Civil society statement on cyber peace and human security
UN General Assembly First Committee on Disarmament and International Security
18 October 2019

Much has happened in multilateral cyber security since the First Committee met one year ago.

The work of two new UN General Assembly-mandated bodies is underway. The first session of the Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security took place in September, marked by a refreshingly positive atmosphere.

The UN's sixth Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace will begin its formal work in December following several regional consultations.

There is effective on-going regional collaboration and cooperation in the area of cyber security.

Unfortunately, other developments have occurred that are far less positive. The pace and severity of malicious operations in cyber space have increased noticeably. The use of cyber technologies as tools of or targets for aggression is becoming more regular and, as a result, normalised by a larger number of states. The last year has seen a spike in data breaches, malware attacks, disinformation campaigns, and continued use of proxies by states.

These patterns show that the trend toward a militarised cyber space is deepening. It is manifesting through the adoption of more offensive strategies and doctrines, aggressive behaviours, and in the vocabulary used to describe cyberspace and actions within it.

It is also manifesting in how governments are using these technologies and spaces to restrict human rights, such as through surveillance, hacking, censorship, and intentional disruption of internet services and access. These measures have been shown to disproportionately impact individuals and groups in society, such as journalists, LGBT and gender non-conformists, women, and human rights defenders, and other people in positions of vulnerability or marginalisation.

These activities all contradict existing normative commitments and must cease. Those responsible must also be held to account. The civil society organisations supporting this statement reject any acceptance or legitimisation of problematic practices that threaten peace in cyber space. We are supportive of solutions that move the global community closer to cyber peace. To that end, we urge the following:

- Halt the development and deployment of offensive cyber capabilities, strategies, and doctrines, which in the absence of transparency and accountability frameworks are leading to the militarisation of cyber space and must be challenged. Instead, the root causes underlying the pursuit of aggressive cyber capabilities must be addressed.

- Implement the already-agreed norms for behaviour in cyber space. While more work is needed to interpret and further develop normative frameworks, the recommendations endorsed by the UN General Assembly in 2013 and 2015 constitute an agreed baseline intended to guide state behaviour and prevent conflict in cyber space that cannot be dismissed and overlooked.

- Attribution is a precondition for ensuring valid accountability. The international community needs to develop independent and impartial capabilities to attribute responsibility for malicious cyber operations.

- Put human security at the heart of cyber security, by recognising that international human rights law applies during times of peace and conflict, including in cyber space. Cyber security includes the protection of human rights, and cyber security-related laws, policies and practices should not be used as a pretext to violate human rights.

- Work toward bridging differences of opinion and building shared understandings, regarding in particular the applicability of international humanitarian law, while retaining the goal of a cyber space free of armed conflict. Efforts must also be made to address the legal challenges posed by state use of proxies in cyber operations.

- Improve transparency and access to UN cyber security fora for non-governmental stakeholders and ensure complementarity between the OEWG and GGE processes while taking into account the norms and dialogue that have occurred in forums external to them, including within human rights bodies.

This statement has been endorsed by 14 organizations working in the areas of peace, disarmament, human rights, and digital security. Their names are listed below and in the online version of this statement, posted on the Reaching Critical Will website.

Endorsed by:
Access Now
Acronym Institute for Disarmament Diplomacy
Article 36
Association for Progressive Communications
Colombian Campaign to Ban Landmines
Derechos Digitales
Global Partners Digital
ICT4Peace

International Peace Bureau
Korean Progressive Network Jinbonet
PAX
Peace Movement Aotearoa
Peace Track Initiative
Women’s International League for Peace and Freedom
World Federalist Movement - Canada