2025 Statement on cybersecurity, peace, and human security

17 October 2024

UN General Assembly First Committee on Disarmament and International Security
Delivered by Peter Micek on behalf of Access Now

Thank you, Madame Chair. Civil society appreciates this opportunity to address the First Committee on the relationship between cybersecurity, peace, and human security, and how to address urgent risks to human rights.

I deliver this statement on behalf of Access Now, the international civil society organisation that provides digital security assistance and seeks to defend and extend digital rights.

Every day we witness civil society calling for the international community to invest in peace and human security, while more States join an irrational arms race, under the sheen of digital and cyber innovation. This race unfortunately occurs amid the degradation of the international humanitarian framework and threats posed by the increasing use of emerging technologies such as AI and unregulated Lethal Autonomous Weapons.

As we recalled during UNGA last year, the advances in machine learning have led to a boom in AI enthusiasm and investments. Despite the calls by civil society for enforceable, human rights-based legal instruments, all the energy and resources went to fuel AI hype and the defence-oriented tech ecosystem. Investments into defence tech startups grew to $155bn globally between 2021 and 2024, up from $58bn over the previous four years.

And this, while the humanitarian and human rights sector are starved of funding, impacting the dignity of millions. Even the traditionally cautious 'big tech' community is showing no hesitation in having children's toys and lethal autonomous systems next to each other in their AI portfolio.

We cannot but emphasize the need for the United Nations and its member states to address the impact on peace and security of the progressive militarization of commercial tech, which is too often left unaddressed in discussions related to AI governance, most of all on the protection of civilians in conflict. The First Committee has made strides by addressing the use of AI in military domains and must press forward to monitor and protect civilians from these encroaching tools, in coordination with civil society.

Access Now and partners repeatedly flag how discussions on cyberwarfare often omit a clear reflection on how to ensure processes that reestablish peace and human security when hostilities cease, also extend to the digital dimension of people's lives. We need what we define

as a ‘digital ceasefire,’ a new mental and operational model to ensure the protection of peacemakers and negotiators from cyber-related threats.

On cybersecurity, invasive and sophisticated tools for surveillance proliferate, powered by the commercial cyber intrusion sector. Government officials and UN representatives negotiating fragile ceasefires have been targeted, as well as journalists covering conflicts. We welcome the increasing recognition of the threat that this poses to peace and security, alongside its very real-world human rights harms. The Security Council held its first Arria formula meeting on commercial spyware earlier this year, whose findings this Committee should reflect and build on.

Access Now further welcomes the consensus conclusion of the Open Ended Working Group (OEWG) on ICT security (2021-2025) on 11 July 2025 and recognizes the constructive work of its Chair, Ambassador Burhan Gafoor, in bringing delegations to agreement on the final report. We note that Singapore will table a draft resolution in the First Committee to endorse this final report, and we welcome the intent to transition to the new global mechanism on developments in ICTs in the context of international security. We also welcome the OEWG’s final Annual Progress Report and its note on the dangers posed by commercial cyber intrusion marketplaces and the efforts being increasingly made by states for further standards and action in this sector.

However, we must emphasize that this institutional transition, while necessary, must represent far more than a procedural shift. We need a genuine and binding commitment to establish permanent, accountable multilateral structures with in-built stakeholder participation for cyber governance. The reality is that time-limited deliberations, despite years of successive working groups and expert processes, have proven inadequate to the scale and speed of evolving cyber threats and their devastating impacts on human rights and human security. We therefore call on member states to ensure that the operationalization of the global mechanism and the establishment of the global ICT security cooperation and capacity-building portal prioritize meaningful civil society participation, robust accountability mechanisms that will hold states responsible for their cyber actions, and human-rights-centered approaches to digital security.

This institutional transition presents a critical opportunity to embed permanent oversight mechanisms into global governance of cyberspace, mechanisms that will ensure international law and agreed normative frameworks are not merely aspirational statements confined to conference rooms, but are operationalized and subject to regular, transparent review by all stakeholders, including non-state actors.

Thank you, Chair.