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

Item 4 - Provisions on criminalisation
31 May 2022

Delivered by Raman Jit Singh Chima (Senior International Counsel and Global Cybersecurity Lead)

[Check against delivery]

Chair, my thanks for allowing Access Now to take the floor. Access Now is an international organization that defends and extends the digital rights of users at risk around the world; in furtherance of this, we operate a global Digital Security Helpline for civil society to mitigate specific technical threats and are a member of the Forum for Incident Response (FiRST).

We again wish to share our appreciation for the tireless efforts made by the Chair, the Vice Chairs, and the secretariat in driving forward this important - albeit challenging - discussion. This process will be successful if we are open about the issues we face, honest about the competing interests that have to be managed, and remain committed to a focused future convention.

We agree with what many delegations have said, namely that issues of broader cybersecurity or technical internet governance are outside the mandate of this AHC. However, as many of us have seen far too often, overbroad cybercrime criminalization and enforcement can indeed negatively impact cybersecurity, by legal uncertainty or even hostility impacting security researchers. We are therefore heartened by many delegates and stakeholders engaging with the AHC recognising this concern, and specifically would like to thank the Chair and Secretariat for very clearly calling out the issue of protecting cybersecurity researchers, including those focusing on penetration testing. As we have said before, any international cybercrime treaty cannot make us more cyber-insecure, by adding to any legal uncertainty or threats faced by the humans who make cybersecurity possible.

We are in favor of cyber-dependent crimes being the main focus of the convention. It is too easy to otherwise create an ever expanding laundry list of cyber-enabled crimes. In particular, we wish to restate that the content-related measures should not be included in the proposed treaty; the scope for those to intrude upon internationally protected human rights is too great and would in turn reduce confidence in and the smooth functioning of any future treaty. We support the suggestion made by several delegates that if several delegations believe they wish to secure increased, gradual

international harmonization on cyber-enabled crimes - despite the clear challenge of that task - that they consider the approach of future, optional protocols to this treaty after securing a consensus way forward on core, cyber-dependent crimes. Additionally, we note the comments made by several states regarding international legal cooperation being possible on cyber-enabled crimes even if they are not universally criminalized; we look forward to the discussions in the days ahead on procedural measures and approaches there, including states views around dual criminality as a possible way forward on cyber-enabled crimes.

We therefore welcome the approach followed by the Chair and Secretariat in the guiding questions, where AHC delegates have been asked to explain and justify the inclusion of additional types of acts as potential cybercrime. We also have recommended that states should indicate where cyber-enabled activities are criminalized at the national level, and that the AHC could consider creating a compendium of such domestic criminalisation definitions in order to facilitate increased international agreement and understanding around where dual-criminality on cyber-enabled crime may already exist amongst states.

Chair, delegates: We urge you to engage in your deliberations over the next few days with the following guiding principle, borne by the lived experience of people in far too many countries across the world dealing with overbroad or vague cybercrime laws: Combating the use of the internet and information systems for criminal purposes must not come at the expense of people's ability to freely exercise their rights, online and offline.

—