Electronic Frontier Foundation 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

March 2, 2022

Katitza Rodriguez, EFF Policy Director for Global Privacy

Item 4- Objective and Scope

Dear Madame Chair,

The Electronic Frontier Foundation (EFF) welcomes the opportunity to participate in the session and would like to thank the outstanding work of the Ad-Hoc Secretariat in hosting the meeting.

As a starting point, the objectives of this treaty should be dual: addressing specific challenges posed by cybercrime, on the one hand, while ensuring robust protection for human rights in cybercrime investigations on the other.

From a human rights perspective, it is essential that the scope of any convention be restricted to criminal matters. It should exclude national security, cybersecurity, cyberwarfare, or rules for internet governance.

In our joint civil society letter, endorsed by 134 NGOs and experts in more than 56 countries,[1] we caution against casting too wide a net when deciding what crimes to include within this instrument. Just because technology is used in the commission of a crime does not make that act a cybercrime nor should the simple use of technology in the commission of an offense be an aggravating factor.

Content offenses such as misinformation, incitement to terror and copyright infringment should be categorically excluded from the scope of the negotiations.

[1] Letter to the United Nations to Include Human Rights Safeguards in Proposed Cybercrime Treaty, https://www.eff.org/deeplinks/2022/02/letter-united-nations-include-human-rights-safeguards-proposed-cybercrime-treaty

Any included offenses should be carefully articulated and scoped to avoid their misuse in ways that infringe fundamental human rights. Technologically-facilitated conduct is complex and broadly scoped cyber crimes have been used to stifle legitimate and important activity.

Broadly scoped investigative powers should not transform this instrument into a general purpose vehicle for digital evidence gathering. Any cross-border investigative powers in particular should be limited in scope to investigations of specific cybercrimes. Investigative powers should be carefully scoped so that they remain closely linked to investigations of specific criminal conduct.

Thank you.