Cyber peace and security

Women's International League for Peace and Freedom

Background

The terms cyber or digital security have come to include an ever-widening spectrum of activities. These include espionage, surveillance, privacy intrusions, denial-of-service attacks, ransomware, and malware operations that variously impact states and individuals, and that can either target or utilise information and communications technology (ICT). Many of these activities have the ability to disrupt, disable, or destroy vital physical infrastructure or national or human security and well-being. Cyber operations have become an effective tool for states seeking to exercise power by causing disruption or confusion in other countries. Such operations are also transforming espionage. Digital technology has added new means by which governments can control or repress the human rights of individuals or groups.

There are also important points of intersection with militarism and traditional arms proliferation: for example, the dark web facilitates illicit arms trafficking while certain other technologies raise concerns related to surveillance and intelligence gathering. The vulnerability of certain existing weapon systems to digital attack present new areas of alarm, but also compelling incentives to disarm.

Since the first instances of malicious cyber operations between states were uncovered, there has been a growing pre-supposition of cyber space as a militarised one. This has been reinforced by the adoption of national cyber strategies that allow for offensive operations or for their integration into military activities. Given the overwhelming civilian use of ICTs, it's vital to protect and promote peace in cyber space as based on a human-centric understanding of security and diversity of perspectives.

In 2018, the First Committee established its sixth Group of Governmental Experts (GGE) and for the first time, an Open-Ended Working Group (OEWG) on ICTs. These are meeting concurrently throughout 2020 and 2021.[1] The two entities have similar, yet not identical, mandates. They also have varying modalities to receive inputs from non-governmental stakeholders or non-Group members. The creation of two similar bodies was against the preference of most UN member states; they emerged as a result of friction between the United States and Russia, each of which sponsored the respective resolutions that led to the establishment of each.

Current context

The COVID-19 pandemic has illustrated the substantial role that ICTs play in multiple dimensions of our lives and the importance of meaningful access to them. Yet, cybercrime against individuals has increased by up to 600 per cent since the start of the pandemic.[2] Multiple digital operations targeting medical facilities worldwide have sought to undermine responses to the health crisis, spread misinformation, or exploit our current increased reliance on digital connectivity.[3] Some governments are instituting digital contact tracing applications that raise concerns about privacy, surveillance, and human rights.[4]

More governments are reporting “attacks” against their critical infrastructure in this time as well.[5] This shows that actors are increasingly incorporating ICT use into their strategies to retaliate against perceived aggressions, or to cause disruption elsewhere; and that relevant norms against such behaviour are not being respected.

Within the First Committee context, the OEWG on developments in the field of ICTs held its first substantive session in September 2019 and its second in February 2020. The third and final substantive session was scheduled for July 2020, in which member states would have sought to adopt a final report containing decisions and recommendations in line with the six agenda items it has focused on: threats, norms and principles; international law; confidence building measures; capacity building; and regular institutional dialogue. [6] It has been tentatively rescheduled for March 2021, although that may require formal confirmation through the General Assembly.

To maintain momentum, OEWG Chair Jürg Lauber of Switzerland is convening a series of informal consultations. A pre-draft report was released in March 2020 and will form the basis of the informal consultations.[7] Participating member states have found much common ground in most of the six agenda items, but significant differences remain in the topics of international law and regular institutional dialogue. There is also some divergence of views about the need for new international law in this area or if the existing norms are sufficient.

In December 2019, more than 100 representatives of civil society, academia, and industry participated in a three-day informal OEWG multi-stakeholder session. Non-governmental organisations without ECOSOC status have been prevented from participating in formal OEWG meetings and civil society has so far not been granted access to any of the virtual informal consultations. Non-governmental stakeholders can make written submissions to the OEWG, which are then made available online.[8]

The GGE held its first meeting in December 2019 but will not submit a final report to the General Assembly until 2021. The group is comprised of 25 members who are working in a personal capacity and is chaired by Ambassador Guilherme de Aguiar Patriota of Brazil. It is also examining new modalities to meet amidst the pandemic.

Recommendations

During First Committee, delegations should:

- Articulate views and priorities for the GGE and OEWG;

- Speak out against hostile and provocative actions in cyberspace and the militarisation of technology, and speak in favour of cyber peace, human rights, and human security; and

- Support the full inclusion of civil society in future meetings of the OEWG; mechanisms for input with the GGE; and any future relevant bodies.

Beyond First Committee, states should:

- Halt the development and use of offensive cyber capabilities, strategies, and doctrines, in particular against critical health infrastructure;

- Adhere to the agreed norms for state behaviour in cyberspace and establish accountability mechanisms;

- Work cooperatively to ensure mutually reinforcing outcomes between the GGE and OEWG and other normative frameworks;

- Supporting technical capacity building to build cyber resilience; and

- Refrain from undertaking or facilitating any repression of human rights or freedoms through digital means.

Author: Allison Pytlak

[1] Learn more: https://www.reachingcriticalwill.org/disarmament-fora/ict.

[2] "UN Warns Cybercrime on Rise During Pandemic," 23 May 2020, https://www.voanews.com/covid-19-pandemic/un-warns-cybercrime-rise-during-pandemic.

[3] See https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19.

[4] See Ray Acheson, "The Risks of Relying on Technology to "Save Us" from the Coronavirus," Women's International League for Peace and Freedom, https://www.wilpf.org/covid-19-the-risks-of-relying-on-technology-to-save-us-from-the-coronavirus/ and Danny Palmer, "Security experts warn: Don't let contact-tracing app lead to surveillance," 7 May 2020, https://www.zdnet.com/article/security-experts-warn-dont-let-contact-tracing-app-lead-to-surveillance/.

[5] See, for example, "Australia cyber attacks: PM Morrison warns of 'sophisticated' state hack," BBC News, 19 June 2020, https://www.bbc.com/news/world-australia-46096768; "Cyberattack shuts down Canadian government accounts," CNN, 17 August 2020, https://www.cnn.com/2020/08/17/tech/cyberattack-canada-government-accounts/index.html; and "Iran threatens retaliation after what it calls possible cyber attack on nuclear site," Reuters, 3 July 2020, https://www.reuters.com/article/us-iran-nuclear-natanz/iran-threatens-retaliation-after-what-it-calls-possible-cyber-attack-on-nuclear-site-idUSKBN2441VY#:~:text=DUBAI%20(Reuters)%20%2D%20Iran%20will,been%20caused%20by%20cyber%20sabotage.&text=nuclear%20watchdog.

[6] Coverage of all open OEWG meetings is available via the *Cyber Peace and Security Monitor,* https://www.reachingcriticalwill.org/disarmament-fora/ict/oewg/cyber-monitor.

[7] Dates and documents can be found on RCW's page for the OEWG: https://www.reachingcriticalwill.org/disarmament-fora/ict/oewg.

[8] See https://reachingcriticalwill.org/disarmament-fora/ict/oewg/documents#papers and https://www.un.org/disarmament/open-ended-working-group/.