19 February 2025

ORAL STATEMENT **Check against delivery*

10th Session of the United Nations Open Ended Working Group on ICTs
UN Headquarters, New York

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

Chair, delegates, thank you for this opportunity to address you all today. This year presents an inflection point with respect to cyber institutional dialogue. We have gone from wondering what an open ended working group could do, to this pen-ultimate session of the OEWG's second iteration. So what's next? We believe there are five critical issues which you all must address today. Underpinning these issues, we call for a commitment to advance a human centric approach to cybersecurity in the context of responsible state behaviour. For reasons of length, I will briefly cover **five** critical issues and turn your attention to our written remarks for further elaboration.

First, on capacity building: our international efforts are doomed to fail if we do not invest in better capacity building on human rights respecting approaches to cybersecurity law and policy. The crucial role of civil society must be acknowledged, starting in the Tabletop exercises.

Second, on threats: the global commercial spyware market must be recognized as a key threat in the OEWG's report. Spyware is regularly being used to target civilian populations and other key stakeholders. Strong encryption enabling secure communications is one of the few, affordable, and accessible tools to protect victims.

Third, on rules and norms: as illuminated in yesterday's event on victim-centric approaches, the OEWG must ensure meaningful implementation and incentivize improved proactive action by states to combat the prevalence of the commercial spyware sector. We agree that this would provide a new, meaningful, proactive action under norm (i).

Fourth, on international law: we welcome the statement on ICRC's 34th Conference and the approval of the first humanitarian "ICT Resolution" and accompanying legal brief assessing humanitarian protection through the lens of ICT systems. Together, they provide a clear first articulation of the legal reality – that international law, including international humanitarian law, does apply to cyberspace and impacts the actions taken by States while not in itself condoning or encouraging militarization.

Finally, on regular institutional dialogue: a few delegates have proposed that the model of the UN AHC to combat cybercrime should be adopted for global cybersecurity, creating a new treaty instrument on the issue of responsible state behaviour to ICTs. We believe this fails to recognize the reality that the Cybercrime Convention was adopted on the unfortunate argument that "no treaty is better than a bad treaty." While the modalities of the UN AHC were an improvement on the model for stakeholder participation for the OEWG, we would challenge that its model of condensed negotiation resulted in an improvement for global cybersecurity, human rights, and our international legal order.

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:

Raman Jit Singh Chima | Global Cybersecurity Lead| raman@accessnow.org

Peter Micek | General Counsel | peter@accessnow.org

Laura O'Brien | Senior International Counsel | laura@accessnow.org