6 March 2024

ORAL STATEMENT **Check against delivery*

Dedicated Stakeholder Segment 7th Substantive Sesion
UN Open Ended Working Group on ICTs 2021-2025
UN Headquarters, New York

Delivered by: Peter Micek, General Counsel & UN Policy Manager at Access Now

Your excellencies, distinguished delegates, and colleagues, thank you for the opportunity to present our viewpoints and add to the significant expertise that is regularly convened thanks to the meetings of this OEWG.

In 2024, we face a global context where the attack surface for cyber operations has increased, given the rapid - if still far too unequal - digitisation of our societies. The effects of malicious cyber attacks are also correspondingly more significant - from spyware and the targeted hack-by-hire operations that so many human rights defenders and journalists face, to systemic efforts that target processes and institutions crucial to voting in this 'year of elections'.

We urge you to recognise the intersectional harms caused by malicious cyber threats. As we celebrate International Women's Day later this week, we draw your attention to our most latest report on Pegasus spyware attacks published last month which showed more than 35 people in civil society attacked, including a founder of a civil society organization aimed at empowering women in politics and an award-winning human rights lawyer who works with human rights organizations to defend women's rights, workers' rights, and freedoms of opinion, expression, and peaceful assembly. Such unlawful, targeted surveillance made possible by the organized, for-profit exploitation of cyber vulnerabilities by the global spyware industry constitutes a form of violence against women and bears particular adverse impacts on women in all their diversity

We therefore urge the OEWG to explicitly name cyber mercenaries and the hack-for-hire industry more generally - and spyware developers and operators in particular - as a key existing and potential threat in its 2024 reporting, which all states are under an obligation to take action against. We need to recognise that the global hack for hire spyware industry constitutes a threat to the stability of the internet as a whole.

We take note of the draft checklist prepared by the Chair of this present OEWG, and welcome the effort that it represents in helping responsibly advance upon the international consensus secured by the past OEWG and the voluntary non-binding norms articulated by the UN Group of Governmental Experts (GGE). Today, we wish to draw your attention to our views regarding the draft guidance proposed regarding Norm E and Norm J in particular, dealing with human rights and responsible reporting, coordination around ICT vulnerabilities.

With respect to the draft guidance on Norm E, we thank the Chair for asking the insightful guiding question around "What global or regional processes already exist to address human rights, including

the right to freedom of expression in the use of ICTs". In this regard, we are glad that the Chair's draft text explicitly recognises the consensus principles advanced by the UN itself via the Human Rights Council resolution on the 'promotion, protection and enjoyment of human rights on the Internet' and the General Assembly's landmark resolution on the Right to Privacy in a Digital Age. We recommend that the checklist include a clear guiding question to states on how they implement these resolutions in their domestic and international cooperation capacities with respect to cybersecurity. We also believe that the checklist would benefit from the recommendations advanced by the Freedom Online Coalitions's 2014 established working group on 'An Internet Free and Secure', specifically on a human rights framed definition of cybersecurity.

We also welcome that the draft guidance for Norm J continues to recognise the importance of legal frameworks and protocols to enable reporting of vulnerabilities, as well as explicitly noting the need to provide legal protections for researchers and penetration testers. As we have stated in this OEWG and other processes dealing with cybersecurity and cybercrime in the United Nations, a human-centric approach to global cybersecurity requires explicitly protecting the human beings who help advance cybersecurity, including good faith security researchers, digital security trainers, as well as civil society and journalists more generally.

We also wish to emphasize that coordinated vulnerability disclosure is a crucial confidence building measure, and one which is still underdeveloped and under discussion within this OEWG. We propose that dedicated time be made available to discuss approaches and potential voluntary initiatives which states and stakeholders could advance on coordinated vulnerability disclosure.

As we have said, further discussion on responsible cyber behavior in open, accessible spaces is itself a confidence building measure. We hope that the OEWG and attending delegations seriously consider the many concerns raised by different stakeholders regarding challenges in accreditation and participation in these global cybersecurity discussions. By broadening meaningful participation, our discussions will also be further informed of the many innovative and diverse capacity building initiatives in the space of responsible cyber behavior which exist. In that spirit, we invite the delegations of the OEWG to participate in the capacity building and confidence building processes taking place at our RightsCon summit series, which will next convene in East Asia in February 2025.

Thank you.

For More Information, please contact:
Raman Jit Singh Chima | Global Cybersecurity Lead | raman@accessnow.org |
Laura O'Brien | Senior UN Advocacy Officer | laura@accessnow.org |
Peter Micek | General Counsel | peter@accessnow.org |