II. Governance of cyberspace and the malicious use of information and communications technology

ALLISON PYTLAK

Information and communications technology (ICT) continued to play an active role in the foreign policy and military activities of states and other actors in 2023. In keeping with the recent general trend, governments appear to be predominantly using their cyber capabilities in combination with, or to complement, other tools, mechanisms and activities applied to the pursuit of various objectives. Cyber capabilities are certainly being used destructively in war and conflict, and much has been written and documented about this in the context of the Russia–Ukraine war; but they are also being leveraged in peacetime or in the context of long-standing rivalry and competition between nations not at war. Such use includes disruptions to critical infrastructure, espionage and data theft, as well as operations affecting electoral processes.

The scope and nature of cyber threats are also evolving. The impact of artificial intelligence (AI) on cybersecurity was a hot-button topic in 2023, as it was for many other facets of daily life (see section I). Many consider AI a double-edged sword when it comes to cybersecurity, with the potential to both improve cyber defence and make attacks and malicious activity more harmful and impactful. In addition, researchers and governments are turning greater attention to the intersection between outer space and cyber space. The interconnection in practice between these two domains means that there are shared threats but also shared scope for resilience efforts and governance.[1]

Cyber governance exists through a patchwork of measures and initiatives implemented at multiple levels and involving multiple actors. While in some instances this enables greater precision and more focused response, it can also lead to governance gaps. It can also be said that while some of the tools in the diplomatic box are good ones, a lack of consistent implementation or consequences is contributing to a growing accountability deficit.

This section presents a non-exhaustive overview of key cyber events and trends in 2023, including how cyber capabilities played a role not only in armed conflict but also in peacetime operations and relations among states. It then provides a summary of developments in cyber governance at international, regional and other levels, including some relevant activities of non-governmental stakeholders.

[1] On space governance see section III of this chapter.

General trends in the malicious use of ICT

Cyber operations in warfare: Russia–Ukraine and Israel–Hamas wars

The role of cyber operations in the Russia–Ukraine war again constituted a relevant dimension of the conflict in 2023, although to a lesser extent than in the preceding year.[2] The volume of destructive attacks that characterized the early stages of the full-scale invasion in February 2022 declined, with Microsoft reporting that 'Nearly 50 percent of destructive Russian [cyber] attacks [it] observed against Ukrainian networks occurred in the first six weeks of the war'.[3] As in 2022, however, the CyberPeace Institute reported that the most commonly targeted sectors were public administration, media and ICT, followed by finance and trade, with distributed denial of services (DDoS) operations accounting for the vast majority of all known incidents in 2023.[4] The Institute also recorded that website defacements became a more prevalent form of activity against Russian entities from within Ukraine, and that on both sides of the conflict there were notable shifts in the actors and entities engaging in operations during 2023.[5] In April 2023 Russia accused North Atlantic Treaty Organization (NATO) countries, including the United States, of launching more than 5000 cyberattacks from Ukrainian territory against its critical infrastructure since 2022.[6] Other analysis noted a shift in 2023 towards greater targeting of Ukraine's allies through malicious cyber activity of various kinds affecting Canada, New Zealand, Poland, Switzerland and NATO, among others.[7]

One notable exception to the decline in aggressive cyber behaviour was a high-profile incident in December 2023 involving Kyivstar, Ukraine's largest telecommunications operator, which supplies over half of Ukraine's population with mobile phone and internet services. The incident reportedly disrupted air-raid sirens, banks, ATMs and point-of-sale terminals, and left

[2] On the Russia–Ukraine war see chapter 1, chapter 2, section I, and chapter 10, sections II and III, in this volume.

[3] Microsoft Threat Intelligence, *Microsoft Digital Defense Report 2023* (Microsoft: Oct. 2023), p. 48.

[4] CyberPeace Institute, *Cyber Dimensions of the Armed Conflict in Ukraine: Quarterly Analysis Report, Q3 July–September 2023* (CyberPeace Institute: Geneva, Dec. 2023), p. 3. A DDoS operation involves the attacker flooding a server with internet traffic to prevent users from accessing connected online services and sites.

[5] CyberPeace Institute (note 4), p. 9.

[6] Toulas, B., 'Russia accuses NATO of launching 5,000 cyberattacks since 2022', *Bleeping Computer*, 14 April 2023.

[7] Mueller, G. B. et al., 'Cyber operations during the Russo–Ukrainian war: From strange patterns to alternative futures', Centre for Strategic and International Studies (CSIS), 13 July 2023; Blackwell, T., '"Trudeau's being cocky": Russian hackers claim attacks on PM, Pearson airport and others', *National Post*, 14 Apr. 2023; 'Parliament of New Zealand cyber attack by NoName in response to sanctions against Russia', *Cyber Express*, 17 July 2023; Greenberg, A., 'The cheap radio hack that disrupted Poland's railway system', *Wired*, 27 Aug. 2023; 'Swiss websites hit by DDoS attack ahead of Zelenskiy video address', Reuters, 12 June 2023; and Millar, M. and Cerulus, L., 'How Russian hackers targeted NATO's Vilnius summit', Politico, 21 Aug. 2023.

Kyivstar users without mobile signal or the ability to use the internet. The Ukrainian bank Monobank was targeted with a DDoS attack at the same time, disrupting access to the bank's website. The British Ministry of Defence described the incident as 'one of the highest-impact disruptive cyber-attacks on Ukrainian networks since the start of Russia's full-scale invasion'.[8]

The prominent role of non-state actors in conducting cyber operations on both sides of the Russia–Ukraine war, whether state-supported proxies or patriotic civilian hackers, is contributing to what the International Committee of the Red Cross (ICRC) described as a 'worrying trend' which gained more visibility in 2023.[9] The ICRC observed that the rise of civilian hackers and the greater role of the private sector in cyber operations during an armed conflict blurred the line between who is a civilian and who is a combatant, potentially resulting in the loss of legal protections for civilians. In October 2023 the ICRC issued eight rules for civilian hackers during war, and four obligations for states to restrain them, drawing mixed reactions globally.[10]

Another notable observation about the role of ICT in the Russia–Ukraine war concerns the growth in misinformation and influence operations. While this is not a new tactic, ICT and other technologies accelerate their spread and can deepen their impact.[11]

Cyber operations also played a role in the renewed conflict between Israel and Hamas that broke out on 7 October 2023 and was still ongoing as at the end of December 2023.[12] Evidence suggests that much of the activity to date has been DDoS attacks and website defacements, along with dis- and misinformation campaigns, against both parties to the conflict.[13] Cloudflare reported that Israeli news media websites were the main target, with 56 per cent of the reported DDoS attacks carried out against them, the most notable being the operation claimed by Anonymous Sudan.[14] Other Israeli sectors being targeted included ICT, education, energy, finance, public administration and transportation.[15]

Diverse Palestinian entities and industries were also targeted by cyber operations. The CyberPeace Institute identified two confirmed DDoS attacks against two non-governmental organizations offering civilian

[8] See e.g. British Ministry of Defence, 'Latest Defence Intelligence update on the situation in Ukraine', X, 16 Dec. 2023, <https://twitter.com/DefenceHQ/status/1735993232247476720>.

[9] Rodenhauser, T. and Vignati, M., 'Eight rules for "civilian hackers" during war, and 4 obligations for states to restrain them', Humanitarian Law & Policy Blog.

[10] Rodenhauser. and Vignati (note 9); and Tidy, J. 'Rules of engagement issued to hacktivists after chaos', BBC, 3 Oct. 2023.

[11] Microsoft Threat Intelligence (note 3), p. 48.

[12] On the Israel–Hamas war see chapter 1, chapter 2, section I, and chapter 10, section II, in this volume.

[13] Scroxton, A., 'What are the cyber risks from the latest Middle Eastern conflict?', *Computer Weekly*, 18 Oct. 2023.

[14] Schappert, S., 'Anonymous Sudan targets Israel premier and Mossad', *Cyber News*, 15 Nov. 2023.

[15] Wagner, T., 'Escalation of threats in the Middle East', CyberPeace Institute Blog, 6 Nov. 2023.

services to Palestinians.[16] Lack of stable internet connectivity also affected the civilian population in Gaza, something that was already a challenge prior to the outbreak of hostilities. Israeli military operations including airstrikes affected both telecommunications and internet services and led to a complete shutdown of these services on 27 October 2023.[17] The communications blackout was condemned by human rights groups and other actors.[18] Such condemnation reflected growing concerns about the impact of internet shutdowns in other parts of the world in 2023, especially in places of crisis or political instability.[19]

Cyber espionage

Outside of armed conflict, states used their cyber capabilities to pursue various objectives in 2023. Some analysts noticed a shift towards a greater use of cyber capabilities for longer-term intelligence-gathering operations and espionage, with fewer large-scale or one-off 'attacks' occurring. One of the higher profile examples is Microsoft's discovery of a Chinese cyber espionage campaign that enabled one of China's proxy actors, the Storm-0558 group, to gain access to customer email accounts in May 2023. Accessed accounts included the US secretary of commerce and the US ambassador to China, among other employees in the US departments of State and Commerce, and in other government agencies. It is estimated that a total of 60 000 emails were stolen from 10 accounts belonging to the US Department of State.[20]

Some analysts have observed a higher level of sophistication in the techniques and operations being utilized by middle power states. Microsoft, for example, observed that 'Iranian and North Korean state actors are starting to close the gap with nation-state cyber actors such as Russia and China'.[21] Another organization documented how the main Iranian advanced persistent threat (APT) groups employed more advanced and sophisticated phishing attacks in 2023, with newer malware, to target entities in the USA and Saudi Arabia, and to conduct cyber espionage activities in sectors such as satellite, defence and pharmaceuticals.[22] Cyber operations against India attributed to Pakistan continued to intensify in 2023 in the context of the rivalry between the two countries.[23]

[16] Wagner (note 15).

[17] Burgess, M., 'The destruction of Gaza's internet is complete', *Wired*, 27 Oct. 2023.

[18] AFP, 'Gaza info blackout "risks providing cover for mass atrocities": HRW', *Economic Times*, 28 Oct. 2023.

[19] As of May 2023, Access Now had preliminarily identified at least 80 shutdowns across 21 countries in 2023; 18 of these shutdowns were ongoing since 2022. See 'Who is shutting down the internet in 2023? A mid-year update', Access Now, 31 July 2023.

[20] Heiligenstein, M. X., 'Microsoft data breaches: Full timeline through 2023', *Firewall Times*, 28 Sep. 2023.

[21] Microsoft Threat Intelligence (note 3), p. 50.

[22] Cyfirma, 'APT quarterly highlights—Q3: 2023', 2 Nov. 2023.

[23] See CSIS, 'Significant cyber incidents', Timeline, [n.d.].

Microsoft also reported a surge in operations and activities focused on Latin America and sub-Saharan Africa in 2023.[24] For instance, Ecuador's national election agency claimed that cyberattacks traced to Bangladesh, China, India, Indonesia Pakistan, Russia and Ukraine caused difficulties for absentee voters during its 2023 general election.[25]

Cybercrime

Cybercrime activity continued apace in 2023. While a significant portion of cybercrime activities affect individuals and private entities, they can also have implications for international peace and security. Speaking at a session of the United Nations open-ended working group (OEWG) on ICT in December 2023, the representative of Germany observed that when cybercrime crosses a certain level of severity it can pose a threat to national and international security.[26] Following a series of ransomware operations targeting government agencies of Trinidad and Tobago earlier in the year, its prime minister described a November 2023 cybercrime incident as a 'national security threat'.[27] The MOVEit hack, widely considered to be among the more significant cyber events of 2023, affected over 2000 organizations, 'with data thefts affecting more than 62 million people'.[28] This included personal data held by public sector entities in Canada, the United Kingdom and the USA, adversely impacting trust in those institutions and hampering their ability to operate.

The Democratic People's Republic of Korea (DPRK, North Korea) has regularly funded its illicit weapons development programme through cryptocurrency theft and other cybercrime.[29] In 2023 this prompted Japan, the Republic of Korea (South Korea) and the USA to establish a new trilateral working group 'to combat DPRK cyber threats and block its cyber-enabled sanctions evasion'.[30] In December 2023 South Korea placed sanctions on the head of North Korea's intelligence services and seven other individuals for 'earning foreign currency through illegal cyber activities and technology

[24] Microsoft Threat Intelligence (note 3), p. 51.

[25] 'Alleged cyberattacks mar online voting in Ecuador', DigWatch Update, 22 Aug. 2023.

[26] See United Nations, Open-ended Working Group on ICT, Sixth substantive session, First meeting, 11 Dec. 2023, UN Web TV, 01:58:20.

[27] 'Trinidad's state telecoms company hit by cyberattack', Caribbean Council, 17 Nov. 2023.

[28] Davis, W., 'MOVEit cyberattacks: Keeping tabs on the biggest data theft of 2023', *The Verge*, 11 Nov. 2023; see also Page C., 'MOVEit, the biggest hack of the year, by the numbers', TechCrunch, 26 Aug. 2023.

[29] Gramer, R. and Iyengar, R., 'How North Korea's hackers bankroll its quest for the bomb', *Foreign Policy*, 17 Apr. 2023.

[30] White House, 'The spirit of Camp David: Joint statement of Japan, the Republic of Korea, and the United States', Briefing Room Statement, 18 Aug. 2023.

theft' to 'generate revenue for the North Korean regime and procuring funds for its nuclear and missile activities'.[31]

Surveillance software and cyber mercenaries

There were numerous revelations about the use of surveillance software (spyware) throughout 2023. While past reports and research have tended to spotlight the targeting of various civil society actors by states, much of the research released in 2023—particularly relating to the use of the Predator spyware developed and marketed commercially by the Intellexa alliance—revealed the extent to which political leaders were also targeted and affected. An October 2023 report from Amnesty International detailed the findings of an investigation which focused on a spyware operation by an Intellexa customer that targeted social media accounts between February and June 2023.[32] Targets of the operation included a Berlin-based independent news website, political figures in the European Parliament, the European Commission, academic researchers and thinktanks, while attempted targets included UN officials, the president of Taiwan, US senators and representatives, and other diplomatic authorities.[33] The report argued that Predator spyware and its rebranded variants should be permanently banned because they are highly invasive and able to access unlimited amounts of data, and are therefore not human rights compliant. A separate Citizen Lab report published with data from Microsoft Threat Intelligence exposed how hacking tools from an Israeli firm were used against journalists, as well as against opposition figures and organizations across at least 10 countries, including in North America and Europe, leading to the closure of the firm in 2023.[34]

Global developments in cyber governance

Cyber governance in 2023 continued to develop and exist through a patchwork of initiatives, many of which are mutually reinforcing. Some are state-driven and rooted in existing international organizations and structures, open in varying degrees to the participation of non-governmental stakeholders. Others are focused more on the roles and responsibilities of the technical community and private sector. In varied yet largely complementary ways, these efforts have sought to elaborate deeper understandings about the applicability of international law to cyberspace or to establish norms and

[31] 'South Korea sanctions North Korean spy chief over illicit cyber activities', Al Jazeera, 27 Dec. 2023.

[32] Amnesty International, *The Predator Files: Caught in the Net—The Global Threat from 'EU Regulated' Spyware* (Amnesty International: London, Oct. 2023), p. 9.

[33] Amnesty International (note 32), p. 10.

[34] Marczak, B. et al., 'Sweet QuaDreams: A first look at spyware vendor QuaDream's exploits, victims, and customers', Citizen Lab, 11 Apr. 2023.

principles that can guide the behaviour of states and other actors. Below are several noteworthy developments in 2023.

UN cybercrime treaty process

Since May 2021 UN member states have been negotiating an international treaty to counter cybercrime through an ad-hoc committee (AHC) tasked with developing a 'comprehensive international convention on countering the use of ICTs for criminal purposes'.[35]

Three formal AHC sessions took place in 2023 (in January, April and August) alongside two rounds of informal intersessional consultations (in March and June). Sessions took place in Vienna and New York under the chair of Faouzia Boumaiza Mebarki of Algeria and with the support of the UN Office on Drugs and Crime. Prior sessions had led to the development of a consolidated negotiating document that formed the basis of the January and April sessions. Member states exchanged views in informal negotiation groups on topics requiring more focused attention, including criminalization, general provisions, procedural measures, law enforcement and international cooperation, and implementation mechanisms.[36]

A draft text of the convention was prepared in advance of the AHC's sixth session in August and September 2023.[37] During the session participants reviewed the text while also meeting informally to discuss more controversial issues. Given that this was the last session before the final negotiation scheduled for February 2024, there was pressure to resolve outstanding differences and work towards consensus. However, reaching agreement does not appear to be an easy task.[38]

Western advocacy groups and others expressed concern that the draft could be 'disastrous for human rights'.[39] Governmental and non-governmental stakeholders sounded the alarm about the potential for the new convention to negatively impact human rights since the start of the process. The AHC process was initiated via resolution introduced by Russia in the UN General Assembly's Third Committee—the committee responsible for human rights.[40] Some states felt this was a rushed process that did not take into account the

[35] The committee was established under UN General Assembly Resolution 74/247, 27 Dec. 2019, which also set out a process for the convention's development.

[36] 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 (AHC on cybercrime), 'Co-facilitated informal negotiations', [n.d.].

[37] UN General Assembly, AHC on cybercrime, 'Draft text of the Convention', A/AC.291/22, 29 May 2023, annex.

[38] See e.g. Kazakova, A., Swift, K. and Kovač, B., 'Key takeaways from the sixth UN session on cybercrime treaty negotiations', DigWatch Analysis, 13 Sep. 2023.

[39] Kazakova, Swift and Kovač (note 38).

[40] UN General Assembly Resolution 74/247 (note 35).

views of all member states.[41] While the nature of those concerns evolved in line with the subsequent negotiations, they tended to focus on (*a*) how cybercrime is defined, including the implications of an overly broad definition for freedom of expression; (*b*) support to victims; and (*c*) the maintenance of existing legal obligations.[42] Since the inception of the process there have also been related concerns over how a new instrument would interact with existing cybercrime law, notably the Budapest Convention on Cybercrime of the Council of Europe, as well as other regional instruments.[43]

Meanwhile, other countries, including Russia and China, raised concerns that the draft did not meet the scope established by the AHC's mandate. Other points of contention included different understandings of the scope of criminalization, international cooperation and mutual legal assistance, and inclusion of the word 'sustainability'.[44]

The AHC's concluding session is scheduled to take place in New York from 29 January to 9 February 2024 where states will consider a revised draft convention.[45] Concerns persist about the ability to reach consensus or about the implications if the current draft is adopted. Further sessions are not mandated so if consensus is not found, those states championing a treaty may need to seek a mandate for further negotiations, or to have the treaty adopted by vote in the General Assembly. If the draft convention is adopted it will become the UN's first binding instrument on a cyber issue, while also providing an important legal framework for cooperation on cybercrime.[46]

UN open-ended working group on ICT security

In 2020 the First Committee of the General Assembly established a second OEWG on security of and in the use of ICTs. The group began work in 2021 and will sit until 2025, under the chair of Burhan Gafoor of Singapore. This is the successor to the 2019–21 OEWG on ICT security and carries forward the

[41] United Nations, 'General Assembly adopts resolution outlining terms for negotiating cybercrime treaty amid concerns over "rushed" vote at expense of further consultations', Meetings coverage, GA/12328, 26 May 2021.

[42] See e.g. 'Multistakeholder manifesto prioritizing human-centric equities within the proposed UN cybercrime treaty', CyberPeace Institute, 30 Sep. 2021; and Hakmeh, J., 'Can a cybercrime convention for all be achieved?', Chatham House, 31 Mar. 2022.

[43] Hakmeh, J. and Peters, A., 'A new UN cybercrime treaty? The way forward for supporters of an open, free, and secure internet', Council on Foreign Relations, 13 Jan. 2020; and Council of Europe, Convention on Cybercrime, ETS No. 185, opened for signature 23 Nov. 2000, entered into force 1 July 2004 (Budapest Convention).

[44] Kazakova, Swift and Kovač (note 38). For more analysis on the sixth session of the AHC see Tropina, T., 'UN cybercrime negotiations: No outcome may be the best outcome', Internet Governance Project; 'The UN Cybercrime Treaty: Is it a crime?', Panel discussion, Stimson Center, 26 Sep. 2023; and Global Initiative Against Transnational Organized Crime, 'UN cybercrime treaty', Briefing note, Nov. 2023.

[45] UN Office on Drugs and Crime, AHC on cybercrime, 'Concluding session of the Ad Hoc Committee', [n.d.].

[46] Wilkinson, I., 'What is the UN cybercrime treaty and why does it matter?', Chatham House, 2 Aug. 2023.

work conducted by the six UN groups of governmental experts (GGEs) on ICT that were convened over the last two decades, and which laid the foundations for what is now referred to as the UN Framework for Responsible State Behaviour in the Use of ICTs. The framework is based on the understanding that international law applies to state conduct in cyberspace and comprises 11 voluntary behavioural norms.

The second OEWG on ICT security is mandated to consider six agenda items: threats; rules, norms, and principles; applicability of international law; capacity building; confidence building measures; and regular institutional dialogue. Over time, the diversity and depth of representation and exchange has improved, although challenges still exist with respect to the participation of non-governmental stakeholders in the formal meetings of the group.[47]

Three substantive OEWG sessions occurred in 2023. The March session was a precursor to July's negotiating session in which states adopted the group's second annual progress report (APR).[48] The December session effectively opened a new cycle of work in the lead-up to the adoption of another APR in 2024.

The OEWG's second APR reflected various proposals tabled and debated over the year. Notably, this included a paper outlining the elements for developing and operationalizing a new global intergovernmental points of contact (POC) directory, deemed as one of the more concrete outputs of the group.[49] While the POC directory received broad enough support from states, several also 'outlined concerns about duplication of existing directories, the capacity [of the UN] to maintain it, and differing ideas about a POC mandate (technical versus political)'.[50]

Importantly, the APR established that three dedicated intersessional meetings will take place in the coming year to discuss three of the six agenda items: threats; rules, norms, and principles; and the applicability of international law.[51] Several next steps were included in the capacity-building section of the APR, including a mapping exercise to be led by the UN Secretariat, and culminating in a report; an intersessional global roundtable meeting on ICT-security capacity building; and continued discussion of India's proposal to create a global cyber security cooperation portal.[52] Other proposals, such as

[47] For more on the OEWG on security of and in the use of ICTs 2021–2025 (OEWG on ICT security) see 'Overview', [n.d.]. For a history of this process see Pytlak, A., 'Cyberspace and the malicious use of information and communications technology', in *SIPRI Yearbook 2022*, pp. 558–71.

[48] Second annual report of the OEWG on ICT security in United Nations, General Assembly, 78th session, 'Developments in the field of information and telecommunications in the context of international security', A/78/265, 1 Aug. 2023.

[49] Second annual report of the OEWG on ICT security (note 48), pp. 12–14 .

[50] Pytlak, A., 'Discord and diplomacy: Reviewing outcomes from the UN's cyber working group', Stimson Center, 14 Aug. 2023.

[51] Second annual report of the OEWG on ICT security (note 48), paras 22, 27, 35.

[52] Second annual report of the OEWG on ICT security (note 48), paras 43–51.

the one from Kenya to create a repository for cyber threats, and the suggestion from others to develop a glossary of technical ICT terms, did not garner enough support to be included in the APR but were discussed again in the December session.[53]

An important OEWG dynamic concerns the long-standing debate over the push for a legally binding instrument. In 2023 Russia and a small group of states (Belarus, North Korea, Nicaragua, Syria and Venezuela) submitted an updated version of an earlier concept note for a UN convention on ensuring 'international information security'.[54] A majority of UN member states, particularly Western countries, have stated their opposition to legally binding measures and their belief that the current UN Framework is sufficient.[55]

The issue of a legally binding treaty came to the fore during the fifth OEWG session in July. States supporting a treaty wanted more references in the APR draft text to the proposal for a convention or potential legal instrument. States opposing a treaty sought to minimize not only such references but also the 'airtime' that future OEWG sessions will give to discussion of legal measures. Ultimately, the impasse was resolved by using footnotes within the APR, allowing the document to be adopted by consensus.[56] However, the issue will continue to trouble future work in the OEWG.

UN Programme of Action

Another global initiative that gained traction in 2023 was the proposal to create a new UN Programme of Action (POA) for advancing responsible state behaviour in the use of ICT. Originally submitted to the second OEWG on ICT security in 2020 by Egypt and France, the concept of a cyber POA has been slowly taking shape following the 2022 adoption of a General Assembly resolution that requested the UN secretary-general seek the views of member states on the scope, structure and content of the cyber POA and on the preparatory work and modalities for its establishment.[57] Broadly, most UN member states see value in a cyber POA as a 'permanent, inclusive, action-oriented mechanism' that will support implementation of the UN Framework, including its confidence- and capacity-building measures.[58] However, views differ on whether a cyber POA should also have the ability to establish new norms and how it will function in practice.

To this end, UN member states submitted views in writing and through several regional consultations convened by the UN Secretariat in early 2023.

[53] Pytlak (note 50); see also McDonald, E. 'Shaky consensus at the OEWG: Where next for UN discussions on state behaviour in cyberspace?', Global Partners Digital, 10 Aug. 2023.

[54] OEWG on ICT, Sixth session, 'Updated concept of the convention of the United Nations on ensuring international information security', Working paper submitted by Russia, 15 Dec. 2023.

[55] Pytlak (note 50).

[56] Pytlak (note 50).

[57] UN General Assembly Resolution 77/37, 7 Dec. 2022.

[58] Resolution 77/37 (note 57), para. 1.

These were compiled into an April 2023 report from the UN secretary-general.[59] Non-governmental stakeholders participated in some of the regional consultations and were also invited to submit views as part of a parallel process convened by the UN Institute for Disarmament Research (UNIDIR).[60]

During the 78th session of the First Committee in 2023, member states adopted a new resolution on the cyber POA, which was later endorsed in the General Assembly by a vote of 161 in favour, 9 against and 11 abstentions.[61] The resolution establishes a UN mechanism after the 2021–25 OEWG on cybersecurity concludes and 'no later than 2026'; the 'scope, structure, content and modalities' of this future mechanism must be 'based on consensus outcomes' of the OEWG.[62] This mandate effectively ties development of the mechanism to whatever can be agreed by consensus within the OEWG. While it makes sense to maximize the opportunities provided by the OEWG and its meetings, including its standing agenda item on 'regular institutional dialogue', there are also risks in not giving the POA sufficient space to be developed and negotiated on its own terms.

Other UN initiatives

In May 2023 Albania and the USA organized an Arria-formula meeting in the UN Security Council with co-sponsorship by Ecuador and non-Council member Estonia. The focus was on the responsibility and responsiveness of states to cyberattacks on critical infrastructure.[63] The meeting invited states to comment on actions the Security Council could take to address cyberattacks against critical infrastructure perpetrated by states; the role of the Council in ensuring a secure and peaceful cyberspace; and the venues and mechanisms for a closer partnership between public and private entities for defence and response.

As part of the process leading to the UN's Summit of the Future in 2024, the UN secretary-general issued a new policy brief in 2023 containing proposals for *A New Agenda for Peace*.[64] Relevant to cyberspace are the recom-

[59] United Nations, General Assembly, First Committee, 78th Session, 'Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security', Report of the secretary-general, A/78/76, 18 Apr. 2023.

[60] UNIDIR Security and Technology Programme, *Drawing Parallels: A Multi-Stakeholder Perspective on the Cyber POA Scope, Structure and Content* (UNIDIR: Geneva, Sep. 2023).

[61] United Nations, 'General Assembly adopts 56 First Committee texts as geopolitical realities test sustainability of non-proliferation regime, scuttle consensus', Meetings coverage, GA/12568, 4 Dec. 2023; and UN General Assembly Resolution 78/16, 6 Dec. 2023.

[62] UN General Assembly Resolution 78/16 (note 61), para. 4.

[63] Security Council Report, 'Arria-formula meeting on 'the responsibility and responsiveness of states to cyberattacks on critical infrastructure' ", *What's in Blue*, 25 May 2023; and Grzegorzewski, M. and Holden, W., '911? We have an emergency: Cyberattacks on emergency response systems', Lawfare, 3 May, 2023.

[64] United Nations, *A New Agenda for Peace*, Our Common Agenda Policy Brief no. 9 (United Nations: New York, July 2023).

mendations to (*a*) develop governance frameworks, at the international and national levels, 'to minimize harms and address the cross-cutting risks posed by converging technologies'; and (*b*) establish 'an independent multilateral accountability mechanism for malicious use of cyberspace by States to reduce incentives for such conduct' and 'enhance compliance with agreed norms and principles of responsible State behaviour'.[65]

Other regional, bilateral and national initiatives

Regional initiatives

The African Union (AU) Convention on Cyber Security and Personal Data Protection (Malabo Convention) entered into force in 2023, nine years after its adoption by the AU Assembly in 2014.[66] The Malabo Convention aims to create a comprehensive legal framework for electronic commerce, data protection, and cybercrime and cybersecurity on the African continent, by harmonizing the national legislation of AU member states in these areas. In that vein, it can also serve as a basis for establishing common positions in other processes or forums, such as the AHC on cybersecurity. Significantly, the Malabo Convention is the only cybersecurity convention that combines cybersecurity, cybercrime, electronic transactions and data protection. While its entry into force was widely welcomed, some commentators expressed concerns that it may need to be updated to reflect developments since 2014 and also about the prospects of the remaining AU member states acceding to it (only 15 of 55 states have done so).[67]

European Union (EU) institutions reached provisional agreement on the text of a proposed EU Cyber Resilience Act (CRA) in November 2023.[68] The CRA aims to protect individuals and businesses when purchasing or using products or software with a 'digital element', a broad term inclusive of both hardware and software. It introduces mandatory cybersecurity requirements for manufacturers and retailers of such products, which contributes to more harmonized rules and a framework for governing product planning, design, development and maintenance. Although the CRA has been widely supported, its provisions around reporting of product vulnerabilities prompted an open letter from more than 50 individuals, who argued that the

[65] United Nations (note 64), Action 11, pp. 26, 27.

[66] African Union Convention on Cyber Security and Data Protection (Malabo Convention), adopted 27 June 2014, entered into force 8 June 2023.

[67] See e.g. 'Continental cyber security policymaking: Implications of the entry into force of the Malabo Convention for digital financial systems in Africa', Carnegie Endowment for International Peace event report, 10 July 2023; and Ifeanyi-Ajufo, N., 'Cyber governance in Africa is weak. Taking the Malabo Convention seriously would be a good start', The Conversation, 31 July 2023.

[68] Council of the European Union, 'Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products', Press release, 30 Nov. 2023.

draft obligation to report a vulnerability publicly within 24 hours and before being patched risks the vulnerability being exploited by others. Signatories to the letter suggested either allowing a longer time frame for reporting (72 hours) with a requirement to do so only after patches had been deployed, or removing this provision entirely.[69]

National-level and bilateral initiatives

Unilateral national-level policy development can have implications for global governance. One national event of note was the US launch of its latest National Cybersecurity Strategy in March 2023. The strategy is made up of five pillars: defending critical infrastructure; disrupting and dismantling threat actors; shaping market forces to drive resilience; investing in a resilient future; and forging international partnerships.[70] The 2023 strategy was followed by the release of the US Department of Defense (DOD) Cyber Strategy in July 2023, which 'implements the priorities' of the National Cybersecurity Strategy.[71] Both strategies continue the sometimes-controversial US practice of 'defending forward', in which the US commits to 'disrupt malicious cyber activity at its source, including activity that falls below the level of armed conflict'.[72] An unclassified summary of the DOD Cyber Strategy was the focus of a USA–China bilateral meeting in September that occurred as a confidence-building mechanism between the two states.[73]

Another important national development was Chile's bill to establish a framework law on cybersecurity and critical information infrastructure, which was approved by the National Congress in December 2023 and was awaiting approval in the Senate.[74] If passed, the bill would, among other things, establish an institutional framework and general regulations to structure, regulate and coordinate Chilean government agencies; establish minimum requirements for the prevention and response to cybersecurity incidents; and create new agencies responsible for matters of cybersecurity. This bill may set a path for other nations in the region to follow.[75]

In 2023 more governments released their national interpretations of how international law applies to their use of ICTs, including Costa Rica, Finland,

[69] Budington, B. and Galperin, E., 'EFF and other experts join in pointing out pitfalls of proposed EU Cyber-Resilience Act', 3 Oct. 2023.

[70] US Government, *National Cybersecurity Strategy* (White House: Washington, DC, Mar. 2023). See also Healy, J., 'Twenty-five years of White House cyber policies', Lawfare, 2 June 2023.

[71] US Department of Defense (DOD), *Summary: 2023 Cyber Strategy of the Department of Defense*, (DOD: Washington, DC, July 2023), p. 1.

[72] US Cyber Command, 'CYBER 101—Defend forward and persistent engagement', News, 25 Oct. 2022.

[73] US DOD, 'US and PRC hold working level meeting on 2023 DOD Cyber Strategy Unclassified Summary and related cyber issues', Press release, 22 Sep. 2023.

[74] 'Chile: Chamber of Deputies approves cybersecurity law, presented for Senate consideration', One Trust Data Guidance, 12 Dec. 2023.

[75] See Hurel, L. M., 'The political cybersecurity blindfold in Latin America', Lawfare, 26 Apr. 2023.

Ireland and New Zealand, among others.[76] Around 30 countries have now done this in an effort to clarify understanding and improve predictability; others have used the OEWG on ICT security or other venues to announce their intention to do so.

Public attribution for cyberattacks and operations is increasingly a tool employed by governments either nationally or in cooperation with like-minded states.[77] However, the impact of such public attribution on improving accountability is unclear, with governments needing to improve the coordination of their approaches to attribution.[78]

Other initiatives

One significant development for bolstering the applicability and enforcement of international law was a 2023 announcement from the lead prosecutor of the International Criminal Court (ICC), Karim A. A. Khan KC, that his office would start collecting and reviewing evidence of cyber misconduct that may amount to one of the offences under the ICC's jurisdiction.[79]

During the sixth edition of the Paris Peace Forum in November 2023, a session on the 'Paris Call for Trust and Security in Cyberspace' spotlighted ongoing work by Forum members to address two critical cybersecurity issues: cyber mercenaries and critical infrastructure attacks. The Forum released new reports on both these topics and is also progressing towards the development of a political commitment for 2024 on commercial spyware and the mercenary market.[80] This builds on other efforts and commitments, such as the executive order issued by US President Joe Biden in March 2023 prohibiting US government use of 'commercial spyware that poses risks to national security'.[81] This was followed by the development by a US-led Freedom Online Coalition—a group of 36 governments dedicated to protecting the same human rights online as offline—of Guiding Principles on

[76] Costa Rican Ministry of External Relations and Worship, 'Costa Rica's position on the application of international law in cyberspace', 21 July 2023; Finnish Ministry of Foreign Affairs, 'National position on international law and cyberspace', 24 July 2023; Irish Department of Foreign Affairs, 'Position paper on the application of inernational law to cyberspace', 7 July 2023; and Government of New Zealand, 'The application of international law to state activity in cyberspace', 24 July 2023.

[77] See e.g. British Foreign, Commonwealth and Development Office, 'UK exposes attempted Russian cyber interference in politics and democratic processes', 7 Dec. 2023, Press release; British National Cyber Security Centre, 'UK and US call out Russia for SolarWinds compromise', News, 15 Apr. 2021; and Gritten, B., 'Albania severs diplomatic ties with Iran over cyber attack', BBC, 7 Sep. 2022.

[78] Pytlak, A., 'Clue, Monopoly, or Risk?', Stimson Center, 16 Jan. 2024.

[79] Khan, K. A.A., 'Technology will not exceed our humanity', *Digital Front Lines: A Sharpened Focus on the Risks of, and Responses to, Hybrid Warfare* (FP Analytics and Microsoft: 20 Aug, 2023), p. 50.

[80] Paris Peace Forum, 'Protecting critical infrastructures against systemic harms: A path forward to overcome national discrepancies?', Issue Brief, 10 Nov. 2023; and Paris Peace Forum, 'Taming the cyber mercenary market a multistakeholder blueprint towards increased transparency and cyber stability', Blueprint, 10 Nov. 2023.

[81] White House, 'President Biden signs executive order to prohibit US government use of commercial spyware that poses risks to national security', Briefing Room Fact Sheet, 27 Mar. 2023.

Government Use of Surveillance Technologies. At the second US Summit for Democracy in March 2023, 44 participating states indicated their support for the Guiding Principles.[82]

Members of the US-led International Counter Ransomware Initiative (CRI) held their third gathering in 2023. The initiative has grown to include 50 members since it was established in 2021. The most recent gathering focused on developing capabilities to disrupt attackers and the infrastructure used to conduct attacks; improving cybersecurity through sharing information and other cooperation and coordination; and fighting back against ransomware actors, such as by pledging to not pay ransoms and committing to assist fellow CRI members.[83]

A diverse range of non-governmental actors has continued to advance important work that supports cyber governance. The Royal United Services Institute (RUSI) launched a Global Partnership for Responsible Cyber Behaviour that connects experts from different sectors and regions, to map practical understandings of responsible cyber behaviour by conducting evidence-based research.[84] Global Partners Digital released a toolkit with guidance on how to develop cyber norms inclusive of marginalized perspectives.[85] Several other organizations that advance work to better incorporate gender diversity in cyber policy response, whether in the context of cybercrime or cybersecurity, continued to advocate for human-centric approaches to cybersecurity within policymaking forums.[86]

The Global Forum on Cyber Expertise (GFCE) co-organized the first global conference on cyber capacity building with the World Bank, the CyberPeace Institute, the World Economic Forum and the Ghanaian Ministry of Communications and Digitalization. The conference brought together the cyber and socio-economic development communities under a common theme of cyber resilience in relation to development. It resulted in the adoption of the Accra Call for Cyber Resilient Development, which sets out a framework containing 16 non-binding direction-setting actions.[87]

The GFCE's long-standing Cybil Portal announced a collaboration with UNIDIR and its Cyber Policy Portal (CPP) in December, by integrating its capacity building data into the CPP. The CPP provides a comprehensive

[82] US Department of State, 'Guiding Principles on Government Use of Technology', Media Note, 30 Mar. 2023.

[83] White House, 'International Counter Ransomware Initiative 2023 Joint Statement', Briefing Room Statement, 1 Nov. 2023.

[84] RUSI, 'Global Partnership for Responsible Cyber Behaviour (GP-RCB)', [n.d.].

[85] Global Partners Digital (GPD), *Inclusive Cyber Norms: Toolkit* (GPD: London, 19 July 2023).

[86] See e.g. 'Joint civil society input to the revised zero draft of the second annual progress report of the OEWG 2021–2025', 24 July 2023.

[87] Global Conference on Cyber Capacity Building (GC3B), Accra, Ghana, 29–30 Nov. 2023; see 'Cyber resilience for development', [n.d.].

overview of cyber policy landscapes across all UN member states and select intergovernmental organizations.[88]

Conclusions

The likelihood of a comprehensive global instrument for cyber governance seems unlikely, at least in the near future. In 2023 the geopolitical climate continued to challenge multilateralism as a means for developing additional norms or instruments; capacity to engage in lengthy negotiations was low; and cyber and ICT-related challenges remained too complex for states to agree on how to comprehensively address them through a single instrument. Instead, the current 'patchwork' approach persisted, with multiple initiatives at various levels. Yet the approach may still have much to offer, provided the initiatives remain centred around commitments set out in the UN framework, without creating loopholes or contradictions, and cyber governance tools incorporate mechanisms for accountability and transparency, without which there is little incentive for curbing harmful cyber behaviour.

[88] Global Forum on Cyber Expertise, 'UNIDIR and GFCE joined forces to enhance knowledge and information on cyber capacity building globally', News, 18 Nov. 2023.