Joint civil society statement on cyber peace and human security
UN General Assembly First Committee on Disarmament and International Security
13 October 2020

Dialogue and action to protect information and communications technology (ICTs) has—relative to the rate of technological development—progressed slowly in the UNGA First Committee. Often, the security and peaceful uses of cyber space and ICTs have felt more like distant concepts rather than the urgently evolving matter of concern that they are; discussed behind closed doors by only a handful of UN member states.

Recent events are compelling greater attention at last.

The COVID-19 pandemic has illustrated the substantial role that ICTs play in multiple dimensions of our lives, which underscores both their ubiquity and the importance of meaningful access to ICTs.

Yet, cybercrime has, according to some estimates, increased by up to 600 per cent since the start of the pandemic. Multiple digital operations targeting medical facilities worldwide seek to undermine responses to the health crisis, spread misinformation, or exploit our current increased reliance on digital connectivity. Some governments are instituting digital contact tracing applications that raise concerns about privacy, surveillance, and human rights; while internet shutdowns are impeding access to updates on health measures and other relevant safety information. Online gender-based violence, including surveillance, has increased, and the gender digital divide has become more blatant.

Indeed, throughout the UN General Assembly's high-level debate this year a record number of leaders highlighted digital insecurity and hostile cyber activity as among the key threats facing our world today.

On an inter-state level, reports of hostile operations against critical infrastructure have increased in this time of uncertainty and instability as well. More states are adopting offensive strategies and doctrines. Actors are increasingly incorporating ICT use into their strategies to disrupt systems in other countries. Relevant norms against such behaviour, including those adopted by UNGA member states in 2013 and 2015, are not being respected.

An accountability gap clearly exists and it is one that enables the drift toward a more militarised cyber space and further weaponisation of technology. The use of digital technologies as tools of, or targets for, aggression is becoming more frequent and, as a result, more normalised, by a growing number of states and other actors.

The pandemic has negatively impacted the two UN General Assembly First Committee-mandated bodies on this subject: the sixth Group of Governmental Experts (GGE) on state behaviour in cyber space, and the Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security. The OEWG was on a good trajectory before having to postpone several planned informal consultations and its third and final substantive session because of the pandemic; a challenge then made more complex by political dynamics amongst states. It's encouraging that a series of informal virtual dialogues will maintain momentum until the final OEWG session can occur, but non-governmental stakeholders have once again found themselves shut out of these talks, compounding pre-existing issues of stakeholder access.

Against this backdrop, the civil society organisations supporting this statement urge the following:

- Halt the development and deployment of offensive cyber capabilities, strategies, and doctrines, in particular against critical infrastructure, including health infrastructure, which in the absence of transparency and accountability frameworks are leading to the militarisation of cyber space and must be challenged.
- Implement the already-agreed norms for behaviour in cyber space. While more work is needed to interpret them, and potentially develop additional norms or laws, 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. This cannot be dismissed and overlooked.
- Close the accountability gap by adopting multilateral mechanisms that will foster transparency and information sharing, such as through reporting, peer review processes, or independent and impartial attribution capabilities.
- 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 must be understood to include the protection of human rights, and cyber security-related laws, policies and practices should not be used as a pretext to violate those rights.
- Promote and ensure regular and meaningful participation of non-governmental stakeholders in UN cyber security fora and include this as a priority for future institutional dialogue.
- Bridge differences of opinion. States should seek complementarity between the OEWG and GGE processes while taking into account the behavioural norms and regulations that have emerged from non-UN forums, including within human rights bodies.

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

Endorsing organisations:
Acronym Institute for Disarmament Diplomacy
APP-Argentina
Article 36
Association for Progressive Communications
ICT4Peace
Latin America and Caribbean Human Security Network (SEHLAC)
Nuclear Age Peace Foundation
PAX
Women's International League for Peace and Freedom