2024 Joint civil society statement on cyber and human security

UN General Assembly First Committee on Disarmament and International Security
Delivered by Peter Micek on behalf of Access Now, October 16, 2024

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

The internet and connected devices are being weaponized in ways that negatively impact human rights and human security, such as through surveillance, state-sponsored cyber attacks, censorship, intentional disruption of internet services and access, and physical tampering of the supply chain. Digital systems that are becoming so ubiquitous in people's lives are turned into a source of risk and threat with concrete repercussions on the safety of their owners and their families, transforming digital risk into physical harm.

These measures disproportionately impact and harm people and groups in society based on their race, gender, sexual orientation, gender identity or expression, and other characteristics or because of their professions such as journalists, aid workers, human rights defenders, or others in situations of vulnerability.

In this context, the rapid deployment of artificial intelligence systems compounds and scales risks. In a 2023 resolution, the UN General Assembly's Third Committee called on states "to refrain from or cease the use of artificial intelligence applications that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights." The First Committee should similarly clarify where certain applications of AI may fail to its standards for the protection of peace and human security.

As recently recalled by the States in the *Pact for the Future*, "Our efforts to urgently address accumulating and diverse threats to international peace and security, on land, at sea, in the air, in outer space, and in cyberspace, should be supported by efforts to rebuild trust, strengthen solidarity and deepen international cooperation." This cannot happen by just recycling the old mental and governance models for the digital era. We need to reimagine preventive action through human-centric and rights-based approaches, informed by a process of meaningful stakeholder engagement that puts communities and especially vulnerable groups at the center.

Yet, we regret the continued lack of implementation of laws, norms, and accountability mechanisms to hold states to account for their cyber actions. Violations of international law and the agreed normative frameworks on responsible state behavior, both online and offline, need to be called out and opposed through all the means made available by local, national, and international systems. State behavior in cyberspace should be subject to monitoring and periodic review, open to input from non-state actors including civil society; states incentivized to ensure that their conduct is actually in conformity with their commitments; and non-state actors

involved in dangerous cyber behaviors reminded of the existing human rights and humanitarian frameworks protecting communities and those civilian objects essential to their survival – which increasingly includes open, secure, and reliable access to the internet.

In light of the current problematic situation, we call on states to take the following actions:

- Stop the deployment of harmful cyber capabilities, activities, strategies, and doctrines, which levy adverse impacts on people globally, obstruct progress under all three pillars of the UN's mandate, and set a precedent for further abuses.
- Put an effective end to all cyber actions directed against critical civilian infrastructure and services, including health and information infrastructure, the public core of the internet, the humanitarian sector, and the civilian population in general.
- Reiterate the necessity to implement the recommendation from *The New Agenda for Peace* to "establish independent multilateral accountability mechanisms for malicious use of cyberspace by States," and to adequately include digital and cyber elements in the legal assessment and proceedings under existing multilateral and international accountability mechanisms. Ensure robust avenues for non-state contributions and inputs throughout these processes.
- Continue to convene focused discussions and exchanges about how international law applies in its entirety in the ICT environment. In particular, states should put forward opinio juris that reaffirms the applicability of international human rights law and international humanitarian law in cyberspace, at all times.
- Recognize human rights and humanitarian impacts of cyber operations and encourage greater transparency in state attribution of responsibility for malicious cyber operations, even when deployed by cyber mercenaries and other proxies. States should invoke international law and the agreed normative framework when condemning state-led and -sponsored cyber actions.
- Refrain from using cybersecurity-related laws, policies, and practices as a pretext to violate human rights and fundamental freedoms. States should address the differential impacts of cyber operations on individuals and groups in society based on their characteristics and identities, such as race, gender, sexual orientation, gender identity or expression, their professions such as journalists and human rights defenders, or other situations of vulnerability or marginalization. We urge states to enable the exercise of civic freedoms in cyberspace and take steps to ensure cyber infrastructure is not weaponized to target human rights defenders.
- Ensure the meaningful participation of non-governmental stakeholders in the current WSIS review, the OEWG, and in the design and operation of any future UN forums or mechanism, as debated in the making of the *Pact for the Future* and the *Global Digital Compact*. Diverse actors have an established role to play in operationalizing and promoting the responsible state behavior framework, including norms and international law, and supported by increasing capacity and resilience, building confidence, and monitoring and responding to cyber incidents.
- The First Committee should clarify where certain applications or uses of AI may fail to meet standards for the protection of peace and human security, actively monitor

developments and deployments, and hold accountable those that threaten to violate these standards.

- Increase complementarity and communication between and among the various processes on cyber-related issues and digital security, including the World Summit on the Information Society (WSIS) and those established by the First Committee, the Third Committee, the UN Security Council, the UN Secretary-General, and related human rights and technical bodies, and by introducing digital and cyber components in the work and language of the other UN bodies and Committees, to make sure that governance, policies, guidelines and regulations are coherent and integrated across sectors and topics.
- Support preventive cybersecurity practices, including by ensuring the legal protection of security researchers investigating and documenting cyber-related issues affecting human security, and promote best practices in this field including but not limited to robust, rights-respecting vulnerability disclosure programs, emergency response teams, and other CBMs that welcome civil society engagement.
- States must explicitly recognize, as the United Nations High Commissioner for Human Rights has, that "encryption is a key enabler of privacy and security online and is essential for safeguarding rights." Secure and end-to-end encrypted communication and storage platforms are crucial for the safety of individuals and cybersecurity infrastructures.

This statement has been endorsed by:

- Access Now
- Amnesty International
- Association for Progressive Communications (APC)
- CIVICUS
- CyberPeace Institute
- Derechos Digitales
- ICT4Peace Foundation
- Global Partners Digital