Access Now's statement to the fourth 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 - Criminalisation
13 January 2023

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

Madame Chair, we thank you for this second opportunity to speak at this fourth session of the Ad Hoc Committee. I know that other stakeholders have been given the chance to take the floor late today on a busy Friday, but we hope that while we may be the last today, that we indeed are not the least in our impact on the further deliberation of delegates.

I will keep my remarks here focused on the issue of the current language of Cluster 1 provisions in the chapter on Criminalisation, and its impact on good faith security research and on human rights.

As we have stated previously in the sessions of the AHC, this proposed international cybercrime treaty should not make us more cyber insecure. We must ensure that legitimate information security research - crucial to revealing and fixing the ICT vulnerabilities that are often exploited for cybercrime - has a legal backstop it can rely on. A positive obligation must be cast on states to help protect and encourage the security researcher community, as well as ensure that criminalisation should not chill the work of journalists, activists and the human rights community.

We have been heartened that many delegations have acknowledged the importance of this, and indicated their openness to ensuring that the language around the core cyber dependent crimes, now those included in Cluster 1, ensures that criminalisation does not chill security research. However, it is clear that AHC delegates need to do more to ensure that they proactively reduce the legal uncertainties triggered by cybercrime provisions for the human beings who make global cybersecurity possible - security researchers, digital security trainers, and the wide responsible/ethical infosec community.

Several delegations have indicated that if the language of Article 10 contains the term "authorized testing", it would serve the purpose of providing legal certainty to good faith security research. Unfortunately, this is not the case. While some elements of cybersecurity assistance and security research may be specifically authorized - for example, penetration testing that is specifically contracted by a party - a large part of the everyday security research that improves the security and

integrity of digital technology is not always authorized in advance. By way of illustration, bug bounty programmes - where security vulnerabilities are disclosed to private sector and public sector entities in exchange for a reward - rarely involve a specific person being authorized in advance. And the work of journalists and others who reveal vulnerabilities in our institutional efforts on cybersecurity and the avenues exploited by cyber criminals, is rarely authorized in advance.

We therefore urge that the AHC consider ensuring that strong language around requiring intent remains in the Cluster 1 provisions, and is included in all the Cluster 1 articles or included as a general safeguard applying to the entire cluster. Language proposing a prerequisite of “authorized” when indicating that security research should be exempt from criminal liability, as originally proposed in Article 10 sub-para 2 of the previous draft of the CND - must not be retained. In that respect, we are glad to note the omission of “authorized” in Article 10 of the updated version of the CND as published yesterday.

Thank you Madame Chair, delegates.

—