Cyber space
Women’s International League for Peace and Freedom

Background
The word “cyber” has come to refer to an ever-widening spectrum of activities encompassing espionage, surveillance, privacy intrusions, denial-of-service attacks, ransomware, and malware operations that variously impact nations and individuals. Many of these activities have the ability to disrupt, disable, or destroy vital physical infrastructure or national or human security and well-being. Some constitute criminal activity while others occur within legal grey areas. Cyber operations have become an effective tool for states seeking to exercise power by causing disruption or confusion in other countries and is transforming espionage. Digital technology has added new means by which governments can control or repress the human rights of their citizens.

There are 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 is a dangerous path for states to continue down, given the civilian and dual-use nature of cyberspace and digital networks. By treating this primarily as a military and security issue, states and other actors risk institutionalising and taking for granted the inevitability of cyber conflict.

In the ongoing discussions about norms of responsible behaviour in cyberspace and increasing ubiquity of digital networks and tools, it’s essential that actors adhere to already agreed norms. But it’s also vital that space is given to articulating the means to guarantee and protect a peaceful cyber space, as based on a human-centric understanding of security and diversity of perspectives.

Current context
The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE on ICTs) is the most immediately relevant UN forum covering cyber issues for First Committee delegates. The first GGE on ICT was established in 2004 with a general purpose of examining existing and potential threats in cyberspace and possible cooperative measures to address them. Subsequent groups expanded the membership slightly and worked to develop
behavioural norms for actions in cyberspace. Following the fourth Group’s adoption of what was generally regarded as a “groundbreaking” report in 2015, expectations were high for the fifth Group, but it was unable to agree to a consensus report at its final meeting in June 2017. Major points of contention were the applicability of international humanitarian law and Article 51 of the UN Charter to the ICT environment, over which the majority of participating Western states had views different to that of China, Russia, and Cuba.

Following this stalemate and breakdown, UN discussions were at an impasse. In 2018, Russia introduced new and controversial elements into the annual UNGA First Committee resolution, prompting the United States to draft its own counter-resolution. While Russia ultimately modified some of the more problematic elements of its draft, wider politicisation during the 2018 UNGA First Committee session contributed to the inability of either states to meet at a compromise. As a result, the UNGA established both a new GGE and for the first time, an Open-Ended Working Group (OEWG) that will meet concurrently throughout 2020 and 2021. The two entities have similar, yet not identical, mandates and varying modalities to receive inputs from either non-governmental stakeholders or, in the case of the GGE, non-Group members.

The OEWG on developments in the field of information and telecommunications in the context of international security, chaired by Swiss Ambassador Jürg Lauber, is open to the entire UN membership. Its first substantive session is in September 2019, with others in February and June. An intersessional meeting with industry and civil society is planned for December 2019, in an effort to ensure broader inclusivity. Yet non-governmental organisations without ECOSOC status have been denied access to observe the September session.

The GGE will hold its first meeting in December 2019 but will not submit a final report to the General Assembly until 2021. The group will be comprised of 25 members, who are working in a personal capacity. It will be chaired by Ambassador Guilherme de Aguiar Patriota of Brazil, who will additionally hold two informal consultations with all UN member states as well as six regional consultations, some of which have already occurred, again in an effort to improve inclusivity.

It will be important that these entities work toward mutually reinforcing outcomes and avoid contradicting one another. In addition, states will need to account for an ever-growing external patchwork of global and regional discussion fora for various stakeholders and ensure input from wider stakeholders into their deliberations. During the 2019 First Committee, it is likely that this message will be reinforced by many states parties who expressed frustration at the outcome in 2018. It is also likely that member states will outline their views and priorities for both entities, notably as the first session of the OEWG will have just occurred.

Recommendations

*During First Committee, delegations should:*

- Speak out against hostile and provocative actions in and the militarisation of cyberspace, and speak in favour of cyber peace and human security online;
- Express concern about unlawful surveillance and digital censorship activities that violate human rights; and
• Articulate their views and priorities for the GGE and OEWG.

**Beyond First Committee, states should:**
• Uphold the behavioural norms that already enjoy broad support;
• Work cooperatively ensure mutually reinforcing outcomes between the GGE and OEWG;
• Ensure information sharing between different international processes that address cyber issues, both within and outside of the UN system;
• Support technical capacity building initiatives; and
• Refrain from undertaking or facilitating any repression of human rights or freedoms through digital means.

*Author: Allison Pytlak*

---

3 More detailed information on dynamics during the 2018 First Committee is available through our coverage in the 2018 First Committee Monitor, available http://reachingcriticalwill.org/disarmament-fora/unga/2018/fcm.
4 For more information on both processes visit http://reachingcriticalwill.org/disarmament-fora/others/ict.
5 Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, and Uruguay.