IV. Developments in governance of cyberspace and the impact of the war in Ukraine

LORA SAALMAN

Cyber governance is understood to mean the legal and normative framework that regulates activities in cyberspace. The norms that have been developed in the long-running United Nations process on cyber governance were severely challenged in 2022 by the war in Ukraine. These norms were violated both prior to and during the conflict, including the alleged use of both Ukrainian and Russian territory with government knowledge and support for wrongful acts using information and communications technology (ICT).[1] Cyberattacks and cyber intrusions by both sides damaged critical civilian infrastructure and harmed information systems (see section II).

Nevertheless, there was international cooperation in prosecuting criminal use of ICT. Notably, intergovernmental cooperation was not just between Ukraine and the United States, or Ukraine and the European Union (EU), but even between Russia and the USA. In addition, cooperation between governments and industry included the provision by a range of companies of computing hardware and software services. However, this engagement with companies did not translate to the UN cyber governance process, where there were efforts to block accreditation of private-sector and non-governmental organizations (NGOs).

This section first reviews developments in UN cyber governance in 2022. It then looks at two sets of international cooperation: between Russian and US law enforcement agencies on ICT-related crimes; and between Ukraine and state and non-state actors on cyber resilience, cyber governance and even alleged cyberattacks. The section concludes by briefly assessing the prospects for achieving consensus in the governance of cyberspace.

The second United Nations open-ended working group on ICT security

The current UN process on cyber governance started with a series of groups of governmental experts (GGEs) established by the General Assembly from 2004. The process bifurcated in 2019, with a US-sponsored GGE—with a limited membership—on 'advancing responsible state behaviour in cyberspace in the context of international security' meeting in parallel with a Russian-sponsored open-ended working group (OEWG)—open to all UN member states—on 'developments in the field of information and telecommunications in the context of international security' (OEWG I). A second

[1] Przetacznik, J. and Tarpova, S., 'Russia's war on Ukraine: Timeline of cyberattacks', European Parliamentary Research Service, June 2022.

OEWG, on 'security of and in the use of information and communications technology 2021–2025' (OEWG II) held its first meeting in 2021.[2]

UN General Assembly reports issued in 2022 indicate that there was a concerted effort to keep channels of engagement open in the context of the war in Ukraine and in the face of 'a challenging geopolitical environment'.[3] This allowed states to address ongoing concerns over the development of ICT capabilities for military purposes; the malicious use of ICT by state and non-state actors; and harmful ICT activity against critical infrastructure that provides essential services to the public, thereby compromising the availability and integrity of internet services and health care.[4] Accordingly, the UN reports included a variety of proposals for both capacity building and confidence building, such as a directory of points of contact on ICT security who 'could be reached in times of urgency'.[5]

The UN General Assembly also adopted a resolution on initiating steps leading to an agreed programme of action (POA) 'to advance responsible State behaviour in the use of information and communications technologies in the context of international security'.[6] However, the proposal of a POA remained contentious due to concerns that it might establish a body parallel to OEWG II.[7] If the General Assembly is able to adopt a POA as a permanent, inclusive, action-oriented mechanism after the conclusion of OEWG II in 2025, this will at a minimum maintain UN channels of engagement. However, NGO participation is likely to face increasing obstacles (see discussion of Ukraine and the private sector below).

Despite these signs of progress, the widespread cyberattacks on civilian critical infrastructure both preceding and during the Russian invasion of Ukraine—and allegedly carried out by state and non-state actors on both sides—showed that challenges to enforcing international law in cyberspace

[2] UN General Assembly Resolution 75/240, 31 Dec. 2020. On the GGE and OEWG processes see Pytlak, A., 'Cyberspace and the malicious use of information and communications technology', *SIPRI Yearbook 2022*, pp. 558–71; and UN Office for Disarmament Affairs (UNODA), 'Developments in the field of information and telecommunications in the context of international security'.

[3] United Nations, General Assembly, OEWG on security of and in the use of ICT 2021–25, 3rd substantive session, Draft annual progress report, A/AC.292/2022/CRP.1, 28 July 2022, para. 1.

[4] United Nations, General Assembly, 'Developments in the field of information and telecommunications in the context of international security', Report of the First Committee, A/77/380, 14 Nov. 2022; UN General Assembly Resolution 77/37, 7 Dec. 2022; and United Nations, General Assembly, OEWG on security of and in the use of ICT 2021–25, 'Developments in the field of information and telecommunications in the context of international security', Note by the secretary-general, A/77/275, 8 Aug. 2022.

[5] United Nations, A/AC.292/2022/CRP.1 (note 3), para. 16(b).

[6] UN General Assembly Resolution 77/37 (note 4).

[7] Meyer, P., 'Cyber security at the UN General Assembly First Committee—Déjà vu all over again', ICT for Peace Foundation, 11 Nov. 2022.

remained. This was reaffirmed by OEWG I in its final report in 2021.[8] In fact, cyberattacks that targeted government, finance, telecommunications and power facilities (see section II) indicated that both Russian and Ukrainian state and non-state actors violated the norms identified by the GGEs and OEWGs on ICT.[9] These violations included government knowledge of its territory being used for intentionally wrongful acts using ICT; intentional damage to or impairment of critical infrastructure; and harming of information systems that provide services to the public.

While such violations highlighted the growing need for strengthened cyber governance, they also revealed the complexity of enforcing it. These difficulties are compounded by the persistent challenge of attribution that is exacerbated by the involvement of both state and non-state actors in the Ukraine conflict and the dual-use nature of cyberspace for civilian and military aims, combined with the voluntary nature of the norms process.

International cooperation with Russia

In the conflict between Russia and Ukraine, other European states and the USA have predominantly supported Ukraine and sought to apply diplomatic pressure to Russia. However, in cooperation with other governments, Russia made some notable efforts in 2022 to implement the cyberspace norms of the GGEs and OEWGs, particularly in terms of information exchange to assist in prosecuting criminal use of ICTs.

In January 2022, just prior to the invasion of Ukraine, the Russian Federal Security Service (Federal'naya Sluzhba Bezopasnosti, FSB) and law enforcement agencies cooperated with US counterparts to arrest four members, including the alleged leader, of the Infraud Organization hacker group (also known as Unicc, Faaxxx and Faxtrod), which had caused losses estimated at US$560 million in its seven years of activity.[10] Earlier that month, the FSB—in response to US requests—conducted raids and arrested 14 alleged members of the DarkSide and REvil ransomware groups. These included a hacker who US officials said executed a cyberattack on Colonial Pipeline, the largest US pipeline system for refined oil products.[11]

[8] United Nations, General Assembly, OEWG on developments in the field of ICT in the context of international security, Final substantive report, A/75/816, 18 Mar. 2021, paras 34–40, and annex II, para. 18. See also United Nations, General Assembly, GGE on advancing responsible state behaviour in cyberspace in the context of international security, Report, A/76/135, 14 July 2021, para. 71(f).

[9] United Nations, A/77/380 (note 4); UN General Assembly Resolution 77/37 (note 4); and United Nations, A/77/275 (note 4).

[10] Ilascu, I., 'Russia arrests leader of "Infraud Organization" hacker group', Bleeping Computer, 25 Jan. 2022.

[11] Burgess, M., 'Russia takes down REvil hackers as Ukraine tensions mount', *Wired*, 14 Jan. 2022; and Dixon, R. and Nakashima, E., 'Russia arrests 14 alleged members of REvil ransomware gang, including hacker US says conducted Colonial Pipeline attack', *Washington Post*, 14 Jan. 2022.

Some have tied these actions to efforts by Russia to mitigate the severity of the US response to its intended invasion of Ukraine.[12] They nevertheless indicate Russia's willingness to cooperate on some key norms in cyberspace, even with countries with which it has adversarial relations.

International cooperation with Ukraine

Support for Ukraine from other governments

During 2022, Ukraine worked in close consultation with other governments in terms of both cyber resilience and cyber governance.

In February 2022 US Secretary of State Anthony J. Blinken issued a statement denouncing cyberattacks against Ukraine and pledging enhanced support for 'Ukraine's digital connectivity, including by providing satellite phones and data terminals to Ukrainian government officials, essential service providers, and critical infrastructure operators'.[13] Further, in May 2022 the head of US Cyber Command, General Paul Nakasone, declared that his agency had deployed a 'hunt forward' team to help Ukraine shore up its cyber defences against active threats.[14] In fact, in June 2022 Nakasone confirmed that the USA had undertaken offensive cyber operations in support of Ukraine, saying that they had 'conducted a series of operations across the full spectrum: offensive, defensive, [and] information operations'.[15] A month later, the USA disclosed evidence of 20 possible intrusions into Ukrainian systems that it had uncovered.[16]

The EU also made cyber commitments to Ukraine. In March 2022 the Estonian e-Governance Academy began implementation of a 12-month, €10 million EU project to strengthen cybersecurity and to keep public services available in Ukraine.[17] The project focused on three main areas: (*a*) the security of the Ukrainian government's Trembita secure data-exchange platform and the management of public registries, including identifying and neutralizing possible cyberthreats; (*b*) protection of critical infrastructure and public data, including the replacement of destroyed equipment; and (*c*) provision of security tools to enable operational staff to maintain and service critical public infrastructure. In December 2022 the EU also unveiled a

[12] Dixon and Nakashima (note 11).

[13] Blinken, A. J., US secretary of state, 'Attribution of Russia's malicious cyber activity against Ukraine', Press statement, US Department of State, 10 May 2022.

[14] Kagubare, I., 'Top US cyber officials warn against underestimating Russia's cyber capability', *The Hill*, 4 May 2022.

[15] Kagubare, I., 'Cyber Command chief confirms US took part in offensive cyber operations', *The Hill*, 1 June 2022.

[16] Cyber National Mission Force Public Affairs, 'Cyber National Mission Force discloses IOCs from Ukrainian networks', US Cyber Command, 20 July 2022.

[17] EU4Digital, 'EU supports cybersecurity in Ukraine with over €10 million', 21 Oct. 2022.

cyber laboratory in Kyiv to develop Ukraine's cyber defence capacities.[18] This was paid for from a €31 million fund to support the Ukrainian armed forces agreed in December 2021 under the EU's European Peace Facility.

More broadly, the 2022 international summit of the Counter Ransomware Initiative was held in October and November in Washington, DC, at which 37 country participants were in attendance, including Ukraine but not Russia.[19] The outcome of the summit was an action plan for states to cooperate on holding ransomware actors accountable for their crimes and not providing them safe haven; disrupting and bringing to justice ransomware actors and their enablers; and information sharing and securing of national cyber infrastructure against ransomware attacks. While not directed at Ukraine, the plan has implications for its combat of 'decoy ransomware' (the use of wipers masquerading as ransomware; see section II) for cyberwarfare aims.

Support for Ukraine from the private sector

The private sector was extremely active in both cyber resilience and cyber governance efforts related to Ukraine in 2022.

Immediately after the invasion, Amazon Web Services (AWS), a US cloud computing company, began to provide Snowball devices to Ukrainian ministries, schools and dozens of other private sector companies.[20] This ruggedized computing and storage hardware helped to transfer data from local servers in Ukraine to the cloud—by June 2022 over 10 petabytes had migrated to more secure, remote storage. Cisco Talos Intelligence Group, a US cybersecurity company, also worked closely with the Ukrainian State Service of Special Communications and Information Protection (SSSCIP), the Cyberpolice Department of the National Police and the National Cybersecurity Coordination Centre (NCCC) to help them respond to cyberattacks.[21] Other vendors, including Bitdefender, Cloudflare, ESET, Google and Sophos, reportedly provided additional or free security services, mechanisms for rapid sharing of intelligence, and encryption key relocation services in Ukraine.[22]

Further, in February 2022 Microsoft issued a statement of support for Ukraine in four areas: 'protecting Ukraine from cyberattacks; protection from state-sponsored disinformation campaigns; support for humanitarian

[18] European External Action Service (EEAS), 'Ukraine: EU sets up a cyber lab for the Ukrainian armed forces', 2 Dec. 2022.

[19] European Commission, 'International Counter Ransomware Initiative: Strengthening cybersecurity cooperation & actions', 3 Nov. 2022.

[20] Amazon Web Services, 'Amazon's assistance in Ukraine', 1 Dec. 2022; and Amazon Web Services, 'Safeguarding Ukraine's data to preserve its present and build its future', 9 June 2022.

[21] Biasini, N. et al., 'Ukraine campaign delivers defacement and wipers, in continued escalation', Talos in the Headlines Blog, 21 Jan. 2022.

[22] Beecroft, N., 'Evaluating the international support to Ukrainian cyber defense', Carnegie Endowment for International Peace, 3 Nov. 2022.

assistance; and the protection of [Microsoft's] employees' in Ukraine, Russia and 'the broader region'.[23] While noting that Microsoft is 'a company and not a government or a country', this statement emphasized an unprecedented level of close consultation with the Ukrainian government, the EU, European states, the US government, the North Atlantic Treaty Organization (NATO) and the UN. In fact, the US deputy national security adviser for cyber and emerging technologies, Anne Neuberger, reportedly asked if Microsoft would consider sharing details of the FoxBlade code with Estonia, Latvia, Lithuania, Poland and other European states (see section II), to address US concerns that the malware would spread beyond Ukraine's borders and cripple NATO or West and Central European banks.[24] Microsoft's support for Ukraine became even more direct in April 2022, when it obtained a court order authorizing it to take control of seven internet domains belonging to the Russian hacking group Strontium (also known by other names, such as Sandworm; see section II), which the group had allegedly used to conduct cyberattacks against media organizations, government institutions and think tanks in Ukraine, the USA and the EU.[25]

In February 2022, in addition to asking for Starlink satellite internet terminals (see section III), Mykhailo Fedorov, a Ukrainian vice-prime minister and minister of digital transformation, appealed to 'all major crypto exchanges to block addresses of Russian users' in order to freeze ordinary users, not just Russian and Belarusian politicians.[26] In response, Binance, a cryptocurrency exchange, said that it would block 'accounts of those on the sanctions list' but would not extend this to ordinary users.[27] Dmarket, a non-fungible token (NFT) platform originating from Ukraine, took a more comprehensive approach by cutting 'all relationships with Russia and Belarus', prohibiting sign-ups and freezing the assets of previously registered users in these countries.[28] In March 2022 Fedorov requested that two US computer software companies—Oracle and SAP—end their business relationships in Russia, to which the companies reportedly agreed.[29]

[23] Smith, B., 'Digital technology and the war in Ukraine', Microsoft on the Issues Blog, 28 Feb. 2022.

[24] Sanger, D. E., Barnes, J. E. and Conger, K., 'As tanks rolled into Ukraine, so did malware. Then Microsoft entered the war', *New York Times*, 28 Feb. 2022.

[25] Burt, T., 'Disrupting cyberattacks targeting Ukraine', Microsoft on the Issues Blog, 7 Apr. 2022; and Microsoft, Digital Security Unit, 'An overview of Russia's cyberattack activity in Ukraine', 27 Apr. 2022.

[26] Mykhailo Fedorov (@FedorovMykhailo), Twitter, 27 Feb. 2022, <https://twitter.com/FedorovMykhailo/status/1497922588491792386>. See also Osborne, C., 'Ukraine asks cryptocurrency firms to block Russian users', ZDNET, 1 Mar. 2022.

[27] Wilson, T., 'Crypto exchange Binance blocks Russian users targeted by sanctions', Reuters, 28 Feb. 2022.

[28] Osborne, 'Ukraine asks cryptocurrency firms to block Russian users' (note 26).

[29] Osborne, C., 'Ukraine calls for corporate support as Oracle suspends Russian operations', ZDNET, 2 Mar. 2022.

Not all cases of industry cooperation with Ukraine, however, have resulted in Russian cyber-related interests being successfully isolated. In part, this has been complicated by alleged Russian false flag operations.[30] To circumvent cyberspace-related restrictions, Russia created its own transport layer security (TLS) certificate authority—a trusted entity that issues digital certificates to authenticate content sent from web servers.[31] This solved website access problems following sanctions that prevented certificate renewals and caused browsers to block access to sites with expired certificates. Moreover, not all cyberspace entities have complied with sanction requests from Ukraine. In March 2022, the Internet Corporation for Assigned Names and Numbers (ICANN) responded to a request from Fedorov, stating:

> Within our mission, we maintain neutrality and act in support of the global Internet. Our mission does not extend to taking punitive actions, issuing sanctions, or restricting access against segments of the Internet—regardless of the provocations. . . . To make unilateral changes would erode trust in the multistakeholder model and the policies designed to sustain global Internet interoperability.[32]

Whether successful or not, such appeals from governments to the private sector have contributed to objections from Russia and China as to the participation of non-governmental stakeholders in OEWG meetings. In 2022, for example, Russia blocked the accreditation of 27 NGOs, including the Cybersecurity Tech Accord, which represents 150 technology companies, from OEWG II meetings.[33]

Challenges to cyber governance from state–non-state cooperation

Some forms of cooperation are potentially more problematic in terms of their impact on cyber governance. In February 2022, for example, Fedorov issued a call for the formation of an Information Technology Army of Ukraine (IT Army)—a crowdsourced community of hackers, including the Anonymous hacker group.[34] Officials from the Ukrainian Ministry of Defence also reportedly approached Yegor Aushev, a Ukrainian businessman and cybersecurity expert, to help organize this unit of hackers via a Telegram channel

[30] Biasini et al. (note 21).

[31] Toulas, B., 'Russia creates its own TLS certificate authority to bypass sanctions', Bleeping Computer, 10 Mar. 2022.

[32] Internet Corporation for Assigned Names and Numbers (ICANN), Letter from Göran Marby to Mykhailo Fedorov, 2 Mar. 2022.

[33] Cybersecurity Tech Accord, 'Industry perspective rejected: Cybersecurity Tech Accord releases joint statement on veto by UN cyber working group', 21 July 2022; and Hurel, L. M., 'The rocky road to cyber norms at the United Nations', Council on Foreign Relations, 6 Sep. 2022.

[34] Brewster, T., '"If Kyiv falls, we keep hacking Putin": On the cyber front line in Ukraine', *Forbes*, 25 Feb. 2022; and Miller, M., 'Ukraine's largest telecom stands against Russian cyberattacks', Politico, 7 Sep. 2022.

listing new Russian targets for volunteers to attack.[35] The head of the Ukrainian mobile operator Kyivstar stressed that Ukraine's IT Army has been essential to the company's defence, while the deputy head of the SSSCIP, Victor Zhora, expressed gratitude for its assistance but stressed that the IT Army had no government connection.[36]

This nexus of state and non-state actors has complicated already contentious UN norm-building efforts, particularly when it comes to cyberattacks on civilian critical infrastructure. According to the Ukrainian Ministry of Digital Transformation—the ministry headed by Fedorov—by late February 2022 the IT Army had conducted offensive cyber operations against the Russian public services portal; financial targets including the Moscow Stock Exchange, Sberbank, the BestChange cryptoexchange and the Belarusian National Bank; the websites of the FSB, Roskomnadzor (the media regulation agency), the president, the government and the parliament; and media organizations including TASS, *Kommersant* and Fontanka.[37] The targets cited for potential cyberattack by the IT Army also included railways and the power grid, while an Anonymous-affiliated hacking group called NB65 made disputed claims to have 'shut down the control center' of Russia's Roscosmos space agency.[38]

Whether or not these incidents are regarded as a legitimate response to Russia's aggression, Ukraine's promotion of non-state and state cyberattacks on civilian critical infrastructure inside Russia suggests a longer-term challenge for cyber governance.[39]

Conclusions

The war in Ukraine has witnessed numerous cyberattacks against both civilian and military critical infrastructure, including government and finance institutions, telecommunications networks and power facilities. These ongoing cyberattacks highlight the difficulties in enforcing cyber norms and enhancing cyber governance.

In the light of continuing hostilities in Ukraine and differing views on priorities for cyber governance, it will be difficult to achieve consensus on future

[35] Reuters, 'Ukrainian cyber resistance group targets Russian power grid, railways', Gadgets360, 2 Mar. 2022.

[36] Miller (note 34).

[37] Ukrainian Ministry of Digital Transformation, 'IT army blocks Russian sites in a few minutes—The main victories of Ukraine on the cyber front', Ukrainian Government Portal, 28 Feb. 2022.

[38] Schectman, J., Bing, C. and Pearson, J., 'Ukrainian cyber resistance group targets Russian power grid, railways', Reuters, 1 Mar. 2022; and Browne, E., 'Roscosmos head rejects Anonymous claim that Russian satellites were hacked', *Newsweek*, 2 Mar. 2022. See also Council on Foreign Relations, 'Ukrainian IT Army'.

[39] For more on these dynamics see Väljataga, A., 'Cyber vigilantism in support of Ukraine: A legal analysis', NATO Cooperative Cyber Defence Centre of Excellence, Mar. 2022.

measures through multilateral deliberations. There remains potential for a future programme of action on cyberspace after the conclusion of OEWG II in 2025, but this proposed mechanism remains contentious. Debates over private sector and NGO involvement in UN processes also highlight the longer-term challenges in engaging both both governmental and non-governmental stakeholders in norm building and in enforcement.

Nevertheless, there are points of intersection, such as Russia's engagement in bilateral efforts to address cybercrime and the Counter Ransomware Initiative's action plan to combat ransomware, which may have implications for addressing evolving trends in cyberwarfare. However, the crossover between cybercrime tactics and cyberwarfare aims, combined with state engagement of non-state actors in conducting cyberattacks, means that there is greater work to be done on incorporating these points of intersection into cyber governance processes.