Dear Madame Chair,

Thank you for the opportunity to speak today.

Cybercrime is a global problem that affects states, businesses, and everyday people around the world. Increased law enforcement powers to gather digital evidence are increasinly requested to combat cybercrime/counter ICT for criminal purposes.

Still, cybercrime has the potential to threaten human rights unless detailed robust safeguards are built into new treaties, and are effectively implemented in national legal frameworks to avoid abuses of power and protect privacy, due process, and other human rights. We believe that states' human rights obligations should guide how Member States respond and act to counter cybercrime. They should be woven into the fabric of treaties as they are developed. This is needed to make absolutely clear that States are bound under international human rights law to ensure that human rights are honored and upheld as a matter of course.

We hope we all can commit to ensuring that this convention does not do more harm than good.

General Provisions

Madame Chair, human rights should be treated in the convention as one of the founding principles of addressing cybercrime/countering ICT for criminal purposes. To this end, the Preamble should acknowledge that the rights people enjoy offline must also be protected online, including the right to freedom of expression and privacy.

We support OHCHR' statement that the Convention should reference international human rights laws or regional human rights instruments and standards in the Preamble to the extent they can guide the elements, interpretation and application of the Treaty.

The Preamble should also acknowledge that the use of encryption and anonymity is vital to human rights and exercising freedom of expression online, as well as to the work of civil society, human rights defenders, and journalists. The treaty should recognize and make clear that restrictions on the use of encryption and anonymity tools constitute restrictions on freedom of expression and must be avoided at all costs. This is consistent with international human rights standards in this area.

We also support OHCHR's statement that human rights provisions should be applicable to both the substantive criminal provision as well as the criminal procedural measures and law enforcemnt.

On the criminalization section,

From a human rights perspective, it is essential to ensure any potential treaty defines offenses in precise terms that do not threaten or undermine rights and to keep the scope of offenses narrow to focus on core cybercrimes. Government responses to cybercrime that are overbroad or vague risk being ineffective or disproportionate and can undermine rights.

International human rights law requires any regulation of freedom of expression to be necessary for a legitimate purpose, and proportionate to that end. Even when a law has a legitimate purpose, governments are obligated to specifically identify the nature of the threat being addressed and how the measure proposed is both a necessary and proportionate means of addressing it.

The third part of my presentation focuses on **Procedural Measures and Law Enforcement.**

We believe that human rights protections and safeguards should drive the scope of the Convention's provisions governing criminal procedure and law enforcement powers. How and under what circumstances police are allowed to access data during investigations can implicate people's rights and put them at risk. We believe that the treaty's scope and its provisions should be narrow and designed explicitly to prevent overreach and abuse. The convention should contain a narrow list of offenses, and provisions concerning procedural and investigative measures should apply only to that list.

At a minimum, the Convention's safeguards should:

- explicitly prohibit all data processing and any interference with the right to privacy that is not lawful, necessary, legitimate, and proportionate.
- be detailed and robust, and should ensure that interferences with privacy are premised on independent, preferably judicial authorization, based on a high degree of probability that the intrusion contemplated could likely yield evidence of a specific serious criminal offense;
- should ensure that all human rights incursions are safeguarded against and that artificial data labels (e.g., 'subscriber data' or 'metadata') are not used to justify disproportionate interference with privacy;

- establish clear data protection obligations that meet the highest standards among state parties concerning personal information collected, used, disclosed, shared, or retained in relation to the Convention.

The Convention's safeguards should also include measures to ensure human rights protections are fully realized in the treaty's implementation. These should include the following obligations on States:

- mandatory annual transparency reporting on the use of any intrusive surveillance powers, including statistical reporting on the number of data requests issued for the crimes being investigated, and how many individuals or accounts were affected by the measure;
    - Mandatory annual transparency reporting on the number of foreign data requests issued and, for each, the country of destination or origin, the crimes being investigated, whether the request was fulfilled in whole, in part, or not at all, and how many individuals or accounts were implicated by request.
- an obligation to notify any individuals implicated by intrusive investigative measures as soon as notification can occur without threatening an investigation or prosecution;
- effective redress mechanisms for any interference with an individual's privacy regardless of that individual's nationality; and
- rigorous oversight by an independent regulatory body of the operation of any future investigative powers adopted by the Convention, including on the legality, necessity, and proportionality of their implementation and including any cross-border cooperation mechanisms.
- Finally, the convention should not legitimize novel intrusive surveillance tools and techniques that can be inherently be disproportionate in nature. Often, these types of techniques are adopted by law enforcement agencies before receiving full scrutiny by courts or legislatures. The Convention's technical assistance provisions and general criminal powers should not act as a vehicle for the dissemination or sharing of these tools, nor should it operate as a means of legitimizing information sharing regarding the use of these intrusive techniques.

Thank you for your kind attention. You can find more information about our involvement, as a recognized NGO, in the UN Cybercrime Treaty process by visiting our website: https://www.eff.org/issues/un-cybercrime-treaty