Access Now's statement to the fifth session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes

Discussion on Item 6: Preventive Measures
19 April 2023

Delivered by Raman Jit Singh Chima (Senior International Counsel | Global Cybersecurity Lead)
Check against delivery

Thank you chair for this opportunity to take the floor again. I address the AHC now on the issue of preventive measures.

We welcome the recognition that participation of civil society is crucial to help prevent cybercrime. We must seek to advance an effective, whole-of-society approach to combating cybercrime rather than approaches that only advance a law enforcement and prosecution centric model. We therefore urge delegates to retain and strengthen the language in this chapter around the meaningful engagement with civil society and stakeholders on how states will advance and implement preventive measures under this proposed treaty.

We also support the recommendations made by the Office of the United Nations High Commissioner for Human Rights on adding language to Article 92 requiring the evaluation of any adverse impact on human rights as a result of the implementation of measures under the Convention. In addition to performing a vital substantive role of ensuring that these safeguards actually work in practice, these assessment and oversight mechanisms will also increase public trust in the treaty mechanisms and improve confidence at the national level amongst stakeholders with agencies seeking to prevent and combat cybercrime.

We have heard repeatedly from several delegations in the discussion on this item that "prevention is better than cure". We agree, but also caution that ill advised preemptive treatment can be as deadly as any disease or badly conducted curative surgery. We therefore strongly caution against proposals to compel private providers and technology platforms to proactively prevent and combat combat, that have the risk of encouraging further unaccountable human rights harming practices by such entities. We are also extremely

alarmed at a proposal made during this discussion to add a provision aimed at preventing “incitement” as a preventive measure within this chapter. As discussed previously, criminalizing “incitement” as a cybercrime is outside the consensus demonstrated during this AHC, and would be detrimental to human rights if forced into this instrument.

We also note the discussion in this item around broader cybersecurity. We recognise the desire of many delegations to keep a limited, precise focus for this proposed treaty and avoid broader discussions around cybersecurity that may be subject to General Assembly First Committee related mechanisms or other UN cyber processes. It is our belief that the broader objective that we all share is to make us more cyber secure. Some proposals made in this present session and in the previous session would undermine that broader objective. Overbroad criminalisation of information security practices would chill security research. Advisories, alerts and more on cyber incidents or cyber criminals will not happen if there is broader chilling of the security research community. And proposals to compel the collection and retention of log data, or forcing technology providers to mandatorily collect identity information and authenticate users would have wider, potentially harmful cybersecurity impacts by creating “treasure troves” of data attractive to criminals and malicious actors, as well as directly intruding upon protected human rights more generally.

Lastly, we support calls made by delegations to include provisions in this chapter on preventive measures that encourage states to provide effective alternate channels so that individuals can find opportunities to use their talents for non-criminal cyber purposes. Our approach to international efforts to address cybercrime must be informed by a pragmatic and informed approach to the human beings involved in these issues and where information security, cyber talents can be used - rather than by focusing solely on demonisation or prosecution heavy approaches.

Thank you for letting us take the floor again, chair, delegates.

—