Access Now remarks for UN OEWG-II Third Substantive Session stakeholder interaction

Guiding Questions 1 and 2

27 July 2022

Remarks delivered by Peter Micek, General Counsel and UN Advocacy Manager

Amb Gafoor, Secretariat members, and OEWG delegates joining this discussion:

Thank you so much for this opportunity to speak. As you know, Access Now is an international human rights organization that defends and extends the digital rights of users at risk; we provide direct technical assistance worldwide through our Digital Security Helpline for human rights defenders and journalists, and engage in key discussions around cybersecurity policy and human rights.

At the outset, we note that we have seen the OEWG as a key confidence building measure in itself. We have been glad to see its efforts to find consensus among states on urgent issues impacting human rights, development, and peace and security. However, we are deeply concerned about the undermining of this way forward. This "smoothie" lacks key ingredients - stakeholders from civil society, the corporate sector, and cybersecurity incident response were prevented from joining our discussions and providing the critical inputs we need.

Advancing improved global network security requires that the OEWG recognise the widely spread, networked nature of different actors involved in furthering cybersecurity. Civil society plays a critical role in supporting and growing capacity-building with respect to cybersecurity. It is civil society security researchers who have detected the use of spyware and unveiled the scale of the global hack-for-hire sector, which is helping proliferate the use of malware and software exploits globally. We document – and our colleagues suffer – adverse impacts on human rights and dignity, including from disruptions to connectivity like internet shutdowns. Independent security researchers at the national level detect vulnerabilities in public and private sector systems, filing bug reports and engaging in public awareness raising and robust conversation on how to better improve cybersecurity across nations and networks. These reports secure elections and protect policymakers, among other beneficiaries.

We engage and build capacity with these communities through many initiatives - the Civil Society Incident Response network (CiVICERT), our global 24/7 Digital Security Helpline, and RightsCon - the global conference summit series on human rights and technology. We welcome discussion with OEWG participants on how these platforms can support this ongoing work.

The OEWG would be enriched by asking civil society cyber security networks on how they seek to spread better digital hygiene, conduct digital security training, and respond to the digital security threats faced by the most vulnerable. As part of this, the OEWG should also seek to collect and document what **best practices exist** at the national level for government and private sector stakeholders to engage with civil society, as well as what threats and systemic challenges may face the civil society information security community. As we have mentioned, a human-centric approach to cybersecurity needs to include a focused pillar on protecting and encouraging the human beings who make cybersecurity possible, especially for our global civic sphere. **Cyber threats to human rights defenders, journalists, and humanitarian actors must be referred to in the report of the OEWG**.

In doing so, the OEWG would also recognize the extraordinary growth in cybersecurity attacks and efforts to compromise human rights defenders and humanitarian actors globally. The work of the OEWG over 2022-23 must include a recognition of these attacks and add to the international consensus against allowing state and non-state actors using cyber means to target humanitarian actors, journalists, and human rights defenders. **Our international *acquis* on cybersecurity must further consolidate the recognition that international humanitarian law applies to cyberspace and that international law does apply to cyber offensive activities**. We support the joint call made by Switzerland on behalf of itself and 16 other states across the Global North and South, and strongly believe **an explicit mention of international humanitarian law, the role of the ICRC, must be added to the report**. **The OEWG must recognise in its report that digital rights violations - including those taking the form of cyber attacks that enable and escalate offline violence, and the calculated attacks targeting digital systems essential to people's safety, rights, and wellbeing are unacceptable**.

Thank you, Chair. I will submit my remarks in writing.