Civil Society Statement on Cyber

UNGA First Committee on Disarmament and International Security, 15 October 2026

Thank you, Chair. I am delivering this statement on behalf of seven civil society organisations and individuals that have signed onto it.

Concerns about the misuse of information and communications technologies (ICTs) and malicious cyber activity continue to grow among the international community. Cyber operations continue to pose threats to peace and security, alongside causing a range of human rights violations. Marginalised populations are disproportionately harmed by practices such as surveillance, state-sponsored malicious cyber operations activities, censorship, intentional disruption of internet services and access, and physical tampering of the supply chain. Additionally, non-state actors launch ransomware attacks, exploit supply chains, and run large-scale fraud operations that inflict significant economic and social harm. Widespread adoption and use of AI is fundamentally changing the cyber landscape.

During this First Committee session, we call on delegations to condemn the malicious use of ICTs by state and non-state actors alike, given their adverse effects on people globally and the challenge they pose to progress under all three pillars of the UN's mandate. Cyberspace has become a domain of strategic competition, and the use of ICTs in conflict, crisis and in peacetime raises risks of miscalculation and escalation.

We urge UN member states to act according to their commitment that international law, including the UN Charter, international humanitarian law, and international human rights law, applies fully to state conduct in cyberspace. States may want to use the First Committee as an opportunity to expand on progress in national or regional norms implementation, or outline views on how international law applies to use of ICTs. We also raise the urgency of moving from agreed principles to implementation of the Framework of Responsible State Behavior, including its voluntary, non-binding norms. The norms are not abstract aspiration but provide important guidelines for many pressing cybersecurity threats and challenges, including the protection of critical infrastructure, ensuring the integrity of ICT supply chains, and exercising restraint in stockpiling and exploiting unreported vulnerabilities, among others.

We also call on all states to 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, including through their acquisition and use of commercial capabilities. States should invest in capacity building so that all states, particularly developing ones, can defend their networks and take part meaningfully in global discussions.

Finally, member states should make full use of the new permanent UN mechanism on ICT security as an inclusive forum for dialogue, and engage the private sector, civil society, and the technical community as essential partners. In this regard, we

would like to recall the importance of guaranteeing meaningful civil society participation. This year, over 90 entities applied for accreditation to participate in the Global Mechanism, of which 50 were blocked. As observed in a cross-regional working paper submitted to the Open Ended Working Group in 2024, “The multistakeholder community plays an essential role in promoting cybersecurity by operating and defending infrastructure, maintaining standards, supporting the implementation of agreed norms and international law, advancing capacity and confidence-building measures while also translating international commitments into practical implementation through trusted public-private collaboration, technical expertise, and operational cooperation.”

For years, we have had the chance to shape cyberspace in a way to secure it from malicious activities. While we have not done enough to stop these practices, action to prevent further harm is still possible. Diverse recent operations targeting telecommunications networks, governments and critical infrastructure — including those perpetuated by artificial intelligence — demonstrate what is at stake and why states need to work together. And it starts in this First Committee, with all the delegations present here. We urge you to take this opportunity to make meaningful change towards a more peaceful cyberspace.

This statement was drafted by Laura Varella of Reaching Critical Will with advice from other experts. The statement has been endorsed by the following organisations and individuals:

Organisations:
Association for Progressive Communications (APC)
ICT4Peace
Protect.ngo Foundation
Women’s International League for Peace and Freedom (WILPF)

Individuals:
Akmal Amode-Adame
Allison Pytlak, Sr. Fellow and Program Director at the Stimson Center
Christopher Painter