

ORAL STATEMENT

**Check against delivery*

United Nations Global Mechanism on ICT Security
First Substantive Plenary Session
UN Headquarters, New York

Delivered by: Laura O'Brien, Senior International Counsel, Access Now

Thank you, Madam Chair. I am making this statement on behalf of Access Now, a grassroots to global organization that defends and extends the digital rights of individuals and communities at risk. Our statement today reflects outcomes from consultations with the broader multistakeholder community that have been taking place in preparation for this week. As stakeholders, we look forward to sharing our expertise and experiences during the DTG in December in a constructive and evidence-based manner.

On existing and potential threats, Access Now fully aligns itself with the [statement made yesterday by Kenya ICT Action Network \(KICTANet\)](#). Particularly, the existing threats surrounding the unchecked proliferation of commercial spyware, surveillance, and state-sponsored cyber-harassment used to monitor, intimidate, and silence journalists, human rights defenders, and political dissent. With respect to threats posed by ICTs in armed conflict, we echo the statement made yesterday by ICRC, regarding the alarming range of ICT operations that have disabled the provision of essential services for civilian populations. Out of the [313 internet shutdowns documented by Access Now and the #KeepItOn Coalition](#) in 2025, 125 shutdowns occurred in situations of conflict, impeding access to essential services and communications.

In light of these existing and potential threats we would like to underscore **three priority areas** for further discussion during the DTGs:

First, we urge the DTGs to make the human cost of critical infrastructure attacks visible and foreground the role of civil society in its defense. This requires direct engagement with, and the protection of, the human beings who make cybersecurity possible, including those who provide research, and handle incident response, especially responding to digital security threats against those most vulnerable. This cannot remain an aspiration. States must ensure that national critical infrastructure protection frameworks give real, operational effect to their human rights obligations, while protecting tools like strong encryption and independent research capabilities that enable civil society to contribute.

Second, the rapid increase in capabilities of AI models is a major topic of discussion. We echo calls not to duplicate existing UN processes grappling with questions regarding AI, but rather build on such discussions with a focus on issues of unique value to the Global Mechanism. With that, we call for the specific recognition of [how AI tools are beset by glaring security vulnerabilities that have grave consequences for the confidentiality of our data, information integrity, and access to and the availability of systems](#) – all problems that a human rights respecting approach can help solve. When

human rights are successfully placed at the center of discussions on AI – as witnessed in the other UN processes – the outcomes shift to concrete, enforceable protections for those most at risk.

Third, DTG 1 should build on the substantial body of State practice already affirming that international human rights law and international humanitarian law apply to State cyber behaviour, and turn consensus into shared understanding implementation. We commend the growing number of States that have proactively published national positions on the application of international law to cyberspace, and call on all States to ensure this same rigour is reflected domestically, so that national cybersecurity laws, policies, and strategies are developed and implemented consistent with their international human rights law and international humanitarian law obligations.

In conclusion, Madam Chair, we reiterate our intention to support all States present in the room, especially small states and those with limited resources in delivering on the commitments made in the framework of responsible state behaviour and the objectives for the Global Mechanism.

Thank you.



Access Now (<https://www.accessnow.org>) defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

For More Information, please contact: un@accessnow.org