Privacy International, Electronic Frontier Foundation, and Human Rights Watch'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
May 2022

Item 4

[check against delivery]

Privacy International, Electronic Frontier Foundation, and Human Rights Watch welcome the opportunity to participate in the second session of the Ad Hoc Committee.

Preliminary remarks on criminalisation

We have observed that, even as cybercrimes often threaten peoples' rights, efforts to address and combat cybercrime have also given rise to risks to human rights abuses due to vague and overbroad definitions of criminal offenses, disproportionate penalties, and abusive applications of criminal law taken in the name of combating cybercrime. As the Office of the High Commissioner for Human Rights noted in its submission to the first session, we have also noted "the common use at national levels of cybercrime laws and policies to restrict freedom of expression, target dissenting voices, justify Internet shutdowns, interfere with privacy and anonymity of communications, and limit the rights to freedom of association and peaceful assembly." (available here: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf)

The discussions at the prior UN debates on cybercrime have shown that there is not yet a shared global consensus on how to define cybercrime. From a human rights perspective, we respectfully suggest states emphasize narrowness, precision, and clarity on the scope of criminal conduct covered by the definition of cybercrime.

We would particularly wish to reiterate the need to focus on crimes that target information and communications technologies (ICTs). Core cybercrimes comprise offenses in which ICTs are the direct objects as well as instruments of the crimes; these crimes could not exist at all without the ICT systems. A useful reference for the types of crimes that are inherently ICT crimes can be found in Articles 2-6 of the Budapest Convention.

Crimes, where ICTs are simply a tool that is sometimes used in the commission of an offense, should not be included in the future treaty. These would include crimes already prohibited under existing domestic legislation, and merely incidentally involving or benefiting from ICT systems without targeting or harming those systems. For example, the extortion of an individual where the demand is delivered by email. The act of extortion is already a crime and email may merely have been the means of delivering the threat.

Even a narrowly tailored treaty that criminalizes core cybercrimes can be misused or abused to violate rights. Ultimately, regardless of what crimes are included in the treaty, they should be narrowly defined and with clear safeguards against abuses.

Furthermore, the proposed convention should reinforce States' obligations under international human rights law to protect people from harm resulting from a criminal activity carried out through the internet while respecting other international human rights standards, in particular in the areas of freedom of expression, the right to privacy, due process standards and general principles of criminal law, for example, equality of resources and proportionality in punishment.