Access Now's statement to the first session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes (11 March 2022)

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

Item 4 - Objectives and Scope [Check against delivery]

Thank you madame chair. We appreciate the efforts made by delegations to this important process, the secretariat, and yourself in driving a consensus way forward on addressing cybercrime in a manner that respects human rights and recognises the nature of present threats to individuals and vulnerable communities.

We note the emphasis laid by many states that the scope of the convention must include encouraging the active participation of individuals and groups outside the public sector in the fight against the use of ICTs for criminal purposes/cybercrime, including in raising public awareness regarding the existence, causes, gravity of and threat posed by the use of ICTs for criminal purposes/ cybercrime.

We agree with the repeated statements made by several delegations on the need to keep the work of this Ad Hoc Committee separate from other General Assembly processes addressing wider issues of cybersecurity. We do however believe that the Ad Hoc Committee must work to ensure that efforts to secure increased international cooperation and harmonization on combating cybercrime must not come at the cost of making it harder to strengthen our cybersecurity. Any international convention on cybercrime must not make us more cyber-insecure.

It is now globally recognised that cybercrime laws and their implementation can sometimes unfortunately result in unlawful surveillance, improper persecution, or harassment of security researchers; the very people who help ensure our cybersecurity is enhanced.

We must protect the humans critical to ensuring global cybersecurity.

The Ad Hoc Committee must therefore ensure that it does not create international legal frameworks that generate uncertainty for or directly enable the persecution of the information security community. Authorities must not create hostile environments for those who speak up with concerns about information security; specifically, they must seek to not persecute, discredit, or defame individuals who express their concerns about computer systems, security mechanisms, databases, and other related tools. We must ensure that we create clear requirements around "intent" when criminalizing unauthorized access, and that national laws across all agreeing states require a heightened intent requirement that is beyond mere knowledge in cases of unauthorized access to computer systems or databases.

We therefore emphasize that protecting security researchers is critical to ensuring the active participation of individuals and groups outside the public sector in the fight against cybercrime.