is that states need to accept a degree of cyber risk as well as the broad margins for interpretation of international law. This suggests that cyber issues fall predominantly within the remit of national resilience rather than an international regulatory framework.

The issue of international information security, or cybersecurity, is not about any past or previous process. The problems of today are not about differences over international law. They are not about cyberattacks or the GGE. They are about fundamental differences about the role of ICT in society, the role of states in shaping the use and development of technology, and the relationship between the state and the individual. They are also about a serious lack of robustness and resilience in the information systems deployed widely in support of societal, industrial and governmental

[84] United Nations, General Assembly, 72nd session, First Committee, 2nd meeting, A/C.1/72/PV.2, 2 Oct. 2017, p. 8. For a brief description and other details of the Non-Aligned Movement see annex B, section I, in this volume.

[85] Kerttunen, M. and Tikk, E., 'National cyber security strategies: Commitment to development', Cyber Policy Institute, Dec. 2018.

[86] For a normative reading of national cybersecurity strategies see Kerttunen, M. and Tikk, E., *A Normative Analysis of National Cyber Security Strategies* (European Union Institute for Security Studies: Paris, forthcoming 2019).

processes. Divergences in world views predate all cyber-related issues and are about fundamental and foundational differences between major powers. Due to unattended vulnerabilities, political differences are now prominently demonstrable in the ICT environment.

Given the highly strategic engagement between Russia and the USA, other governments must treat the security of ICT not as an isolated cyber policy issue, but as an issue of the utmost importance for national and international stability and security. However, resolving this security issue does not have to start from a conflict-prevention perspective. Robust national systems and processes and resilience will be key to eliminating the risk of opportunistic mainstream cyberattacks by focusing on the necessary safety aspects in the use of ICT. Advanced national approaches and experience will pave the way for a more focused dialogue on state-sponsored cyber operations and the relevant tolerance levels.

It is therefore essential for states to orient themselves in cyber concepts and processes, but also to acknowledge that they are just a current reflection of an old theme. The UN dialogue may already be shifting to a more inclusive and comprehensive digital agenda that promotes the harnessing of ICT for national and global development and moves away from the currently predominant Russian–US brinkmanship in and around the ICT environment.