Joint civil society statement on cyber peace and human security
UN General Assembly First Committee on Disarmament and International Security
8 October 2021
(Delivered by Allison Pytlak, Women's International League for Peace and Freedom)

It has been an important year for multilateral efforts seeking to advance international cyber peace and security within the United Nations.

Both of the First Committee-established cyber processes concluded their work in the first half of 2021. The sixth Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyber space and the first Open-ended Working Group (OEWG) on information and communications technologies (ICTs) both adopted reports[1] by consensus that re-affirm past agreements and recommendations, while also setting out some new understandings. Despite the politicised establishment of the two groups, their respective outputs are substantive and highly complementary. They have also generated momentum toward the establishment of new and potentially more permanent forums. Moreover, the high level of participation in the OEWG from diverse governmental and non-governmental stakeholders speaks to the importance of this issue. It also demonstrates that a wide range of stakeholders, including those affected by cyber security, have a crucial role to play in the First Committee-cyber processes.

Despite these developments, the threat landscape is bleak. Throughout the COVID-19 pandemic, operations targeting medical facilities and agencies worldwide have sought to undermine responses to the health crisis, spread misinformation, or exploit our reliance on digital connectivity for nefarious ends. Multiple high-profile operations involving supply chains, and critical physical and information infrastructure, have shown the far-reaching impacts of aggressive action in cyber space. Such actions demonstrate that the legal ambiguities surrounding the application of international law to state behaviour in cyber space are being exploited, and that relevant norms against such behaviour are not being respected.

Meanwhile, disturbing revelations about human rights abuses enabled by surveillance technologies have prompted warnings from the UN High Commissioner for Human Rights and calls for a moratorium on their sale. And within disarmament and arms control processes, there is rising concern about the digital vulnerabilities of existing weapon systems and the implications for illicit weapons trafficking.

Whatever its form, technology-facilitated violence must be understood in light of its impact on lives and livelihoods. Human security is at the heart of cyber security and therefore demands human-centric and rights-based approaches to establishing a peaceful ICT environment. It has been encouraging to see a growing number of states call for such an approach including recognition of the differentiated impact of cyber operations on marginalised people, women and girls, and people of diverse sexualities and gender expressions.

With the above considerations in mind, the 13 organisations endorsing this statement offer the following recommendations to member states at the First Committee:

- Halt the development and deployment of intentionally harmful cyber capabilities, strategies, and doctrines, in particular those directed against critical infrastructure, including health and information infrastructure, and the public core of the Internet.
- Implement the already-agreed norms for behaviour in cyber space while seeking common understandings about *how* international law, including international humanitarian and human rights law, applies to state action in cyber space.

[1] See A/76/135 (GGE final report) and A/AC.290/2021/CRP.2 (OEWG final report).

- States should follow through on the recommendations in the GGE and OEWG final reports to publicly release statements on how they understand their own obligations for responsible behaviour under international law.
- States should also invoke international law or refer to the UN norms when condemning state-led and -sponsored cyber actions to build awareness of and support for legal and normative limitations.

- Close the existing accountability gap by adopting multilateral mechanisms that will foster transparency, uphold state responsibility, and prevent conflict, as well as deter technology-enabled human rights abuses.
  - States should establish a permanent forum to consider international cyber peace matters. After 23 years of UN cyber talks, ad-hoc deliberations do not go far enough to meaningfully address current and future threats. While the establishment of the second OEWG is welcome, continuity is important. In this regard, the proposal for a cyber programme of action, now supported by over 50 states, merits expedited examination.
  - Whether in the second OEWG or a future permanent forum, states should prioritise establishing accountability mechanisms. Proposals have already been circulated in the OEWG and elsewhere, that variously outline possible peer review processes, surveys, reporting practices, and the creation of structures for independent and impartial attribution.

- Recognise the human rights impact of international cyber operations and refrain from using cyber security-related laws, policies, and practices as a pretext to violate human rights and fundamental freedoms.

- Ensure the regular and meaningful participation of non-governmental stakeholders in the second OEWG and in any future UN forums. Diverse actors have an established role to play in operationalising and promoting the cyber norms and relevant international law, building capacity and resilience, and in monitoring and responding to cyber incidents. This experience and expertise needs to be better integrated into UN cyber dialogues.

- Seek complementarity and communication between and among the various processes on cyber-related issues and digital security, including those established by the First Committee, the Third Committee, the UN Secretary-General, and related human rights and technical bodies.

This statement has been endorsed by:

Acronym Institute for Disarmament Diplomacy
Association for Progressive Communications
Colombian Campaign to Ban Landmines
Cybersecurity Tech Accord
Derechos Digitales
Digital Peace Now Society
Global Partners Digital
ICT4Peace
Jokkolabs Banjul
Kaspersky
Media Rights Agenda
Microsoft
Women’s International League for Peace and Freedom