V. Cyberspace and the malicious use of information and communications technology

ALLISON PYTLAK

Cyber risks and the malicious use of information and communications technology (ICT) continued to intensify throughout 2021, in keeping with the broader growth in harmful cyber activity that has occurred over the past several years. This intensification also mirrored the heightened dependence on ICT during the Covid-19 pandemic, in which a growing number of industries and individuals increasingly used digital networks and devices to work, study and socialize. The number of malicious cyber operations targeting food, energy, information supply chains and critical infrastructure increased in 2021—and with diverse and significant offline impacts.[1]

In 2021 it is estimated that, each week, one in every 61 organizations was affected by ransomware, and the global annual cost of cybercrime is estimated to have been US$6 trillion.[2] Furthermore, an estimated 486 million people were affected by intentional internet shutdowns in 2021, which was 80 per cent more than during 2020.[3] Disinformation and propaganda campaigns, often state sponsored, affected domestic political processes as well as pandemic responses, and there is growing awareness of the extent to which spyware is being used by authorities to repress human rights.[4] Humanitarian actors can also be negatively affected by cyber operations, such as those that target critical infrastructure and impede relief work.[5]

As attack surfaces in cyberspace—that is, the number of points vulnerable to attack—expand and the threat landscape grows more complex, more effective cyber governance mechanisms are needed, as are efforts to increase cyber capacity and build confidence. Although all countries agree that international law is applicable to cyberspace and related actions, the novel characteristics of the cyber context generate ambiguity and uncertainty about how individual states interpret the law. This complicates the ability of the international community to meaningfully respond to violations and

[1] Center for Strategic and International Studies (CSIS), 'Significant Cyber Incidents' tracker, [n.d.].

[2] 'As battle against cybercrime continues during Cybersecurity Awareness Month, Check Point Research reports 40% increase in cyberattacks', Check Point blog, Oct. 2021; and Morgan, S., 'Cybercrime to cost the world $10.5 trillion annually by 2025', Cybercrime Magazine, 13 Nov. 2020.

[3] Apps, P., 'From Kazakhstan to Ethiopia, the growing internet shutdown', *National Post*, 12 Jan. 2022.

[4] On how elections and the pandemic response were affected by disinformation and propaganda see University of Oxford, 'Programme on Democracy and Technology'.

[5] International Committee of the Red Cross (ICRC), 'Eight digital dilemmas debate: Cyber operations against humanitarian organizations', Oct. 2021.

hold perpetrators to account.[6] This is further compounded by the political implications that accompany the technical attribution of operations as well as the ongoing role of proxy actors within such operations. In addition, more governments are outlining national cybersecurity strategies and doctrines aimed at offensive or intrusive cyber operations.[7]

While the Covid-19 pandemic brought digital security threats more sharply into focus, it initially slowed efforts to further develop governance mechanisms.[8] However, in 2021 progress was made in relevant forums. Indeed, the virtual nature of meetings of relevant norm-setting bodies sometimes helped to facilitate broader and more diverse participation, although in a few contexts, meaningful participation remained difficult for non-governmental stakeholders.

Efforts to develop governance structures for ICT use and to achieve cyber-stability have developed through a patchwork of initiatives. Some have been state driven and based in the United Nations. Others have focused more on engaging with the technical community and private sector exclusively. Yet others have included a wider range of diverse stakeholders, including academia and civil society (e.g. the Global Commission on Stability in Cyberspace, the Paris Call for Trust and Security in Cyberspace, and the Cybersecurity Tech Accord). In varied yet largely reinforcing ways, these efforts have sought to elaborate deeper understandings about the applicability of international law to cyberspace or to establish norms and principles that can guide the behaviour of states and other actors.

This section outlines recent cyber governance initiatives at the multilateral, regional and national levels in turn, with a particular focus on current UN processes. This is followed by a description of non-governmental and collaborative initiatives.

[6] The applicability of international law, in particular the United Nations Charter, was first recognized by the 3rd UN Group of Governmental Experts on Developments in the Field of Information and Communications in the Context of International Security, in its consensus report of 2013 and later endorsed by the UN General Assembly. 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; and UN General Assembly Resolution 70/237, 23 Dec. 2015. Subsequent UN expert group reports and related General Assembly resolutions have reaffirmed this.

[7] Digital Watch, 'In context: The state of offensive cyber capabilities', Geneva Internet Platform, [n.d.].

[8] Richards, L., 'Cyberspace and the malicious use of information and communications technology', *SIPRI Yearbook 2021*, pp. 525–30.

Cyber governance structures within the United Nations

ICT in the context of international peace and security has been on the UN agenda since 1998, when Russia first tabled a resolution about 'information security' in the UN General Assembly's First Committee.[9]

Six UN Groups of Governmental Experts (GGEs) have been convened since 2004 to study the threats that come with the use of ICTs in the context of international security and to determine how these threats should be addressed.[10] Mandated by General Assembly resolutions adopted through the First Committee, the GGEs have reported their findings back to the UN membership. They have ranged in size from 15 to 25 states, and their meetings were always closed.

The report of the third group was welcomed for its breakthrough statement that international law is applicable to cyberspace.[11] The 2015 report of the fourth group set out 11 recommendations for state behaviour in cyberspace. The norms are concrete in setting out the positive actions that states should take—as well as actions to refrain from. Taken together, the norms variously do the following: highlight the applicability or recognition of existing law (i.e. to refrain from internationally wrong acts, and to respect human rights); indicate boundaries for items that should not be targeted or need protection (i.e. critical infrastructure and computer emergency response teams, supply chains); and encourage significant cooperation, information exchange and trust building (e.g. in response to incidents or for vulnerability disclosure).[12]

Amid intense politicization at the 2018 session of the First Committee, a sixth GGE was proposed, this time by the United States rather than Russia, the traditional sponsor.[13] The USA did so because Russia instead proposed creating the first ever open-ended working group (OEWG I) on cyber issues through a different resolution—'open' in the sense that all UN member states could participate.[14] Both the sixth GGE and OEWG I were established and commenced work in 2019.

[9] For more in-depth background on the UN cyber processes see Tiikk, E. and Kerttunen, M., 'Parabasis: Cyber-diplomacy in stalemate', Norwegian Institute of International Affairs (NUPI), 2018; Digitial Watch, 'UN GGE and OEWG', Geneva Internet Platform, [n.d.]; and UN Office for Disarmament Affairs (UNODA), 'Developments in the field of information and telecommunications in the context of international security', Fact sheet, July 2019.

[10] The timeframes of the six GGEs were as follows: first GGE (2004–2005), second GGE (2009–10), third GGE (2012–13), fourth GGE (2014–15), fifth GGE (2016–17), and sixth GGE (2019–21).

[11] United Nations, A/68/98 (note 6), para. 19.

[12] 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, 22 July 2015, A/70/174, para. 13.

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

[14] UN General Assembly Resolution 73/27, 'Developments in the field of information and telecommunications in the context of international security', 5 Dec. 2018.

Like most international diplomatic processes, the Covid-19 pandemic made it hard for the GGE and OEWG I to meet as planned in 2020 and conclude their work within their mandated time frames. Extensions were granted, and both switched to virtual and informal meeting formats to maintain momentum and advance discussion.[15]

OEWG I

In March 2021, OEWG I held its final substantive session in a hybrid format, with some delegates participating live in New York and others attending virtually.[16] The aim was to adopt a substantive final report by consensus, which would include conclusions, recommendations and reflection of discussions held across the six thematic areas under the OEWG's consideration: threats; international law; rules, norms and principles; capacity building; confidence-building measures (CBMs); and regular institutional dialogue.

OEWG I adopted a final report, in what was widely described as a win for diplomacy and multilateralism because of the flexibility and compromise demonstrated by participating member states.[17] As in any consensus process, however, no one was completely satisfied. Some states, mainly those in the West, were uncomfortable with some of the compromises made during the final meeting of the session. Iran disassociated itself from 'parts of the report that do not match with its principles and positions', and Israel also disassociated itself from any reference to the need for a legally binding instrument.[18] Concerns included the removal of the reference to the applicability of international humanitarian law from the negotiated part of the report; references to the ordering of the subsections on law and norms; references to certain aspects of the UN Charter; and about binding instruments, among other points.[19]

[15] On developments in 2020 see Richards, L., 'Cyberspace and the malicious use of information and communications technology', *SIPRI Yearbook 2021*, pp. 525–30.

[16] Documents, working papers and other materials from all the OEWG substantive sessions can be found online at <https://www.un.org/disarmament/open-ended-working-group/> and <https://reachingcriticalwill.org/disarmament-fora/ict/oewg>.

[17] The final report of the 2019–21 OEWG consists of 2 main parts: a non-negotiated chair's summary (annex II), which includes those elements of the draft report that could not be agreed by consensus, with an annex of language or textual proposals made throughout the process; and the negotiated substantive report (annex I) outlining the negotiated conclusions and recommendations. These were issued along with a procedural report. United Nations, General Assembly, Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/75/816, 18 Mar. 2021. An additional compendium of statements outlines positions on the final report. United Nations, General Assembly, Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Compendium of statements in explanation of position on the final report', A/AC.290/2021/INF/2, 25 Mar. 2021, Add.1, 14 Apr. 2021, and Add.2, 29 Nov. 2021.

[18] Pytlak, A., 'A win for diplomacy: Questions remain for cyber peace', *Cyber Peace & Security Monitor*, vol.1, no. 10 (17 Mar. 2021). Additional reporting and analysis of state positions can be found in other parts of the same edition of the *Monitor*.

[19] Pytlak (note 18).

Noteworthy aspects of the final OEWG I report include recognition of the potentially devastating humanitarian consequences of cyberattacks and acknowledging the impact of malicious ICT activity during the pandemic; progress on assessing the threat landscape (including attacks on health facilities and human rights implications); the reaffirmation of the applicability of international law, in particular the UN Charter, and of the normative framework; and agreement to implement several practical measures in the area of CBMs and capacity building.

Despite differences between states, the convening and conclusion of OEWG I was significant. It was the first time that a dialogue process on the subject of ICTs in the context of international peace and security had been convened by the UN, which made it possible for all states (regardless of size) to exchange views, begin to develop common understandings and identify gaps.[20] That the report, and by extension the wider UN membership, re-affirmed the outputs of the UN's five prior GGE's—which is referred to as the *acquis*—is important politically, even if it did not break new ground substantively.[21] Furthermore, over the course of OEWG I, multiple unique proposals were put forward by states and other stakeholders presenting suggestions about how to operationalize the UN cyber norms, for accountability mechanisms, and how to standardize information sharing, among others. While not all proposals were adopted or included in the final report, the process of developing and sharing these ideas helped to propel wider thinking and dialogue about cyber governance issues.

From OEWG I to OEWG II

One of the main points of contention among UN member states is about the future UN deliberations on international cyber governance and the form they will take. Cuba, Egypt, Russia and Venezuela, among others, have been calling for a legally binding instrument for many years. Some other states, including Costa Rica, Ecuador and Peru have indicated that they are open to developing a legal instrument, but not at this time. However, the majority of states—in particular, Australia, Canada, European Union (EU) members, Israel and the USA—believe that existing international law, coupled with the normative framework as developed within the UN, is sufficient to guide state behaviour in cyberspace. These differing views complicated how the

[20] It is not possible to include the full range of positions, proposals and dialogue that surfaced during the 2019–21 OEWG sessions. These can be accessed directly on the OEWG website, <https://www.un.org/disarmament/open-ended-working-group/>. Various civil society groups have also published reports and analysis. See e.g. Global Partners Digital, 'The OEWG's consensus report: Key takeaways', 18 Mar. 2021, DiploFoundation, 'What's new with cybersecurity negotiations? UN Cyber OEWG Final Report analysis', 19 Mar. 2021, and WILPF, *Cyber Peace & Security Monitor*, vol. 1, no. 10 (17 Mar. 2021).

[21] Gold, J., 'Unexpectedly, all UN countries agreed on a cybersecurity report. So what?', Council on Foreign Relations, 18 Mar. 2021; and ICT4Peace, 'The OEWG final report: Some progress, much remains unresolved', Mar. 2021.

section on 'regular institutional dialogue' was presented in the final report of OEWG I.[22] The politics around these different perspectives also underpin various other initiatives that are now the main vehicles for advancing cyber governance at the UN.

This is particularly relevant to the establishment of the UN's second OEWG on ICT (OEWG II), which was agreed during the 2020 session of the First Committee and before OEWG I had completed its work.[23] At the time, many states voted against or abstained from the Russia-led resolution, on the basis that the creation of a successor body was premature and would prejudge the outcomes of the OEWG in progress.[24] Nonetheless, the resolution secured sufficient votes to be adopted. OEWG II has a longer time frame (2021–25) than OEWG I, which is a source of concern to those who do not want to wait five years for the UN to adopt decisions or act on what is an increasingly pressing security matter.

In addition, a proposal introduced by Egypt and France in 2020 to develop a politically binding programme of action (POA) on state behaviour in cyber space has now been endorsed by more than 50 states.[25] Inspired somewhat by the UN Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspect (on which see section I), the initial proposal was articulated during 2021 through working papers submitted to the OEWG I by Egypt and France, and informal discussion among its supporters.[26] Generally, POA-supporting states suggest that the instrument could reflect the *acquis*, be action-oriented rather than deliberative, and become a mechanism to facilitate capacity building. OEWG II could be a space to further develop thinking around a POA, but there is also a concern that doing so might see the POA proposal being stunted by those who do not support it. It is not yet clear if a negotiation mandate for a POA will be sought at the 2022 session of the First Committee or if another avenue will be pursued.

OEWG II held its first substantive session in December 2021, chaired by Ambassador Burhan Gafoor of Singapore. It mainly focuses on the same six thematic topics as its predecessor. At the December 2021 session, many states

[22] United Nations, A/75/816 (note 17), annex I, paras 68–79.

[23] Note that the name of OEWG II is slightly different than that of OEWG I: 'Open-ended Working Group on *security of and in the use of* information and communications technologies 2021–2025'.

[24] United Nations, General Assembly, First Committee, 'Developments in the field of information and telecommunications in the context of international security', Draft resolution, A/C.1/75/L.8/Rev.1, 26 Oct. 2020.

[25] United Nations, Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 'The future of discussions on ICTs and cyberspace at the UN', Submission by France and others, 2 Dec. 2020.

[26] United Nations, 'Working paper for a Programme of Action (POA) to advance responsible state behaviour in the use of ICTs in the context of international security', Dec. 2021; and Pytlak, A., *Programming Action: Observations from Small Arms Control for Cyber Peace* (Women's International League for Peace and Freedom: New York, Feb. 2021).

emphasized two important points about the second OEWG: that it should be action oriented; and that they should not be required to wait until the end of its mandate to make decisions or produce results. Many also stressed the need for exchange about how international law is being applied in national cyber strategies and action.[27]

The sixth GGE on responsible state behaviour in cyberspace

In May 2021 the sixth GGE released its final report as well as a compendium containing national views about how international law applies to state use of ICT, which had been submitted on a voluntary basis.[28] The report is notable for providing additional layers of understanding and guidance for implementing the UN norms. This is done through the inclusion of explanatory or contextual information in relation to each norm, as well as recommended actions for their implementation.

By taking this approach, the report provides an updated assessment of ICT threats, including references to the Covid-19 pandemic and operations targeting health infrastructure; considers some of the complexities relating to technical and political attribution; describes what states might consider as critical infrastructure; gives significant consideration to protecting supply chain integrity; and provides specific actions to take as confidence- and transparency-building measures and in capacity building. The perennially thorny issue of the applicability of international humanitarian law was partially resolved, in that states 'took note' of its applicability only in situations of armed conflict; agreed to further study the applicability of the principles of international humanitarian law; and recalled that these principles do not legitimize or encourage conflict.

The sixth GGE was also more consultative than its predecessors, having held a series of regional consultations for non-group members, some of which were also open to non-governmental stakeholders.

Participation by non-governmental stakeholders

An issue that has dominated both OEWGs is the participation of non-governmental stakeholders in formal meetings. Ahead of the first OEWG session, in 2019, all organizations that lacked accreditation from the UN Economic and Social Council (ECOSOC) had their requests to participate anonymously vetoed; this pattern was repeated ahead of the second session,

[27] United Nations, Open-ended Working Group on security of and in the use of information and communications technologies, 1st substantive session, Statements, 13–17 Dec. 2021.

[28] United Nations, General Assembly, 'Report of the group of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security', A/76/135, 14 July 2021; and 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by states', submitted by participating governmental experts in the GGE, A/76/136, 13 July 2021.

in 2020. Such a blanket rejection is extremely rare in General Assembly-based forums and generated significant concern, particularly given the significant role that non-governmental stakeholders, including the private sector, play in the ICT environment. No official reason for the accreditation denials was provided; most assume it was either politically motivated or because objecting states prefer to limit the role of civil society, including the private sector, generally. Throughout the OEWG I process and especially in 2021, some governments worked with civil society and the private sector to organize informal opportunities for stakeholders to input their views, and its chair was also receptive to creating such opportunities.[29]

During the June 2021 organizing meeting for OEWG II, Canada and other states requested greater transparency in the accreditation process and, ultimately, improved stakeholder access to future formal OEWG meetings.[30] These requests were not taken on board by the incoming OEWG II chair when he outlined meeting modalities ahead of the December 2021 session. Dozens of states protested these modalities when the session was convened on 13 December, stalling the adoption of the session's agenda, and the topic became the focus of informal consultations throughout the week.[31] As of early 2022, a compromise had not been reached on this matter (in relation to the OEWG's second session, in March 2022), and the continued sidelining and exclusion of relevant civil society stakeholders risked damaging OEWG II's credibility and its practical impact in the world outside the UN.

Finally, it is worth noting how other parts of the UN system are addressing cyber-related topics. First, Estonia convened the first ever UN Security Council open debate on cybersecurity in June 2021.[32] Second, the International Telecommunication Union (ITU) is providing technical coordination and standards development. Third, a process is underway to negotiate a new treaty on cybercrime, initiated in the General Assembly's Third Committee (the Social, Humanitarian and Cultural Committee).[33] Fourth, human rights bodies have adopted resolutions or issued statements of concern regarding the human rights impact of digital technologies over recent years; notably, in 2021 the UN Working Group on Mercenaries

[29] One example is the Let's Talk Cyber Initiative, <https://letstalkcyber.org/>.

[30] Pytlak, A., 'Building on—and establishing—foundations', *Cyber Peace & Security Monitor*, vol. 2, no. 1 (3 June 2021), pp. 3–4.

[31] Pytlak, A., 'Summary: Civil society participation modalities', *Cyber Peace & Security Monitor*, vol. 2, no. 3 (21 Dec. 2021), pp. 3–6.

[32] Permanent Mission of Estonia to the United Nations, 'Maintaining international peace and security in cyberspace', Concept Note to the UN Security Council High-level Open Debate on Cyber Security, 29 June 2021.

[33] UN Office on Drugs and Crime, 'Ad-Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes', [n.d.].

published a report on cyber mercenaries and human rights.[34] Finally, the UN secretary-general gave priority to reducing cyber risks in 'Our Common Agenda', released in September 2021, where he also referenced the need for a ban on cyberattacks against civilian infrastructure.[35]

Regional cyber governance initiatives

Regional efforts at cyber governance have the potential to be somewhat less politically challenging than those that are global, and it is widely recognized that existing regional good practice should be built upon and accounted for within global initiatives. This point was made repeatedly by states and other actors during many of the multilateral forums described above. In some regions, collaboration has been more practical and technical (rather than political), particularly given the transboundary nature of ICT threats and infrastructure. Elsewhere, activities have focused on building common policies and understanding. The following examples of recent developments or events are meant to illustrate recent regional initiatives, but are by no means exhaustive.

The Association of Southeast Asian Nations (ASEAN) has long been active in coordinating around cyber issues, particularly in building resilience and protecting critical infrastructure.[36] The ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) was established in late 2020 and is mandated to work across sectors on cybersecurity issues. ASEAN holds annual ministerial conferences on cybersecurity issues and has recently launched a regional action plan on the implementation of the norms of responsible state behaviour in cyberspace, in line with UN norms.[37] South East Asia is also home to two cybersecurity centres of excellence, in Bangkok and Singapore.

In June 2021 South Korea and the Organization for Security and Co-operation in Europe (OSCE) co-convened the third Inter-Regional Conference on Cyber/ICT Security.[38] In 2013 the OSCE began developing a

[34] United Nations, General Assembly, 'The human rights impacts of mercenaries, mercenary-related actors and private military and security companies engaging in cyberactivities', Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, A/76/151, 15 July 2021.

[35] United Nations, *Our Common Agenda*, Report of the secretary-general (United Nations: New York, 2021).

[36] Van Raemdonck, N., 'Cyber diplomacy in Southeast Asia', EU CyberDirect, May 2021.

[37] Yu, E., 'Asean champions regional efforts in cybersecurity, urges international participation', ZD Net, 6 Oct. 2021.

[38] Organization for Security and Co-operation in Europe (OSCE), 'Cyber/ICT security between OSCE and Asian regions focus of OSCE and Republic of Korea-hosted discussion', 24 June 2021.

set of cyber CBMs, of which there are now 16.[39] It launched a new training course on these measures in March 2021.[40]

In line with the above example, a growing number of cross-regional initiatives focus particularly on cyber capacity building. One example is the Latin America and the Caribbean Cyber Competence Centre (LAC4), which was established in 2021 in Santo Domingo as a collaboration with the EU's CyberNet to build ICT capacity in Latin America and the Caribbean. The EU published a cybersecurity strategy in late 2020 not only to focus on building resilience but also to lead dialogues on international norms and standards. In 2021 the EU joined the Paris Call.[41]

National cyber initiatives and policy

A growing number of states publish national policies and strategies on issues ranging from preventing and addressing cybercrime via data protection to building the resilience and capacity to respond to cyber threats. For most, this has necessitated creating new governmental entities to oversee or implement relevant initiatives; passing legislation; refining public–private partnerships; and developing bilateral cooperation agreements with other states.[42] In 2021 the ITU published the fourth edition of its Global Cybersecurity Index, which tracks a range of national efforts including governance and coordination mechanisms within countries that address cybersecurity.[43]

Throughout 2021 the UN Institute for Disarmament Affairs (UNIDIR) continued to update its Cyber Policy Portal, which provides the profiles of the national cyber policy documents of all UN member states, various intergovernmental organizations and multilateral frameworks.[44]

The evolution of national offensive cyber strategies and policies—often in connection with other military tactics or strategies—is also relevant to international cyber governance efforts. In general, it is difficult to determine the precise number of states with offensive cyber capabilities, in part because defining what that means is a matter of debate, and in part because of the intrinsically non-transparent nature of the subject. A few states have openly explained how they understand the term and their intentions around them,

[39] Organization for Security and Co-operation in Europe (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.

[40] Organization for Security and Co-operation in Europe (OSCE) Secretariat, 'New e-learning course on OSCE cyber/ICT security confidence-building measures now available', 22 Mar. 2021.

[41] European Commission, 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient', 16 Dec. 2020.

[42] Calam, M. et al., 'Asking the right questions to define government's role in cybersecurity', McKinsey & Company, 19 Sep. 2018.

[43] International Telecommunication Union, 'Global Cybersecurity Index 2020', 2021.

[44] UNIDIR Cyber Policy Portal, <https://unidir.org/cpp/en/>.

including Australia, France, Germany and the USA.[45] While it could be argued that there is a benefit in states being transparent about their cyber abilities, the growing spread of offensive capabilities—if they can be neatly defined as such—raises other concerns about cyber-related militarism and the weaponization of technology. Moreover, two nuclear-armed states, the United Kingdom and the USA, have indicated in recent years that they would consider responding to a highly destructive cyber incident with nuclear weapons.[46] In 2021, UNIDIR launched a research paper series to consider the national doctrines and cyber capabilities of 15 countries across diverse global regions, which has aided in facilitating transparency among states.[47]

Towards the end of 2021 and in connection with the December 2021 session of the OEWG II, a few states (including China, Estonia, France and Italy) provided national views on how specific legal principles apply in cyberspace.[48] Others indicated during the session that they are engaging in domestic processes to outline these views. Clarifying how, at a national level, states understand and interpret international law as relevant to cyber actions was a recommendation from OEWG I and the sixth GGE and will therefore be important for ongoing cyber governance efforts.

Non-governmental and collaborative initiatives

A range of non-governmental actors are currently undertaking diverse initiatives to deepen understandings of cyber norms, governance and legal questions, which are sometimes carried out in partnership with states or international organizations.

[45] Relevant resources for comparative analysis include a 2021 survey from the International Institute for Security Studies that assesses how 15 states approach cyber capability in the context of power. International Institute of Security Studies (IISS), *Cyber Capabilities and National Power: A Net Assessment* (IISS: London, [2021]). The Belfer Center at Harvard University publishes an annual Cyber Power Index that measures 30 countries' cyber capabilities in the context of 7 national objectives. Voo, J. et al., *National Cyber Power Index 2020: Methodology and Analytical Considerations* (Belfer Center for Science and International Affairs: Cambridge, MA, Sep. 2020). On the countries mentioned in the text see Hansen, F. and Uren, T., 'Australia's offensive cyber capability', The Strategist, 10 Apr. 2018; Schultze, M. and Herpig, S., 'Germany develops offensive cyber capabilities without a coherent strategy of what to do with them', Council on Foreign Relations, 3 Dec. 2018; Stroebel, W. P., 'Bolton says US is expanding offensive cyber operations', *Wall Street Journal*, 11 June 2019; and Parly, F., French Minister of Armed Forces, 'Stratégie cyber des Armées' [Cyber strategy of the armed forces], Speech, Paris, 18 Jan. 2019.

[46] US Department of Defense (DOD), *Nuclear Posture Review 2018* (DOD: Arlington, VA, Feb. 2018); and British Parliament, House of Commons Library, 'Integrated Review 2021: Increasing the cap on the UK's nuclear stockpile', Briefing Paper no. 9175, 21 Mar. 2021.

[47] Kastelic, A., *International Cyber Operations: National Doctrines and Capabilities*, International Cyber Operations Research Paper Series no. 1 (UN Institute for Disarmament Research (UNIDIR): Geneva, 2021).

[48] United Nations, Open-ended Working Group on security of and in the use of information and communications technologies, 'Member State views and inputs', 2021.

The Global Commission on the Stability of Cyberspace is a multi-year, multi-stakeholder and non-UN process that produced a set of eight norms of responsible cyber behaviour. It launched a new paper series in 2021 that focuses on cyberstability and explores the expanding 'constellation' of related cyber initiatives and changing conditions in cyberspace.[49]

The Cybersecurity Tech Accords bring together more than 150 technology companies under a common commitment to protect cyberspace. In 2021 and in collaboration with the Paris Call, it advocated for improved stakeholder access to the UN cyber processes, as based on experiences with multistakeholder governance models.[50]

The Cooperative Cyber Defence Centre of Excellence (CCDCOE) of the North Atlantic Treaty Organization (NATO), the International Committee of the Red Cross (ICRC) and other partners provided a 2021–22 update to their collaborative Cyber Law Toolkit.[51] Based on 25 hypothetical scenarios, the toolkit is an interactive web-based resource for legal professionals who work at the intersection of international law and cyber operations.

Established in 2020, the Oxford Process on International Law Protections in Cyberspace is an initiative of the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) and Microsoft. It has identified five statements on international law protections that consider how international law applies to specific sectors and objects.[52] The fourth and fifth of these statements, on the Regulation of Information Operations and Activities, and on Ransomware Activities, were developed in 2021.

Another ongoing initiative is the Tallinn 3.0 process. The process seeks to update the *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* and reflect on current state practice regarding cyber operations. The new manual will consider activities and statements delivered in international forums, such as the UN processes, alongside academic publications and multistakeholder initiatives.[53] The project is hosted by the CCDCOE, although the earlier manuals have not been endorsed as NATO documents. The *Tallinn Manual 3.0* is anticipated to be released in 2025–26.[54]

A prominent message from many civil society actors following the UN and other multilateral cyber governance processes in 2021 has been their

[49] Klimburg, A. (ed.), *New Conditions and Constellations in Cyber* (The Hague Centre for Strategic Studies. The Hague, Dec. 2021).

[50] 'The third anniversary of the Paris Call and results from Working Group 3: Advancing a multistakeholder approach', Cybersecurity Tech Accord, Nov. 2021.

[51] Cyber Law Toolkit, 2021/22 update.

[52] Oxford Institute for Ethics, Law and Armed Conflict (ELAC), 'The Oxford process on international law protections in cyberspace', University of Oxford, May 2020.

[53] NATO Cooperative Cyber Defence Centre of Excellence, 'CCDCOE to host the Tallinn Manual 3.0 process', 2020.

[54] Dunlap, C., 'International law and cyber ops: Q & A with Mike Schmitt about the status of Tallinn 3.0', 3 Oct. 2021, Lawfire blog.

call for human-centric approaches to cybersecurity and governance. A human-centric approach builds on earlier relevant concepts of 'human security' and 'humanitarian disarmament' by questioning whose security is at the core of policy and normative efforts and, within that, seeking to better highlight—and prevent—the human cost of cyber operations.[55] This approach also aligns with the protection of human rights and fundamental freedoms even when considering cyber operations within the framing of 'international peace and security', much in the way that conventional arms control instruments are increasingly motivated by humanitarian concerns (see section I). Subsequently, documenting and exploring the human cost of cyber operations is becoming more of a focus for some non-governmental actors and is likely to influence their inputs into cyber governance and norm-building processes.[56]

Within the push for human-centric approaches to cyber governance is a growing interest in addressing the gendered impact of cyber operations and the gender dimensions of cyber diplomacy more broadly. In 2021 a diverse range of publications and capacity-building activities sought to advance earlier research on this subject, and the final OEWG I report included recognition of women's participation in cybersecurity, with some governments having advocated for more specific recommendations in this area.[57] This is in line with increased support for addressing the gender dimensions of violence and conflict in other weapon-related forums.

Conclusions

While 2021 is generally considered to have been a productive year for cyber governance mechanisms, real-world events overtook the pace of diplomacy and multilateralism. The ability of existing frameworks to prevent cyber harm and maintain cyber peace and stability is being severely tested. There are ample normative frameworks, as well as guidelines within existing law, for state behaviour and the governance of ICTs.[58] This is not the ungoverned and unruly sphere it is sometimes portrayed as. However, further clarity

[55] E.g. Deibert, R. J., 'Toward a human-centric approach to cybersecurity', *Ethics and International Affairs*, Dec. 2018; and Kumar, S., 'The missing piece in human-centric approaches to cyber norms implementation: The role of civil society', *Journal of Cyber Policy*, vol. 6, no. 3 (2021).

[56] E.g. CyberPeace Institute, 'Cyber Incident Tracer #HEALTH',.

[57] United Nations, A/75/816 (note 17), annex I, para. 12 and annex II, para. 37. See also e.g. Millar, K., Shires, J. and Tropina, T., *Gender Approaches to Cybersecurity: Design, Defence and Response* (UN Institute for Disarmament Research: Geneva, 2021); and Sharland, L. et al., *System Update: Towards a Women, Peace and Cybersecurity Agenda* (UN Institute for Disarmament Research: Geneva, 2021).

[58] For an overview of the frameworks and how they overlap see Brown, D., Esterhuysen, A. and Kumar, S., *Unpacking the GGE's Framework on Responsible State Behaviour: Cyber Norms* (Association for Progressive Communications and Global Partners Digital: 2019); and the Carnegie Endowment for Peace, 'Cyber norms index and timeline', [n.d.].

on some core legal questions is required, as is improved transparency and capacity building.

Bringing the diverse patchwork of existing frameworks together under a single roof—perhaps via a UN programme of action—could help to create an environment with greater potential for accountability mechanisms and transparency. Calls for accountability mechanisms are growing stronger, particularly from the non-governmental community. Yet what will ultimately be most crucial for the effectiveness of any governance model are trust and political will.