30 July 2024

ORAL STATEMENT
UN Headquarters, New York

**Check against delivery*

United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes

Intervention during 4th meeting of reconvened concluding session (Day 2 Afternoon)

Delivered by: Raman Jit Singh Chima, Global Cybersecurity Lead | Senior International Counsel and Asia Pacific Policy Director

Thank you Madame Chair. We appreciate the efforts made by you and many participating delegates to the AHC over the last three years in trying to ensure that we have meaningful deliberations and a fit-for-purpose, human rights-respecting convention.

Access Now supports the interventions made by several other stakeholders, particularly my colleagues from Human Rights Watch, Derechos Digitales, and R3D, as well as the inputs shared by the Cybersecurity Tech Accord, Microsoft, and the International Chamber of Commerce.

As an organization that has been committed to and engaged with this process from its start, we will speak with full candor. We should not be happy with where we are. We draw your attention to what we said in February this year: **the United Nations should only put its name on a cybercrime convention that narrowly focuses on tackling cybercrime, and which is not used as a tool to undermine human rights**.

Today, in July, while recognising some efforts made to improve the text, including the proposed Article 6 on human rights and other language, we unfortunately would repeat what we were forced to say earlier: **this text should not be accepted as-is by the United Nations**.

Despite what we may sometimes be tempted to think while we are enmeshed in the heat of these time-bound negotiations, **having a bad UN cybercrime treaty is not better than having no treaty**. If this treaty is not further improved, if states are not clearer on protecting human rights and ensuring due-process safeguards, protections to security researchers, then this convention - even if accepted - will be born into uncertainty and turbulence. States will not be able to sign, and even fewer able to say with certainty that they will be able to ratify. But even if states do not sign or ratify, the harm will be done - **this AHC will change international law and put in place standards that will be referred to**. It is in that spirit that we draw your attention to areas of language where we have deep alarm. Our colleagues have drawn attention to several areas; we ask you to focus on the following:

Firstly, on security researchers and what has sometimes been called “good faith” protections. We appreciate the recognition of this key issue through these deliberations. However, the language currently in the treaty is still insufficient, as has been said by civil society and industry engaged in

cybersecurity repeatedly. Security research is not done merely for service providers, and is not pre-authorised in each instance. Therefore, the AHC must fix the language of Arts 7.2 and 11.2 in the criminalisation chapter; references to "authorized" with respect to security testing and penetration should be removed. And delegates should alter proposals to add to the preventive measures provision, to improve the language of the new Art 53(e) by removing the language that limits it only to security research that benefits service providers. We would not want the legacy of the UN's cybercrime convention to be that it actually made us more cyber insecure.

Secondly, address calls to improve the issue of intent language. We support the calls to improve the intent language in Articles 7 to 11. And we draw attention to the current draft Article 18 lacking clarity concerning the liability of online platforms for offenses committed by their users, specifically that it lacks the requirement of intentional participation in offenses established in accordance with the Convention. This also contradicts Article 19 which does require intent.

Thirdly, and the most disappointing of all, on the proposed safeguards in Articles 24 and 35 and how it seeks to wind back the clock - or perhaps even delete - current protections around the right to privacy in a digital age. The standard that must be used is that of "necessity, legality and proportionality", as called for in international human rights law and numerous domestic legal systems.

A UN Cybercrime Convention should not be used to delete or unjustly alter the last two decades worth of international law on human rights and privacy in the digital age.

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 | Senior International Counsel | raman@accessnow.org

Laura O'Brien | Senior UN Advocacy Officer | laura@accessnow.org