Joint civil society statement on cyber peace and human security

UN General Assembly First Committee on Disarmament and International Security
13 October 2022

One year ago, civil society jointly delivered a statement to this Committee in which we acknowledged that, despite several important developments in the United Nations to advance international cyber peace and security, the threat landscape remained bleak.

Unfortunately, several of the concerns we highlighted then persist and the overall security of the online environment continues to deteriorate.

Offensive cyber capabilities are more widespread among states, as is the use of cyber mercenaries. Cyber operations have become more frequent and more sophisticated, including in their targeting of critical infrastructure and to disrupt critical services such as healthcare, as well as supply chains, including information and communications technology (ICT) supply chains.

Within disarmament and arms control processes, states and civil society have registered concern about the digital vulnerabilities of existing weapon systems, including nuclear weapons.

In the context of the ongoing Russian invasion of Ukraine, cyber operations are being frequently employed in support of or alongside kinetic military operations to disrupt delivery of critical civilian services or against critical infrastructure. These operations have impacted the civilian population, while also causing destabilizing spill-over effects. The use of cyber in the hostilities between Russia and Ukraine raises important points for clarifications with regard to the application of international law and international humanitarian law in particular—while simultaneously underscoring the need for accountability mechanisms and clear condemnation of acts which violate international law and agreed norms of state behaviour in cyberspace.

The Internet and connected devices are being weaponised in ways that have impacts on human rights, such as through surveillance, hacking, censorship, and intentional disruption of internet services and access. These measures have been shown to disproportionately impact and harm individuals and groups in society, such as journalists, human rights defenders, LGBT individuals, women, and others who may already be in positions of vulnerability or marginalisation.

The toll of unrestrained cyber operations on human security mounts daily and as such, discussions and decisions arising from the relevant UN processes needs to address them more effectively. These efforts should be guided by human-centric and rights-based approaches to establishing a peaceful ICT environment, including the principle of inclusivity and meaningful stakeholder engagement. The accreditation modalities that have allowed the vetoing of over 30 non-governmental stakeholders from participating in the UN Open-ended Working Group (OEWG) on ICTs, for example, should improve to allow meaningful participation of all relevant stakeholders. Despite recent progress in OEWG participation modalities, there is much room for improvement.

Against this backdrop, we collectively set out the following calls to action:

- Halt the deployment and use of harmful cyber capabilities, activities, strategies, and doctrines. We are particularly concerned over actions directed against critical infrastructure and services, including health and information infrastructure; the public core of the Internet, actions against the humanitarian sector; the use of cyber mercenaries; and those that impact people, especially civilians.

- Take urgent action to implement the agreed cyber norms and operationalise the cyber capacity-building principles agreed to by the 2019-2021 OEWG, in cooperation and consultation with non-governmental stakeholders.

- Take rapid action to establish mechanisms that will foster transparency and close accountability gaps. Ad-hoc deliberations such as those currently existing within the UN do not go far enough to meaningfully address current and future threats—a permanent UN forum with meaningful stakeholder engagement is needed. In this regard, the proposal for a cyber programme of action merits expedited consideration.

- Conduct focused discussions and exchanges about *how* international law applies in the ICT environment. It is encouraging that more states are publishing their national interpretations and understandings about how international law governs their cyber behaviour but more ambition is needed. In particular, states should put forward opinion juris that reaffirms the applicability of international human rights law in cyberspace, at all times. The international community including non-governmental actors could also map gaps in existing law and produce recommendations for addressing them, with a view to building on, not duplicating, existing work in this area.

- The growing tendency of states to attribute responsibility for cyber operations is positive, but we would support greater transparency in the criteria and attribution policies used and encourage states to invoke international law or refer to the UN norms when condemning state-led and -sponsored cyber actions in order to build awareness of and support for legal and normative limitations.

- 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. For this, states should recognise and address the differential impacts of cyber operations on individuals and groups in society who are already in positions of vulnerability or marginalisation, such as journalists, human rights defenders, LGBT individuals, and women, among others. Relevant outputs from the UN human rights community, including the Human Rights Council and the Office of the High Commissioner on Human Rights, offer guidance in this regard.

- Ensure the regular and meaningful participation of non-governmental stakeholders in the current 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, building confidence, and in monitoring and responding to cyber incidents. This experience and expertise need 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 as well.

This statement was delivered by:

Allison Pytlak, Women's International League for Peace and Freedom

This statement has been endorsed by:

Association for Progressive Communications (APC)
Campaña Colombiana Contra Minas and SEHLAC
Center for Middle East Affairs
Centre for Feminist Foreign Policy
Center for Peace Education-Miriam College
CyberPeace Institute
Derechos Digitales
Foundation for Media Alternatives (FMA)
Fundación Karisma
Global Partners Digital
ICT4Peace
Igarapé Institute
Jokkolabs Banjul
JONCTION
KICTANet
Korean Progressive Network Jinbonet
Media Rights Agenda
Microsoft
Pax Christi-Pilipinas
Project Ploughshares
Red en Defensa de los Derechos Digitales
SEHLAC
Women's International League for Peace and Freedom
World Federalist Movement – Canada