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 1, 2022

Katitza Rodríguez, EFF Policy Director for Global Privacy

Item 3- General Debate

The Electronic Frontier Foundation (EFF) welcomes the opportunity to participate in the first session of the Ad-Hoc Committee. EFF would like to focus on the importance of having a human-right-by-design approach in the proposed Cybercrime treaty. This priority was also addressed in a joint letter endorsed by 134 civil society organizations and experts in more than 56 countries and sent to the chairperson of the Ad-Hoc committee.[1]

Substantive Criminal Provisions
Madame Chair, efforts to address cybercrime are of concern because cybercrime poses a threat to human rights, but also because cybercrime laws are currently being used to undermine people's rights and fundamental freedoms in ways that are contrary to the obligations and commitments of States under international human rights law. We therefore support previous speakers in calling for the inclusion of human rights safeguards applicable to the proposed Treaty's substantive and procedural provisions. Failing to prioritize the protection of fundamental rights can have dire consequences.

[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

Cybercrime laws have been used against journalists, whistle-blowers, political dissidents, security researchers, LGBTQ communities, and human rights defenders. Indeed, a 2019 UN General Assembly Resolution recognized that cybercrime laws in some instances are being "misused to target human rights defenders or have hindered their work and endangered their safety in a manner contrary to international law".[2]

In its written submissions, the OHCHR raised similar concerns about the misuse of cybercrime offenses and concluded that any cybercrime convention must "expressly ensure that its provisions neither apply nor could be interpreted to apply to improperly restrict conduct protected under human rights standards." To prevent these adverse implications on enjoyment of human rights, in line with ICCPR Articles 2, 17 and 19, the Treaty should focus on core cybercrimes and contain precise and narrow definitions, leaving no room for harmful interpretations in practice.

Procedural & Investigative Criminal Measures

When it comes to procedural criminal measures, we believe that any proposed obligations to enable investigation and prosecution should come with detailed and robust human rights safeguards. Human rights protections should not be optional, and should not defer to case-by-case agreements to define how people will be protected against potential abuses or misuses of new potential powers. It should also avoid barriers that would prevent states from adopting stronger human rights protections. Reliance on any proposed law enforcement powers should explicitly comply with the principle of legality, necessity, and proportionality.

Moreover, it's imperative to apply robust protections when authorities are seeking access to cross-border digital evidence. In a report of the UN Security Council's Counter-Terrorism Committee, it noted the risk of ending up with lower procedural standards in the process to universalization. It highlighted that, in attempting "to address law enforcement's jurisdictional problems, the substantive law will become weakened, giving law enforcement too-quick access with too-little due process."[3]

Indeed, as we state in our joint civil society letter, "there is a real risk that, in an attempt to entice all States to sign a proposed UN cybercrime convention, bad human rights practices will be accommodated, resulting in a race to the bottom." Bearing in mind the global nature of the Treaty, it will be crucial that human rights stay front and center in the treaty negotiations and that a race to the bottom in terms of human rights protections is avoided.

We do not want a global treaty that does more harm than good, and therefore, call for adherence to strong human rights and procedural safeguards into the Treaty. This will

---

[2] Resolution adopted by the General Assembly on 18 December 2019, https://undocs.org/en/A/RES/74/146

[3] United Nations Security Council Counter-Terrorism Committee, The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspectives, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf

ensure compliance with States' international human rights obligations under the Universal Declaration of Human Rights and ICCPR, and most importantly, prevent a chilling effect on human rights all around the world.[4]

[4] OHCHR key-messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf