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

LUKE RICHARDS

As the cyber landscape develops, so too do cybersecurity threats—both from states and non-state actors such as cybercriminals. Notably, alongside the significant digitalization driven by the Covid-19 pandemic, which led to years of digital adoption being achieved in mere weeks, there was a 600 per cent increase in malicious emails attempting to exploit the growing digital dependency.[1] Computational propaganda—such as the use of cyber-influence operations and the spreading of disinformation—by state and non-state actors also increased around the globe.[2] Growing geopolitical tensions around the security of information and communications technology (ICT) have also led states to increase their scrutiny of ICT supply chains.[3]

As these developments continue, the need to better understand a state's ability to wield its cyber power through the malicious use of ICT grows.[4] Cyber activity often takes place below the threshold of armed conflict. For example, during the final weeks of 2020 the United States Government suffered what appeared to be one of the biggest cybersecurity breaches in its history, the Solar Winds hack, which can be described as an act of espionage rather than war.[5] It was the result of a supply chain vulnerability that also left companies and other governments around the world vulnerable.[6]

International efforts to control the malicious use of ICT were slowed by the Covid-19 pandemic. States' differing interests and normative preferences have also made concrete progress difficult. This section first reviews key developments in cyberspace itself and then describes these efforts to govern it through new global instruments and via multilevel dialogue.

[1] Baig, A. et al., 'The Covid-19 recovery will be digital: A plan for the first 90 days', McKinsey Digital, 14 May 2020; and Lederer, E. M., 'Top UN official warns malicious emails on rise in pandemic', AP News, 23 May 2020.

[2] Oxford Internet Institute, Project on Computations Propaganda, 'Industrialized disinformation: 2020 global inventory of organized social media manipulation', University of Oxford, 13 Jan. 2021.

[3] Kuehn, A., 'TechNationalism: Cybersecurity at the intersection of geopolitics', EastWest Institute, 17 Sep. 2020.

[4] On how state cyber power can be measured and an international ranking see Voo, J. et al., *National Cyber Power Index 2020: Methodology and Analytical Considerations* (Belfer Center for Science and International Affairs: Cambridge, MA, Sep. 2020).

[5] Paul, K. and Beckett, L., 'What we know—and still don't—about the worst-ever US Government cyber-attack', *The Guardian*, 18 Dec. 2020.

[6] Smith, B., 'A moment of reckoning: The need for a strong and global cybersecurity response', Microsoft, 17 Dec. 2020.

A divided internet and divided interests

The debate around governing the use of ICT at the international level is not just technical, but also has ideological and strategic aspects.[7] As the competing interests and the use of ICT have grown, the internet's infrastructure has also changed—a trend that continued in 2020.

While seemingly borderless, the internet is not entirely abstract but is bound to an infrastructure with a physical geography.[8] Some states, such as China and Russia, have postulated notions of cyber sovereignty. In 2019 Russia—in emulation of China's closed-off internet and information control—began attempting to cut its internet off from the rest of the world. This process continued in 2020 with a ban on the use of several forms of encryption and plans to replace some of them with Russian alternatives.[9]

Notably, the European Union (EU) is also moving towards a more gated system—that is, towards digital and technological sovereignty. For example, in 2020 the EU began a project to create a European cloud system, GAIA-X, to increase cloud and data services protected by the EU's data laws.[10] Also in 2020 the European Court of Justice invalidated Privacy Shield, a data-exchange agreement between the EU and the USA, in part due to concerns over the surveillance practices of US intelligence agencies and EU data-protection laws.[11]

The USA, too, has tested policies that have had an impact on the internet's infrastructure and development. These include sanctioning Chinese technology companies (e.g. Huawei and ByteDance, the owner of TikTok) and persuading allies not to use Chinese equipment in their telecommunications networks.[12]

[7] Henriksen, A., 'The end of the road for the UN GGE process: The future regulation of cyberspace', *Journal of Cybersecurity*, vol. 5 (2019), tyy009.

[8] Graham, M., 'Geography/internet: Ethereal alternate dimensions of cyberspace or grounded augmented realities?', *Geographical Journal*, vol. 179, no. 2 (June 2013), pp. 177–82.

[9] Weber, V., 'The sinicization of Russia's cyber sovereignty model', Council on Foreign Relations, 1 Apr. 2020; and Kolomychenko, M., 'Russia's Digital Development Ministry wants to ban the latest encryption technologies from the RuNet', 21 Sep. 2020.

[10] Hushes, O., 'What is Gaia-X? A guide to Europe's cloud computing fight-back plan', TechRepublic, 10 June 2020.

[11] Court of Justice of the European Union, *Data Protection Commissioner* v *Facebook Ireland Limited and Maximillian Schrems*, Case no. C-311/18, Judgment of the Court (Grand Chamber), 16 July 2020. See also Ettari, S. V., 'European Court of Justice invalidates EU–US Privacy Shield framework', Kramer Levin Naftalis & Frankel LLP, 1 Oct. 2020.

[12] On the US response to China see Williams, R. D., 'Beyond Huawei and TikTok: Untangling US concerns over Chinese tech companies and digital security', Working paper, University of Pennsylvania, Penn Project on the Future of US–China Relations, 2020; and Baxendale, H., 'Huawei or our way?: Fissures in the Five Eyes alliance in the face of a rising China', Centre for International Policy Studies, 16 Oct. 2020. On the impact in the EU see Anthony, I. et al., *China–EU Connectivity in an Era of Geopolitical Competition*, SIPRI Policy Paper no. 59 (SIPRI: Stockholm, Mar. 2021).

These examples of states' responses to the shifting cyber landscape and splintering of the internet across 2020 are likely to feed into debates on the governance of ICT in the years ahead.

Governing the malicious use of information and communications technology

Multilevel dialogue

Dialogue around the governance of ICT and cyber norms has taken place at multiple levels. It builds on a raft of measures and initiatives to regulate the use of cyberspace and to develop normative frameworks at a range of levels, from multinational interstate efforts to collaborations by private enterprises.[13] These frameworks have included the Global Commission on Stability in Cyberspace, which was launched in 2017 and reported in 2019; the Paris Call for Trust and Security in Cyberspace of November 2018, which established nine principles on responsible behaviour; and the Cybersecurity Tech Accord, under which 147 technology companies have agreed to protect their customers from malicious threats.[14] This wide proliferation of efforts to create an ecosystem of cyber norms has allowed for the cross-pollination of ideas.

In May 2020 the Oxford Process on International Law Protections in Cyberspace was launched.[15] This partnership between the University of Oxford and Microsoft aims to examine international law as it applies to specific objects of protection, such as within the healthcare sector and electoral processes.

United Nations processes

The main state-driven efforts to govern the malicious use of ICT continued in 2020 within the United Nations. In 2010, 2013 and 2015, groups of governmental experts (GGEs) on this topic had resulted in consensus reports.[16] The process split in 2018 after the adoption by the UN General Assembly of competing resolutions tabled by Russia and the USA which reflected the

[13] Ruhl, C. et al., *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*, Working paper (Carnegie Endowment for International Peace: Washington, DC, Feb. 2020), pp. 13–15.

[14] Global Commission on Stability in Cyberspace (GCSC), *Advancing Cyberstability*, Final report (The Hague Centre for Strategic Studies/EastWest Institute: The Hague/New York, Nov. 2019); and Paris Call for Trust and Security in Cyberspace, 12 Nov. 2018.

[15] Oxford Institute for Ethics, Law and Armed Conflict (ELAC), 'The Oxford Process on International Law Protections in Cyberspace', University of Oxford, May 2020.

[16] UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 'International law in the consensus reports of the United Nations groups of governmental experts', Background paper, Feb. 2020.

enduring differences in their approaches to ICT risks.[17] The USA has a narrower focus on cybersecurity and the technical protection of ICT systems and the information that they contain. It sees no need for new international regulation as it considers that international humanitarian law already applies to cyberspace in armed conflicts. Instead, it favours the adoption by states of voluntary and non-binding norms aimed at supporting the security of infrastructure and information in peacetime. Russia meanwhile has a broader perspective that includes risks posed by information itself and reflects its desire to control information within its national borders. It would like to see the development of a legally binding regime with elements that legitimize its view of information security.[18] The US-sponsored resolution established a new GGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.[19] The Russian-sponsored resolution established the Open-ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security.[20]

The GGE—the sixth in the series—is comprised of representatives of 25 UN member states. It continued with states sitting for the second substantive session in February 2020. It was unable to sit for a scheduled third session due to the Covid-19 pandemic. Instead, its third and fourth (and final) sessions were rescheduled to convene before May 2021.[21]

The OEWG is the larger of the two processes since it is open to any interested member state. It was unable to meet in person during 2020 for its third and final substantive session and the July deadline for a consensus report. Instead, states met informally over the course of the year. An informal multi-stakeholder cyber dialogue open to all interested stakeholders also took place in December.[22] The OEWG was engaged through documents produced by states and civil society groups, alongside non-papers and the chair's pre-drafts of the OEWG report.[23] The chair rescheduled the missed session for March 2021.[24]

[17] UN Office for Disarmament Affairs (UNODA), 'Developments in the field of information and telecommunications in the context of international security', [n.d.].

[18] For a thorough discussion on Russia and US differences and how they have shaped the UN process see Tikk, E., 'Cyber arms control and resilience', *SIPRI Yearbook 2019*.

[19] UN General Assembly Resolution 73/266, 'Advancing responsible state behaviour in cyberspace in the context of international security', 22 Dec. 2018, A/RES/73/266, 2 Jan. 2019.

[20] UN General Assembly Resolution 73/27, 'Developments in the field of information and telecommunications in the context of international security', 5 Dec. 2018, A/RES/73/27, 11 Dec. 2018.

[21] United Nations, General Assembly, Decision no. 75/551, 31 Dec. 2020, Official Records, Supplement no. 49, A/75/49 (Vol. II), 2021, p. 23.

[22] Informal Multi-stakeholder Cyber Dialogue, 'Summary report', 4–10 Dec. 2020.

[23] All the documents can be found at UN Office for Disarmament Affairs (UNODA), 'Open-ended working group', [n.d.].

[24] Lauber, J., OEWG Chair, Letter to all permanent representatives and permanent observers from the permanent mission of Switzerland to the United Nations, 9 June 2020.

A group of 47 states suggested a programme of action (POA) as one way to move the debate forward.[25] The proposal suggests the creation of a framework and a political commitment based on recommendations, norms and principles already agreed in previously endorsed GGE reports along with the outcomes of the current GGE and OEWG. The proposed POA would focus on areas such as implementation and capacity building, along with regular monitoring and review of the process itself.[26] Action under the POA would be reported to the UN General Assembly, and it would remain a process of the Assembly's First Committee.

During October 2020, Russia and the USA again proposed competing ways forward, in line with their differing ideological and strategic interests.[27] The USA tabled a draft resolution proposing that future work be decided once the current GGE and OEWG processes had concluded.[28] The following day Russia submitted a draft resolution (later revised) that would establish a new OEWG on Security of and in the Use of Information and Communications Technologies to run in the period 2021–25.[29] The two drafts were both adopted by the General Assembly during plenary sessions on 7 and 31 December.[30] The US proposal to conclude the current processes before deciding what to do next was thus only shortly lived.

The new OEWG is to start its work after the earlier OEWG concludes. The potential POA would thus run concurrently with the new OEWG, rather than acting as a means of bringing the two parallel process into one forum as initially envisioned.

[25] UN 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] UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Concept-note on the organizational aspects of a Programme of Action for advancing responsible state behaviour in cyberspace', Dec. 2020.

[27] Gold, J., 'Competing US–Russia cybersecurity resolutions risk slowing UN progress further', Council on Foreign Relations, 29 Oct. 2020. See also Tikk (note 18).

[28] United Nations, General Assembly, 'Developments in the field of information and telecommunications in the context of international security', Report of the First Committee, A/75/394, 6 Nov. 2020, paras 5–6.

[29] United Nations, A/75/394 (note 28), paras 7–10.

[30] The USA sponsored UN General Assembly Resolution 75/32, 'Advancing responsible state behaviour in cyberspace in the context of international security', 7 Dec. 2020, A/RES/75/32, 16 Dec. 2020. Russia sponsored UN General Assembly Resolution 75/240, 'Developments in the field of information and telecommunications in the context of international security', 31 Dec. 2020, A/RES/75/240, 4 Jan. 2021. On the debate on the competing resolutions see United National, 'First Committee approves 15 draft resolutions, decisions on disarmament measures, including 2 following different paths towards keeping cyberspace safe', Meetings coverage, GA/DIS/3659, 9 Nov. 2020.

Conclusions

Overall, dialogue around cybersecurity and the malicious use of ICT is moving forward, and changes to the digital landscape caused by the Covid-19 pandemic may hasten the need for action. The multilevel approach will probably continue. However, it seems that it will be difficult for states to reach a consensus agreement on the outcomes of the current GGE and OEWG. Looking ahead, the parallel processes will continue through the new OWEG and the POA if the outlined proposal is accepted.